Arcserve® Backup for Windows

Implementation Guide

r16.5

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.

© 2015 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.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Updated to include user feedback, enhancements, corrections, and other minor changes to help improve the usability and understanding of the product or the documentation itself.
- Updated How the Installation Process Affects Operating Systems (see page 59). Updated the list of files and objects that are affected by installing Arcserve Backup.
- Updated Unsigned Binary Files (see page 65) and Binary Files Containing Incorrect File Version Information (see page 67) with the latest files.
- Add Binary Files that do not Comply with Windows Security Requirements (see page 69). This topic displays a table of the binary files that do not comply with Windows Security requirements.
- Updated the following topics to include the Allow the Remote Registry service to run for the duration of the remote installation process option.
  - Deploy Agents to Remote Computers Using Automatic Upgrade (see page 113)
  - Deploy Agents to Remote Computers Using Custom Deployment (see page 115)
  - Deploy Agents to Virtual Machines Using Virtual Machine Deployment (see page 117)
- Updated Installing and Upgrading Arcserve Backup in a Cluster-aware Environment (see page 127) chapter. We now support CLUSTERPRO/ExpressCluster X 3.1 for Windows.
- Add Prepare MSCS Cluster Resources on Windows Server 2012 Systems (see page 133). This topic describes how to prepare MSCS cluster resources for Windows Server 2012.
- Updated Ports Configuration File Configuration Considerations (see page 249). This topic now includes information that describes how to configure a custom port or a range of ports for NAS filer to server backups.

Contents

Chapter 1: Introducing Arcserve Backup 11

Introduction 11
Purpose of This Guide 12

Chapter 2: Planning Storage Environments 13

Preliminary Tasks 13
Enterprise Storage Requirements 14
- Budget Considerations 14
- Network and Computer Infrastructure Requirements 15

Data Transfer Requirements 15
- Backup Schedule Requirements 16
- Data Backup Window Considerations 16
- Hardware Data Transfer Rates 16
- Network Bandwidth Considerations 18
- Data Transfer Requirements and Resources Calculations 19
- Data Path Considerations 20
- Alternate Data Path Considerations 21
- Parallel Storage Operations (Multiple Streaming) 24

Storage Capacity Requirements 24
- Online Recovery Data Storage Requirements 24
- Backup Data Storage Requirements 25
- Global Dashboard Data Storage Requirements 25
- Storage Capacities and Resources 26
- Testing Plans and Assumptions 27

Catastrophic Events 28
- Risk Assessment 28
- Off-Site Repository Considerations 28
- Disaster Recovery Archive Considerations 29
- Disaster Recovery Testing 30

Sample Calculations 30
- Transfer Rate for Clients and Servers on a 100Base-T Ethernet LAN With No Subnets 31
- Transfer Rate for Clients and Servers on Two 100Base-T Ethernet Subnets 32
- Transfer Rate for Clients and Servers on a Gigabit Ethernet Network 33
- Transfer Rate for a Server With No Clients 33
- Transfer Rate For Server With SAN Option 34
- Storage Capacity for Two Sets of Recovery Data, One Full and One Incremental Backup 35

Chapter 3: Planning Arcserve Backup Installations 37

Supported Platforms 37
Supported Devices 37
Tape Library Installations 38
Storage Area Network (SAN) Installations 38
Amount of Disk Space Required to Install Arcserve Backup 39
Installation Methods 40
Types of Arcserve Backup Server Installations 41
Arcserve Backup Server Options 45
caroot User Account 45
Database Requirements 46
Microsoft SQL Server 2008 Express Edition Considerations 46
Microsoft SQL Server Database Considerations 48
Agent for Arcserve Database 51
Installation Progress Logs 52
Global Dashboard Considerations 53
Upgrade Considerations 54
Supported Upgrades 55
Backward Compatibility 56
Global Dashboard Upgrades 56
Data Migration from a Previous Release 57
Product License Requirements 57
ALP Key Certificate 58
Arcserve Backup File System Agents Release Levels 58
How the Installation Process Affects Operating Systems 59
Unsigned Binary Files 65
Binary Files Containing Incorrect File Version Information 67
Binary Files that do not Comply with Windows Security Requirements 69
Binary Files that are not Uninstalled Completely 75
Binary Files that do not Contain an Embedded Manifest 77
Arcserve Backup MSI Installer Package Identification 79

Chapter 4: Installing and Upgrading Arcserve Backup 81

How to Complete Prerequisite Tasks 81
Install Arcserve Backup 86
Upgrade Arcserve Backup from a Previous Release 94
Create a Silent Installation Response File 101
Upgrade Arcserve Backup Agents Silently to the Current Release 107
Deploy Agents to Remote Computers from the Primary Server 110
Remote Deployment Considerations 112
Deploy Agents to Remote Computers Using Automatic Upgrade 113

Deploy Agents to Remote Computers Using Custom Deployment 115
Deploy Agents to Virtual Machines Using Virtual Machine Deployment 117
How to Install Arcserve Backup Using Unicenter Software Delivery 120
Register Arcserve Backup on the Unicenter Software Delivery Server 120
Components and Prerequisites 121
Install Arcserve Backup Components Using Unicenter Software Delivery 125
Post-Installation Tasks 126

Chapter 5: Installing and Upgrading Arcserve Backup in a Cluster-aware Environment 127

Introduction to Cluster-aware Installations 127
Deployment Considerations 127
Plan Your Arcserve Backup HA Deployment 128
Deploy Arcserve Backup Server on MSCS 130
MSCS Hardware Requirements 131
MSCS Software Requirements 131
MSCS Cluster Resource Preparation 131
Prepare MSCS Cluster Resources on Windows Server 2008 Systems 132
Prepare MSCS Cluster Resources on Windows Server 2012 Systems 133
Install Arcserve Backup in an MSCS Cluster-aware Environment 134
Upgrade Arcserve Backup from r12.5, r15 and r16 to r16.5 in an MSCS Cluster Environment 143
Uninstall Arcserve Backup from an MSCS Cluster 147
Delete Arcserve Backup Cluster Resources 148
Deploy Arcserve Backup Server on NEC Cluster 150
NEC CLUSTERPRO/ExpressCluster Hardware Requirements 150
NEC CLUSTERPRO/ExpressCluster Software Requirements 151
NEC CLUSTERPRO/ExpressCluster Resource Preparation 151
Install Arcserve Backup in an NEC Cluster-aware Environment 152
Upgrade Arcserve Backup from r12.5, r15, and r16 to r16.5 in an NEC CLUSTERPRO Environment 167
Manage and Configure NEC CLUSTERPRO/ExpressCluster X 3.1 171
Uninstall Arcserve Backup from an NEC CLUSTERPRO/ExpressCluster 172
Stop NEC Cluster Groups 174
Disable Arcserve Backup in NEC Cluster Scripts 175
Enable Arcserve Backup in NEC Cluster Scripts 177
How to Verify a Cluster-aware Installation and Upgrade 180

Chapter 6: Integrating Arcserve Backup with Other Products 183

CA Antivirus Integration 183
Arcserve Replication Integration-IMPW 183
Arcserve Backup Patch Manager Integration 184
Arcserve D2D Integration 184
Define How You Will Back Up Arcserve D2D Sessions 185

How You Manage Arcserve D2D Servers from the Backup Manager 186
How Arcserve Backup Processes Encrypted Arcserve D2D Backup Sessions 192

Chapter 7: Configuring Arcserve Backup 193

Open the Manager or Manager Console 193
Arcserve Backup Home Page 195
First-Time Home Page and User Tutorial 199
Service State Icons 200
Log in to Arcserve Backup 200
Specify Arcserve Backup Manager Preferences 202
Code Pages 204
How Arcserve Backup Supports Multiple Code Pages 204
Specify Code Pages in the Backup Manager Window 205
Specify Code Pages in the Restore Manager Window 206
Arcserve Backup System Account 206
How Arcserve Backup Manages Authentication 207
How to Use the System Account for Job Security 207
Start the Arcserve Backup Database Protection Job 207
Fine-Tune the Arcserve Backup SQL Server Database 208
How to Calculate the Number of Required SQL Connections 209
Database Consistency Checks 209
Specify ODBC Communication for Remote Database Configurations 209
Configure Devices Using the Device Wizard 210
Configure Enterprise Module Components 211
Configure Global Dashboard 211
Configure the Central Site 213
Configure a Branch Site 216
Create File System Devices 220
How to Define Include and Skip Parameters for Arcserve Backup Database Agents 222
Configuring Firewalls to Optimize Communication 223
Ports Configuration File Guidelines 224
Modify the Ports Configuration File 225
Ports Used by Arcserve Backup Components 226
Test Communication Through a Firewall 251

Chapter 8: Uninstalling Arcserve Backup 253

Uninstall Arcserve Backup 253
Uninstall Arcserve Backup Components Using the Command Line 255
Uninstall Agent Deployment Setup Files 258

Appendix A: Troubleshooting Arcserve Backup Installations 261

Setup Cannot Communicate with Remote Microsoft SQL Server Databases 261
Unable to Log In to Arcserve Backup After Installing This Release 263
Arcserve Backup Services Fail to Initialize 264
The Tape Engine Does Not Start on Member Server Upgrades 265
Unable to Log in to Arcserve Backup After Upgrading to This Release 265
Unable to Determine What Devices Are Supported by Arcserve Backup 266
Cluster HA Resources Not Created 268

Appendix B: Using Best Practices to Install and Upgrade Arcserve Backup 269

Best Practices for Installing Arcserve Backup 269
- How to Complete Prerequisite Tasks for Installing Arcserve Backup 270
- Installing Arcserve Backup into a Single-server Environment 271
- Installing a Primary Server with Member Servers 274
- Installing a Primary Server with Member Servers and Devices 278
- Installing a Primary Server with Member Servers and Shared Devices in a SAN 284
- Installing Multiple Primary Servers with Member Servers in a SAN 289
- Installing Arcserve Backup into a Cluster-aware Environment 295

Best Practices for Upgrading Arcserve Backup from a Previous Release 299
- How to Complete Prerequisite Tasks for Upgrading Arcserve Backup 300
- Upgrading a Stand-alone Server or Primary Server 301
- Upgrading Multiple Stand-alone Servers in a Domain 306
- Upgrading Multiple Stand-alone Servers Sharing a Remote Database 312
- Upgrading Servers in a SAN Using a Local or Remote Database 318
- Upgrading Multiple Servers in a SAN and Non-SAN Environment to this Release 324
- Upgrading Multiple Servers Using a Central Database 330
- Upgrading Multiple Servers in a Cluster-aware Environment 336

General Best Practices 343
- Where to Install the Manager Console 344
- How to Install and Manage Licenses 344
- How to Install Arcserve Backup Server-Based Options 348

Appendix C: Acknowledgements 349

MD5 Message Digest Algorithm 349
VMware VDDK 5.1 350
JRE v.1.7 350
Amazon Web Services SDK for Java 1.3 351
Windows Azure SDK for Java 2.0 352

Glossary 359

Index 361

Chapter 1: Introducing Arcserve Backup

This section contains the following topics:

Introduction (see page 11)
Purpose of This Guide (see page 12)

Introduction

Arcserve Backup is a high-performance data protection solution that addresses the needs of businesses with heterogeneous environments. It provides flexible backup and restore performance, easy administration, broad device compatibility, and reliability. It helps you to maximize your data storage abilities by letting you customize your data protection strategies based on your particular storage requirements. In addition, the flexible user interface allows advanced configurations and provides a cost-effective way for users at all levels of technical expertise to deploy and maintain an extensive range of agents and options.

This release of Arcserve Backup for Windows is the next generation in the Arcserve Backup family of products. It builds upon the features of previous releases while providing new functionality to help you maximize your backup and restore performance. Arcserve Backup delivers comprehensive data protection for distributed environments and provides virus-free backup and restore operations. An extensive set of options and agents extends data protection throughout the enterprise and delivers enhanced functionality, including online hot backup and restore of application and data files, advanced device and media management, and disaster recovery.

Purpose of This Guide

This *Implementation Guide* describes how to do the following:

- Plan your storage environment
- Plan your Arcserve Backup installation
- Perform prerequisite installation tasks
- Install Arcserve Backup
- Upgrade Arcserve Backup from a previous release
- Uninstall Arcserve Backup
- Set up alternate installation methods
- Perform post-installation tasks
- Integrate with other Arcserve products
- Use best practices to install Arcserve Backup and upgrade Arcserve Backup from a previous release

Chapter 2: Planning Storage Environments

This section contains the following topics:

Preliminary Tasks (see page 13)
Enterprise Storage Requirements (see page 14)
Data Transfer Requirements (see page 15)
Storage Capacity Requirements (see page 24)
Catastrophic Events (see page 28)
Sample Calculations (see page 30)

Preliminary Tasks

Protecting your data and managing your backup storage is fundamentally a policy issue rather than a technical problem. Technology can implement policy, but it cannot tell you what your policy should be.

Before you can use Arcserve Backup software effectively, you need to analyze your organization's data storage requirements. You need to do the following:

- Understand how your organization's data resources are used.
- Understand how security and availability at any given time can affect your corporation's bottom line.
- Develop a comprehensive, high-level storage plan before you purchase additional hardware or configure Arcserve Backup.

After you have a clear idea of your storage needs, you can develop an implementation plan that allows for:

- Fast recovery of user-deleted files and directories, and database-related data.
- Centralized, single-point backup administration for networked systems.
- Backup operations that do not interfere significantly with normal business operations.
- Adequate quantities of media and adequate numbers of devices for your needs.
- Full recovery from catastrophic data loss.

Enterprise Storage Requirements

To determine your need for vault space, storage hardware, and storage media, you have to translate your high-level plan into a set of concrete requirements. You need to decide:

- How much you have to spend on media, hardware, and network improvements?
- How much data you really need to protect?
- When can you run backups without interfering with other work?
- How much traffic your network can handle during backup periods?
- How long you can wait for an average file or file system to be restored following a data loss?

The following sections discuss these issues in more detail.

Budget Considerations

Sometimes it pays to stress the obvious early in the planning of a major project: each of the parameters discussed in this section comes with a price tag attached. If you need speed, you need a faster, higher-bandwidth network and more and faster backup devices. Both require premium prices.

To meet your speed or data security requirements, you may need to buy more media. Media elements are surprisingly expensive, particularly for newer and faster backup devices.

You need to decide how much your organization can afford:

- To spend on a backup and recovery solution
- To lose in lost data and staff time

Then, do the following:

- Decide what you are prepared to do in order to keep both kinds of costs in bounds.
- Decide whether performance or economy is your primary concern.
- Evaluate the trade-offs discussed in the next section in light of this initial decision.

Network and Computer Infrastructure Requirements

If you have not already done so, you should familiarize yourself with the hardware, network, and site configuration that your backup and recovery plan supports. You should know:

- The numbers and types of computers and workstations you need to back up.
- The identities of computers that have media libraries or devices attached (these are the Arcserve Backup servers).
- The type of SCSI or fiber cabling connecting each library to its server and the transfer rate of the cabling.
- The type of library on each server.
- The type of devices in each library and their transfer rate.
- The degree of data compression that you plan to use, if any.
- The types and capacities of your network, subnets, routers, and so on.

Data Transfer Requirements

The overall data transfer rate for your backup and recovery system sets the amount of time required for storage operations. You have to balance your backup window, backup data, and recovery speed requirements against the capabilities of your existing infrastructure and the budgetary constraints of your organization.

After you have quantified the amount of data that you have and the times when you can back it up, you can roughly estimate the minimum data transfer rate that you must achieve to fully back up the data in the allotted time. Use this requirement as a starting point for the decisions you make later in this section.

To calculate a rough, minimum transfer rate, divide the amount of data by the amount of time available to back up the data:

databackedup ÷ backup_window = required_rate

Example: Data Transfer Calculation

If you have 1 Terabyte to back up and 5 hours available each night and you intend to back up everything in one session, you need to achieve a rate of 200 GB per hour.

Backup Schedule Requirements

The more data you have, the more time, hardware, media, and network bandwidth you require.

You need to decide:

- Whether you need to back up user data only.
- Whether you must also include system configurations and installed applications.
- Estimate the total size for the data that you must back up, allowing a reasonable margin for growth based on past experience in your organization.

Data Backup Window Considerations

As well as the amount of data that you have to back up, your infrastructure and management requirements will depend on the time that is available for backup operations in any given period. Ask yourself the following questions:

- Can you run backups during non-working hours, at night or on weekends?
- Do you have to run backups concurrently with normal business operations because your network is in use round the clock?

Identify the blocks of time that are available during the day and the week. If your organization shuts down for any long periods during the month or year, you might consider these times as well.

Hardware Data Transfer Rates

Your backup hardware is unlikely to be a limiting factor in reaching your target data transfer rate. Most devices are very fast. However, you should evaluate hardware speed at the planning stage. At a minimum, you must have enough hardware, or fast enough hardware, to write your data to storage media within the time allowed. Smaller numbers of fast devices or larger numbers of slower devices can often achieve the same total throughput. Use the information that follows to estimate the aggregate data transfer rate for your hardware.

SCSI or Fibre Interface Considerations

No device is faster than its connection to its data source. Current backup devices connect using standard SCSI or fibre interfaces. The following table lists the common varieties.

Version	Bus Width	Approximate Maximum Data-transfer Rate
Wide Ultra SCSI	16 bits	40 MB/seconds=144 GB/hour
Ultra2 SCSI	8 bits	40 MB/seconds=144 GB/hour
Wide Ultra2 SCSI	16 bits	80 MB/seconds=288 GB/hour
Ultra 160 SCSI	16 bits	160 MB/seconds=576 GB/hour
Ultra 320 SCSI	16 bits	320 MB/seconds=1152 GB/hour
Fibre Channel	1 Gb	100 MB/seconds=360 GB/hour
Fibre Channel	2 Gb	200 MB/seconds=720 GB/hour

You can see that many of the SCSI interfaces and fibre interfaces will be able to handle your requirement of 200 GB per hour. For example, if you are using a Wide Ultra2 SCSI you can achieve 200 GB in less than an hour. Even if you are using a slower SCSI controller you can use multiple SCSI controllers to achieve the aggregate data transfer rate of 200 GB per hour.

Obviously, the SCSI bus or fibre interface should seldom limit your ability to achieve your required data transfer rate. Any of these SCSI varieties could easily meet the 40 GB per hour requirement in our example. Indeed, most could handle the whole 200 GB job in under two hours. A Wide Ultra 160 SCSI could do it in about 30 minutes.

Tape Drive Considerations

There are many kinds of devices. A few of the most common are listed in the following table.

Device type	Approximate Transfer rate 2:1 (compressed data)	Maximum Capacity (compressed data)
DDS-4	6.0 MB/seconds=21.6 GB/hour	40 GB
AIT-2	12.0 MB/seconds=43.2 GB/hour	100 GB

Device type	Approximate Transfer rate 2:1 (compressed data)	Maximum Capacity (compressed data)
AIT-3	31.2 MB/seconds=112.3 GB/hour	260 GB
DLT 7000	10.0 MB/seconds=36.0 GB/hour	70 GB
DLT 8000	12.0 MB/seconds=43.2 GB/hour	80 GB
Super DLT	24.0 MB/seconds=86.4 GB/hour	220 GB
Mammoth-2	24.0 MB/seconds=86.4 GB/hour	160 GB
Ultrium (LTO)	30.0 MB/seconds=108.0 GB/hour	200 GB
IBM 9890	20.0 MB/seconds=72.0 GB/hour	40 GB
IBM 3590E	15.0 MB/seconds=54.0 GB/hour	60 GB

Even though a single device may not be able to give the data transfer rate of 200 GB per hour set by our example, using multiple media devices should be able to achieve this aggregate transfer rate. For example, if you are using Ultrium tape drives, you need 2 tape drives to achieve 200 GB per hour, or 5 DLT 8000 drives to achieve the same throughput.

Network Bandwidth Considerations

Now you need to consider your network. More than any other factor, your available network bandwidth determines the amount of data that you can realistically transfer during a backup period. The following table compares the performance of different types of networks. As you can see, network performance can significantly impede large backup operations.

Network Type	Theoretical Transfer Rate	Realistic Throughput	Realistic Transfer Rate*
10Base-T Ethernet	10 mbps =1.25 MB/seconds	40-50%	500 KB/seconds=1.8 GB/hour

Network Type	Theoretical Transfer Rate	Realistic Throughput	Realistic Transfer Rate*
100Base-T Ethernet	100 mbps=12.5 MB/seconds	80%	10 MB/seconds=36 GB/hour
1 Gigabit Ethernet	1000 mbps=125 MB/seconds	70%	87.5 MB/seconds=315 GB/hour

Note: If you are backing up concurrently with other operations, remember that your backup operations will not achieve the maximum, realistic transfer rate listed.

Data Transfer Requirements and Resources Calculations

If the preliminary calculations outlined in the preceding sections show that your required data transfer rate is feasible given your existing infrastructure, you may be able to stop here. However, preliminary calculations usually uncover conflicts between stated requirements and available time and resources.

If minbandwidth is the amount of data that can be sent in a given time through the narrowest, slowest bottleneck in the path from the backup source to the backup media and if backupwindow is the time available, then the backup process is governed by the following equation:

datatransferred = backupwindow × minbandwidth

In our example, we have a 5-hour window, fast storage devices, and 100Base-T Ethernet. So the Ethernet LAN is our weakest link, and the following equation is true:

datatransferred = 5 hrs × 36 GB/hour = 180 GB

Therefore, to back up 1 Terabyte of data, you have to do at least one of the following tasks:

- Increase the amount of time available to back up data.
- Increase the bandwidth available at the narrowest part of the data path.
- Reduce the size of *datatransferred* by backing up our 1 Terabyte in a series of smaller, independent operations.

The following sections suggest several possible alternatives that will achieve one or more of the above tasks.

Data Path Considerations

If you cannot decrease the amount of data that you need to move in the time available, then a possible solution is to increase the available bandwidth. You can do this either on the network that links data hosts to the Arcserve Backup server or in the hardware that connects the server and the backup media.

Network Enhancements

The network is usually the most significant source of delays in the enterprise-backup environment. If a faster technology is available or feasible, an upgrade may be a good investment.

Example: Network Enhancements Calculation

For example, if we have a 100Base-T Ethernet LAN and the same data transfer requirement as in the example we have been using so far (200 GB per hour), we cannot get backups done in the time allowed (5 hours). It would take approximately six times as long as we have to back everything up. A Gigabit Ethernet network would back up everything with time to spare and would benefit other business operations as well.

Storage Area Networks

A Storage Area Network (SAN) can improve backup performance significantly by moving data over the high-speed fibre connections rather than the slower network connections. In addition to the performance benefits derived from the high bandwidth fibre connectivity and low host CPU utilization, a SAN also improves the overall network performance by off loading the backup data transfer from the enterprise network to a dedicated storage network.

Though a SAN is expensive to implement and maintain, benefits go beyond just backup. A careful analysis of your requirements is necessary before a decision is made to implement a SAN. For information on how Arcserve Backup can help you take advantage of a SAN, see the *Administration Guide*.

SCSI Bus and Device Enhancements

In cases where poor device throughput is the limiting factor or when you have excess capacity on a fast network, you may need higher performance devices or more of your existing devices. If you use an older, slower drive technology, it may pay to upgrade to higher speed devices and faster SCSI buses. But in many cases, it may be better to add devices and, where necessary, libraries. You can then run storage operations in parallel using several devices at once.

Alternate Data Path Considerations

If you cannot upgrade the network or expand the time available for backups, you can almost always reduce the size of the data set that has to be handled during any particular instance of your backup. You achieve this by doing one of the following tasks:

- Segment your network.
- Segment your data so that it is backed up during a series of successive backups.
- Restrict the scope of your backups such that they only store data that has changed since the data set was last stored.

Segment Your Network

In many cases, you can make better use of your existing network bandwidth by placing Arcserve Backup servers on different subnets.

- In the absence of subnets, all backup data has to cross a single network to reach the Arcserve Backup servers. In effect, every piece of data travels sequentially to every node on the network.
- When you subnet your network, in effect you create two or more networks of equal speed, each of which handles a fraction of the backup data. Data travels in parallel.

In our example, if we backed up 500 GB on two subnets instead of 1 Terabyte on the entire network, we could back up twice as fast. Each subnet could transfer its 500 GB at 36 GB per hour for a total elapsed time of 14 hours (versus 28 hours). In our 5-hour backup window, we could transfer 360 GB, which, though not enough, is still far better than the 180 GB we could attain over a network that is not subnetted.

Segment Data

Nothing forces you to treat all of your organization's data as a single unit. It often makes better sense to *segment* the data into logically related chunks before trying to back it up. This reduces the time required for any single storage operation, makes better use of short backup periods and works better on slow networks. You still back up all of your data. You just do it in a series of shorter operations spread over several days.

We might, for instance, back up 20% of the 1 Terabyte of data in our example each night, Monday through Saturday. In the course of a week, this approach would back up our entire 1 Terabyte across the 100Base-T network, without exceeding the daily 5-hour backup period. As an added benefit, the compact backup elements make locating and restoring our data faster and easier by reducing the scope of searches.

The downside of this approach is that the entire data will not be backed up daily. Most organizations cannot afford to not have daily backups of complete data; therefore, this approach may not be suitable.

You might segment your data for backup purposes in any of the following ways:

- Business function (such as accounting, engineering, personnel management, sales, and shipping)
- Geographical location (such California development lab, St. Louis distribution center, New York business office, Miami business office, Tokyo business office, and Paris distribution center)
- Network location (such as NA005, NA002, NA003, JP001, and EU001)

Your segmentation scheme should, however, group the data into reasonably contiguous backup sources, so that the speed you gain is not lost in lengthy searches and additional network traffic.

Backup Scope

After you have segmented your data, you can further reduce the required data transfer rate by reducing the scope of some backups. Typically, a relatively small percentage of your data changes from day to day. While these changes need to be saved, a full backup is usually unnecessary.

Example: Backup Scope

If you try to back up everything daily and only 10% of the data changes in the course of a day, you are spending 90% of your limited backup time storing data that is already backed up. When you include media consumption and wear and tear on your backup devices, this can be an expensive proposition.

You should consider backing up everything weekly, after 50% or more of your data has changed. You could then use the longer, weekend backup period for your longest storage operation. On a daily basis, you could back up the changes only. This would let you stay within the short, nightly backup window and would economize on media.

Arcserve Backup provides options for you to address this issue with the following types of backups.

- Full backups--stores everything, regardless of when the data last changed.
- Differential backups--stores files that have changed since the last full backup.
- Incremental backups--stores files that have changed since the last full or incremental backup.
- Synthetic full backups--for r16 or higher Windows Client Agents, synthesizes a previous full backup session and all incremental sessions to a full session without the need for previous incremental sessions.

Creating the right mix of full and partial backup operations is something of a balancing act. Ideally, you want each version of each piece of data backed up once. You want to minimize unnecessary duplication that consumes media and time. Therefore, you should keep the following considerations in mind:

- Full backups store all of your data at once. They produce a complete, coherent image of the data as it was at the time of the backup. They also store the backed up data together in a single, easily managed storage object. As a result, backup strategies that rely exclusively on full backups are usually inefficient because the relative percentage of new data in the overall data set is generally small. Full backups save too many files that are already adequately backed up by a previous storage operation.

  In exceptional situations, however, where the bulk of an organization's data changes substantially over short periods, a plan that relies on full backups exclusively may be the best choice. Because, in this case, most of the data is fresh at any given time, the full backup may actually be less prone to needless duplication than a mix of full and partial storage operations.

- Incremental and differential backups let you avoid network congestion and excessive media consumption. They better fit your existing hardware and bandwidth constraints and mesh better with your users' working hours. Incremental and differential backups are faster than full backups. If you do several of them between full backups, many files are still backed up more than once, because the differential backup backs up all files that have changed since the last full backup. This redundancy means that you can restore quickly, because all the data you need for a full recovery is stored in, at most, two data sets (the full and the last incremental).

  Incremental and differential backups are only economical when the volume of changes is small compared to the volume of the data set as a whole. When this is the case, you can store changes on a small amount of media that is rewritten frequently.

- For r16 or higher Windows Client Agents only, synthetic full backups also let you avoid network congestion and excessive media consumption. Synthetic backups are faster than full backups. After you execute the first real full backup (parent), you schedule incremental and synthetic full backups as needed. The synthetic full backup takes the first full backup and all the following incremental sessions and synthesizes them into one synthetic full session. If you need to restore files, only the synthetic full backup is needed since the last full session and all incremental sessions are combined. This redundancy means that you can restore quickly, because all the data you need for a full recovery is stored in one data set (the last synthetic full backup).

Parallel Storage Operations (Multiple Streaming)

If device transfer rates limit your operations and if the necessary network bandwidth is available, you may want to set up your operations to use all of the available devices at once. By distributing the data across parallel streams, this approach greatly reduces the time required for backup operations. It does, however, consume more network bandwidth. Recovery after a catastrophic loss may be faster, since all available devices collaborate to restore all or most of the backup data at once. Arcserve Backup has the capability to automatically create multiple streams based on the availability of tape devices.

Storage Capacity Requirements

So far, we have discussed factors that affect the speed with which backup and restore operations can be performed. But you also need to consider the volume of online data storage that you require.

Online Recovery Data Storage Requirements

You need to figure out how much recovery data you need to store online, in your robotic libraries. Data that is used primarily for archival purposes or for recovery after a catastrophe can be stored offline in a repository or vault. It is unlikely to be needed quickly. But recent backup data generally has to be available in a robotic library so that users can easily locate and swiftly recover the most recent, intact copies of the files they are most likely to lose.

To calculate the amount of recovery data you must store online

1. Estimate the size of an average, full backup.
2. Add the estimated size of an average incremental backup.
3. Multiply by the number of backup sets that your organization wants to have immediately available (“1” for the most recent, “2” for the two most recent, and so on). This is the amount of recovery data you need to keep online:

   recoverydata = (avgsizefull + avgsizeincrements) × numberbackupskept

Backup Data Storage Requirements

You need to reserve online storage space for scheduled backup operations.

To calculate the amount of space required

1. Estimate the size of an average, full backup.
2. Add the average, percent growth of the data set during a typical, full backup cycle.
3. Add the estimated size of an average incremental backup.
4. Add the average percent growth of the data set during a typical, incremental backup cycle.

Global Dashboard Data Storage Requirements

In a Global Dashboard environment, the collected dashboard data (Arcserve Backup data and SRM-related data) from each registered Branch Primary Server is synchronized to the configured Central Primary Server, where it is stored in the central Arcserve Backup database (ASDB). As a result, when selecting the Central Primary Server, the main consideration should be database size. Make sure the selected Central Primary Server is capable of storing dashboard data received from all registered Branch Primary Servers.

Note: For a Branch Primary Server, no additional hardware or software is required beyond the minimum requirements for any Arcserve Backup primary server or stand-alone server.

To calculate the approximate amount of space required for the central ASDB in your Global Dashboard environment, consider the following:

- As each branch site uploads data to the central ASDB on a daily basis, it is estimated that the central ASDB will grow by approximately 4 MB for every 100 nodes (assuming 4 volumes in each node) every day (or 1MB for every 100 sessions every day).
- The number of sessions is calculated by multiplying the number of nodes by the average number of volumes in a node. The number of days of database retention time is determined by the branch Arcserve Backup setup.

- You can calculate the approximate required disk space at the central site by multiplying the estimated daily ASDB growth (1MB for every 100 sessions) by the number of days of database retention time.

  For example:

  If you have 10 branch sites with each site having 10 nodes and each node contains 4 volumes, then the central ASDB will grow by 4MB every day. If the database record is retained for 180 days, then the central ASDB will need to be 720MB.

  - 10 branch sites x 10 nodes x 4 volumes = 400 sessions
  - 400 sessions = 4MB database space growth per day (1MB per 100 sessions)
  - 4MB daily growth x 180 database retention days = 720MB total database space required for the central ASDB

  Note: Any database pruning that is performed at a branch ASDB will be reflected in the central ASDB the next time data synchronization is performed.

Storage Capacities and Resources

Your ability to meet your storage-capacity requirements depends on the following criteria:

- The types of libraries you have
- The number of each type you have
- The types of media each library uses

After you have identified types and numbers of libraries that will be available, you can calculate the capacity of each library using the following formula:

totalcapacity = numberslotsavailable × mediaelementcapacity

In this formula, the numberslotsavailable is the number of slots available in the robotic library and mediaelementcapacity is the capacity of the media elements used by the installed drives.

Media Capacities

The raw capacity of the media varies with the type of drives, the type of media, and the degree of data compression that you are using. You should deduct the following from the raw capacity to arrive at the real data capacity:

Deduct ~10% for overhead.

This allows for the Arcserve Backup media header and various engine-specific overhead information. Note that the overhead may be more if you are backing up a large number of very small files.

Example: Media Capacities

For example, if you try to back up 1 Terabyte on ten media elements that hold 100 GB each (after deducting overhead), media usage will require 100% efficient every time you back up. Because this is unlikely, you need to use eleven media elements. On the other hand, you can back up 1 Terabyte to six cartridges that hold 200 GB each (after deducting overhead), because you have a healthy 200-GB (20%) cushion.

The allowances specified above are important. If you do not set aside space for overhead and variations in media usage, you may run out of media during a backup operation and may, consequently, not have a timely and complete backup.

Factors Affecting Storage Capacity Calculations

Media elements have lifetimes that are usually specified in usage time or numbers of uses or passes across the media. Make sure you take media aging into account when calculating the number of tapes required. Consult the manufacturer's recommendations.

Restrictive media-selection criteria and extensive off-site storage can increase your need for media well beyond the minimums calculated previously.

Finally, the overall size of the data you need to back up usually increases over time. The amount of data increases faster in some organizations than it does in others, but the total amount almost always increases. The preceding calculations assume a more-or-less constant amount of data. So, when you estimate how much you need to back up (1 terabyte in the examples), always allow for growth. Then check periodically to be sure that you always have enough extra storage to accommodate emerging needs.

Testing Plans and Assumptions

After you have made the required estimates, performed all the necessary calculations, and formulated a plan that should work for your organization, you should test it. Set up a pilot test configuration using a scaled down environment and run tests.

Using the Arcserve Backup logs, you can see how good your estimates were. Use the backup logs to:

- Determine if you estimated the correct amount of backup data correctly by checking the size of a full backup generated by your plan.
- Check your estimate of the average percent change in your data by checking the size of the incremental backups.
- Make sure that all the data that should be backed up is backed up.
- Verify if your data and network segmentation tactics have worked as intended.

Catastrophic Events

So far, we have focused on the major threat to your data—routine losses due to equipment failure or operator error—and on the processes common to all backup and recovery efforts. But there are some additional considerations when you are planning your organization's recovery from a major catastrophe.

A catastrophe is a natural or man-made disaster, such as a fire or flood that results in the loss of multiple hosts, a data center, or an entire network, including locally stored backup media and hardware. To handle an extreme emergency, you must provide secure, off-site storage for some of your backup media, and you must keep the off-site data current.

Risk Assessment

Before going further, decide what sorts of disaster you can realistically prepare for, given the importance of your data, the expense of protecting it, the magnitude of the risk, and the corporate policies that apply to your sites.

Consider the following questions.

- What is the likelihood that your organization will face a large-scale disaster that affects the whole region or metropolitan area? Such catastrophes might include earthquakes, large floods, or acts of war.
- What is the likelihood of smaller disasters, such as building fires, localized flooding, or vandalism?
- How much data would you lose in a large disaster? In a small disaster?
- How severely would the loss affect your organization in each case?
- How much is your organization prepared to spend to defend against each of the risks you identify?

Off-Site Repository Considerations

In storage management, the selection of an off-site repository or *vault* is the result of a series of trade-offs.

Vault Security Considerations

The vault should be isolated enough from your main facility to protect the off-site data from the kind of catastrophes you are prepared to guard against.

Example: Vault Security Considerations

- If earthquakes are the biggest threat you need to deal with, the vault should be in an earthquake-resistant building at some distance from your main site or even in another city or a different seismic zone.
- If fire or local flooding is the danger, a storage room in an upper floor of the building across the street might be enough.

Vault Accessibility Considerations

Measures that isolate your data repository from your primary site also make it harder (and more expensive) to keep the data in the remote repository current. To be of use, off-site data has to be reasonably up-to-date, which means it has to be reasonably accessible. A vault in a distant city might protect the data against even the most extreme disasters, but it might be impractical to ship media there on a daily basis.

Vault Expense Considerations

In general, the more secure a vault is, the more expensive it is to use. You pay more for more secure storage facilities. It often takes longer to get media to and from these facilities. The more media you store off-site, the more you have to buy for your main site.

Disaster Recovery Archive Considerations

Because catastrophes will, by definition, strike your infrastructure as well as your backup media, you should assume that you will have to rebuild systems completely before you can start the actual data recovery. For this reason, you should always maintain the following off site:

- Media elements that contain bootable operating systems for the Arcserve Backup servers.
- A current, complete backup of the file systems, databases, and mail servers supported by Arcserve Backup.

You may want to include Arcserve Backup distribution media and a text file that lists your hardware configuration parameters.

Disaster Recovery Testing

To be sure that your data is available after a disaster, you have to periodically test the data that you are archiving. Routine file-backup routines get tested every time a user cannot restore a deleted file. You soon hear about problems and, in general, the results are not too costly. But disasters are, by definition, rare and expensive. When your data center has just burned down, it is too late to find out that your backup routine does not work. So be sure to test these infrequently used processes on a regular basis.

Whenever you install new software or hardware, or change existing procedures, complete the following tests:

- Backup to media as you would for off-site storage and disaster recovery.
- Verify that the backup operation stored all the specified data successfully.
- Simulate a post-catastrophe recovery operation using the backup media from the test.

You should also run brief, simulated, backup and restore operations whenever the opportunity arises. Routine testing lets you exercise and assess your storage processes on an ongoing basis.

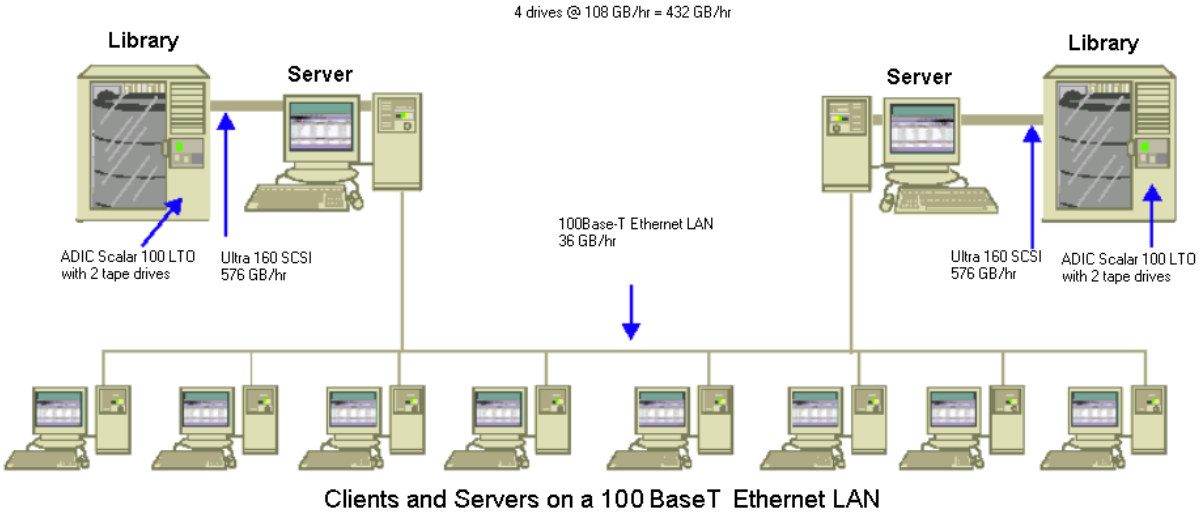
Sample Calculations

The examples below illustrate some representative situations that a backup and recovery plan has to deal with.

Note: It is assumed that the backup server has enough CPU power and memory, and the hard disk speed on the client or server is adequate.

Transfer Rate for Clients and Servers on a 100Base-T Ethernet LAN With No Subnets

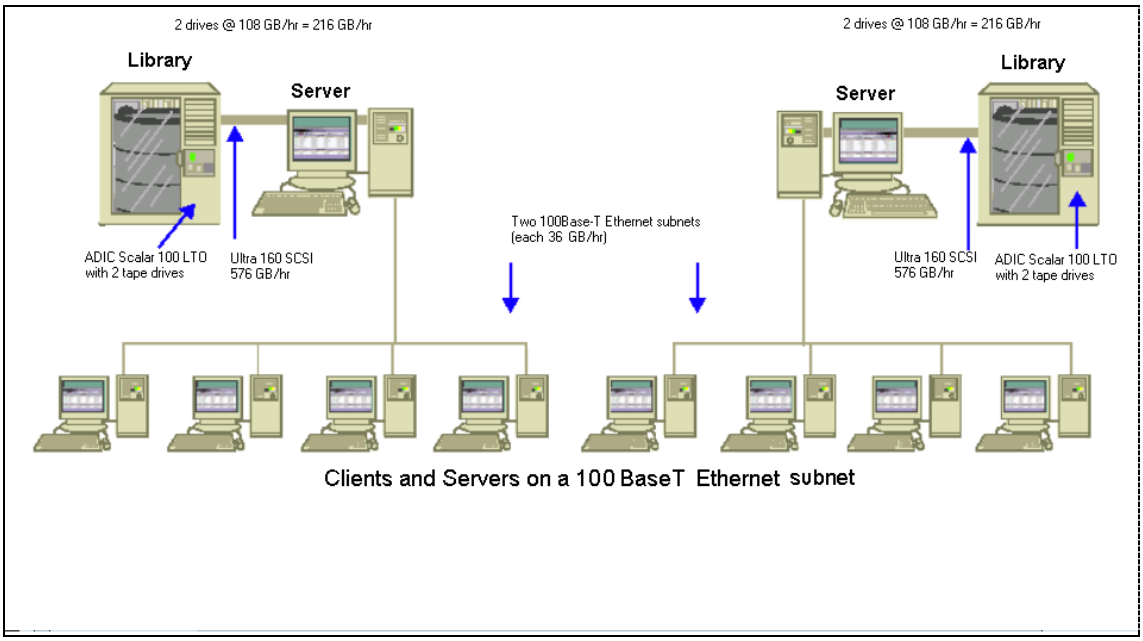
In this configuration, data cannot move across the network faster than 36 GB per hour, regardless of the number of servers and libraries available. To back up 1 Terabyte of data, the backup operation must run for 28 hrs.



Clients and Servers on a 100 BaseT Ethernet LAN

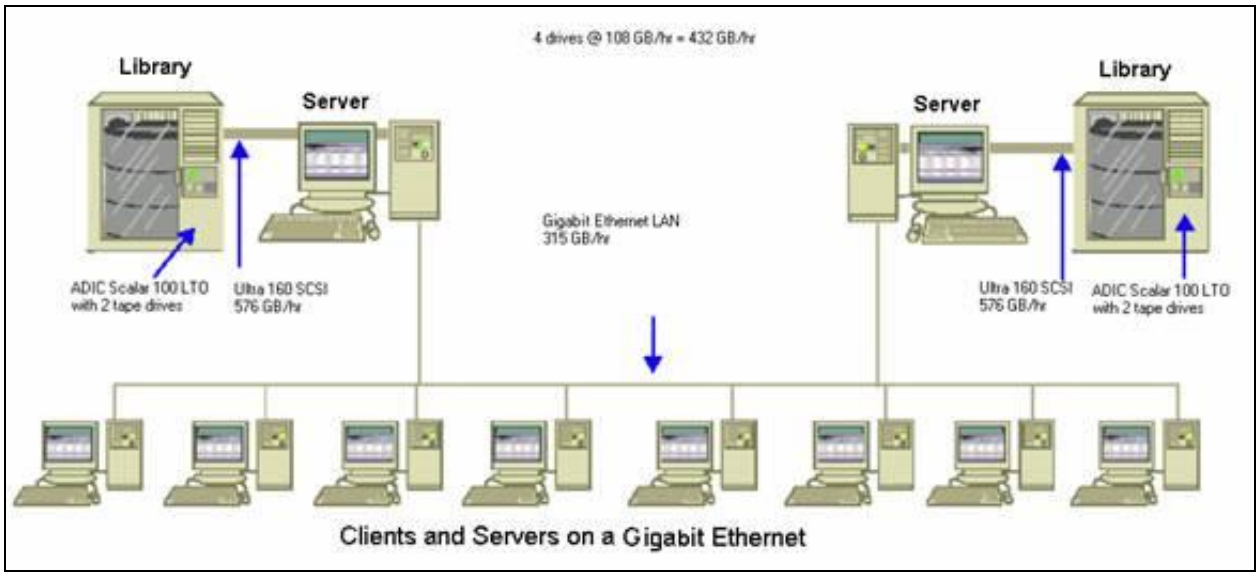
Transfer Rate for Clients and Servers on Two 100Base-T Ethernet Subnets

In this configuration, you can move twice as much data at the 36 GB per hour 100Base-T data rate. To back up 1 Terabyte of data, each subnet has to handle only 500 GB, so the operation takes 14 hours. Some performance is lost because the network cannot keep the media drives in each library streaming along at their combined 36 GB per hour optimum speed.



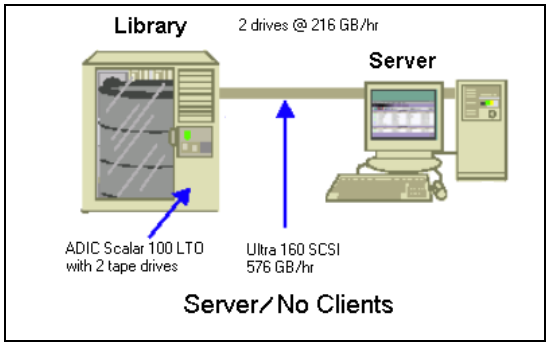
Transfer Rate for Clients and Servers on a Gigabit Ethernet Network

In this configuration, you move data at 315 GB per hour data ratio. To back up 1 Terabyte of data, the backup operation must run for 3 hours.



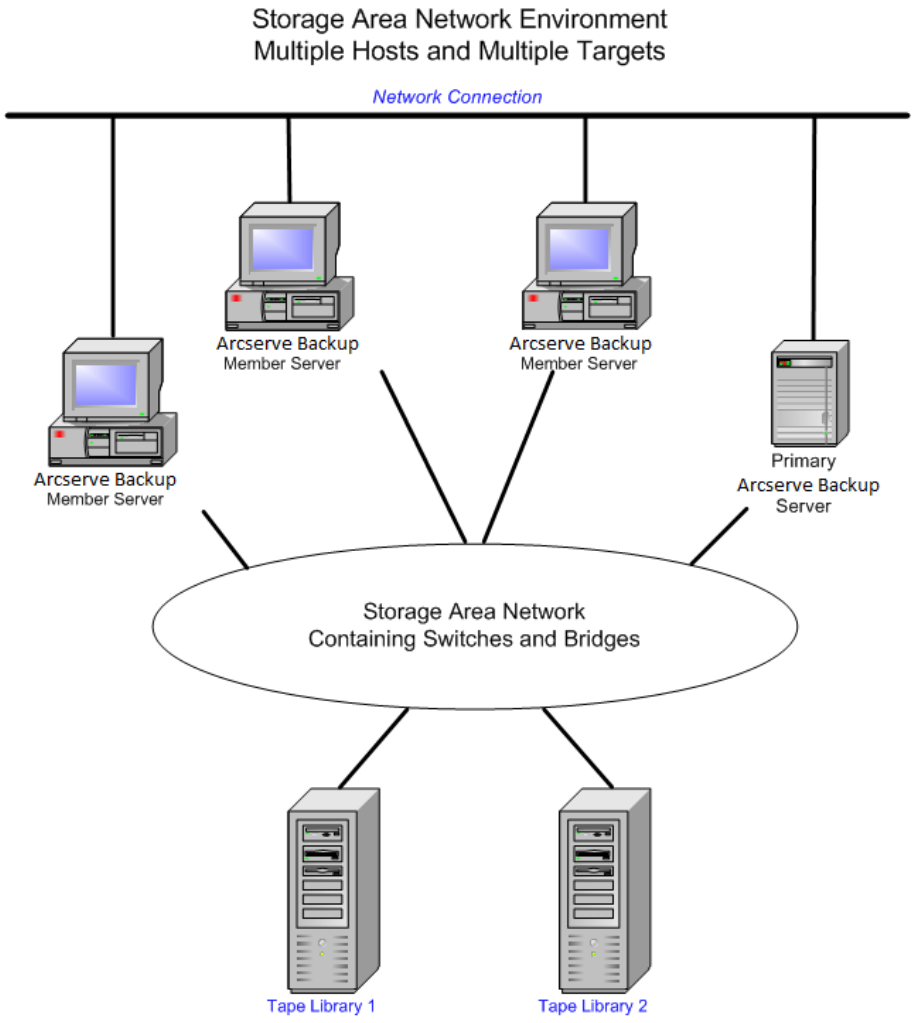
Transfer Rate for a Server With No Clients

In this case, the 216 GB per hour drives are the limiting factor, assuming that disk system or server is not the bottleneck. The system would take 5 hours to back up 1 Terabyte.



Transfer Rate For Server With SAN Option

In this configuration, local backups of each server on the SAN can achieve a data transfer rate of 432 GB per hour.



Storage Capacity for Two Sets of Recovery Data, One Full and One Incremental Backup

Assume the following:

- You have to do a full backup of 1 Terabyte of user data per week.
- You have to do daily incremental backups.
- About 10% of the data changes daily.
- The data from the last two backup cycles are available, online, for fast recovery.
- You are using LTO tape drives with 2:1 compression in a library with 20 slots.
- All media are used as efficiently as possible.

First, calculate the amount of capacity you need to store the output of the current backup operations. LTO media elements have a raw capacity of 200 GB with 2:1 compression. After you deduct 10% for overhead, the real capacity is close to 180 GB. The 1 Terabyte full backup thus requires:

1 Terabyte ÷ 180 GB / media element = 6 media elements

Using the above equation, you can also calculate the safety margin as follows:

(6 X 180 - 1000) / 1000 = 8%

Because six tapes (1 Terabyte) provide an 8% safety margin, you do not need to add extra tapes. In this example, you need only 6 LTO tapes to store a full backup. Based on the rate of change you estimated, the incremental backups amount to:

1 Terabyte × 10% changed / incremental × 5 incrementals = 500 GB changed

Therefore, at a minimum, you need the following:

500 GB ÷ 180 GB / media element = 3 media elements

Because three tapes (500 GB) provide a 9% safety margin, you do not need to add extra tapes. You need only three tapes to store a single set of incremental backup data.

Next, calculate the amount of storage space you need for your online recovery data. You need to retain the last two backup sets in the library, so you need 9 tapes for the oldest set of recovery data and 9 tapes for the newest set. To store your recovery data you need 18 tapes.

Therefore, your total storage requirement is as follows:

9 tapes for current backup + 18 tapes for recovery = 27 tapes

Next, you calculate the capacity of the library by deducting cleaning slots:

20 slots/library - 1 cleaning slot = 19 available slots

Therefore, you have a deficit of 27 - 19 = 8 slots and must do one of the following:

- Add a library.
- Compress the stored data.
- Store only one set of recovery data online.

Chapter 3: Planning Arcserve Backup Installations

This section contains the following topics:

Supported Platforms (see page 37)
Supported Devices (see page 37)
Amount of Disk Space Required to Install Arcserve Backup (see page 39)
Installation Methods (see page 40)
Types of Arcserve Backup Server Installations (see page 41)
caroot User Account (see page 45)
Database Requirements (see page 46)
Global Dashboard Considerations (see page 53)
Upgrade Considerations (see page 54)
Product License Requirements (see page 57)
Arcserve Backup File System Agents Release Levels (see page 58)
How the Installation Process Affects Operating Systems (see page 59)

Supported Platforms

The Arcserve Backup for Windows Server component lets you protect agents running on the following platforms:

- Windows
- UNIX
- Linux
- Mac OS X
- Mainframe Linux

For the most current list of supported operating systems, see the readme file or access the Arcserve website at www.arcserve.com.

Supported Devices

To ensure that your hardware devices are compatible and that Arcserve Backup can communicate with your system, you obtain the latest Certified Device List from the Arcserve website, www.arcserve.com.

Tape Library Installations

The Arcserve Backup base product includes support for single-drive tape libraries. If you are using a tape library with more than one drive, a separately installed Tape Library Option is required, and you must license it on each Arcserve Backup primary server or Arcserve Backup stand-alone server with an attached multiple drive library.

Arcserve Backup automatically configures single-drive libraries for you the first time the Tape Engine starts.

To perform Tape RAID operations in your environment, you must license the Tape Library Option. After you license the option, you can set up your Tape RAID devices by running Device Configuration on a primary server or member with locally attached Tape RAID devices. For more information, see the *Tape Library Option Guide*.

Storage Area Network (SAN) Installations

The Arcserve Backup base product includes support for Storage Area Network (SAN) operations.

If your SAN contains a primary server and one or more member servers that share a library, a separately installed Storage Area Network (SAN) Option is required. You must install the option and issue the license for the option on the primary server.

Amount of Disk Space Required to Install Arcserve Backup

You can install Arcserve Backup for Windows on Windows x64 and x86 operating systems. The amount of free disk space required varies based on the version of Windows that is installed on the backup server and the type of Arcserve Backup server that you install.

The information that follows describes the amount of free disk space required to install the Arcserve Backup for Windows base product, Arcserve Backup Client Agent for Windows, and Arcserve Backup Diagnostic Utility.

- Windows x64 Systems
  - Primary Server and Stand-alone Server--1 GB to 2.13 GB of free disk space.
  - Member Server--.71 GB (727 MB) to 1.97 GB of free disk space.
- Windows x86 Systems
  - Primary Server and Stand-alone Server--.77 GB (788 MB) to 1.34 GB of free disk space.
  - Member Server--.67 GB (690 MB) to .91 GB (932 MB) of free disk space.

Note: Add 1.4 GB to the above amounts if you wish to install Agent Deployment setup files on the backup server.

Installation Methods

You can install Arcserve Backup using the following methods:

- **Installation Wizard--**The installation wizard is an interactive application that lets you install Arcserve Backup on local and remote systems.

  The installation wizard lets you specify the following installation options:

  Installation or Upgrade Type

  Lets you install Arcserve Backup on local systems, remote systems, cluster environments, and create a response file that you can use to perform an unattended installation.

  When you perform remote installations, the installation wizard lets you install Arcserve Backup on one or more remote systems simultaneously. With remote installations, the target remote systems can consist of different Arcserve Backup server types, different Arcserve Backup agents and options, or both.

  Note: If you are upgrading from a previous release to an Arcserve Primary Server, you must select the Local Installation/Upgrade option. Arcserve Backup does not support upgrading from a previous release to an Arcserve Primary Server on a remote system.

  Arcserve Server Type

  Lets you specify the type of Arcserve server that you want to install. For more information, see Types of Arcserve Backup Server Installations (see page 41).

  Arcserve Backup Products

  Lets you specify the Arcserve Backup agents, options, and other components that you want to install on the target system.

  Arcserve Database

  Lets you specify and configure the application that you will use for the Arcserve Backup database. You can install Microsoft SQL Server 2008 Express Edition or Microsoft SQL Server.

  Microsoft SQL Server 2008 Express is a free database application that is packaged with Arcserve Backup. Microsoft SQL Server 2008 Express Edition must be installed on the Arcserve Backup server. For more information, see Microsoft SQL Server 2008 Express Edition Considerations (see page 46).

  Microsoft SQL Server is a highly scalable database application that can be installed on the Arcserve Backup server or on any other system in your environment. For more information see, Microsoft SQL Server Database Considerations (see page 48).

- **Silent Installation**--The silent installation process eliminates the need for user interaction and is facilitated by the use of a response file.

  Important! Arcserve Backup does not support upgrading from a previous release to an Arcserve Primary Server using a response file.

- **Unicenter Software Delivery**--Unicenter Software Delivery is a flexible tool for distributing, installing, verifying, updating, and uninstalling software from a central location.

  For information about silent installation and Unicenter Software Delivery installation, see Create a Silent Installation Response File (see page 101) and Install Arcserve Backup Using Unicenter Software Delivery (see page 120).

Types of Arcserve Backup Server Installations

Arcserve Backup supports the following types of installations:

Express

Lets you simplify the installation process by installing the Arcserve Backup products and components that you need to protect your backup environment. The Express installation eliminates some setup pages, allowing you to skip the Arcserve Database setting and install Microsoft SQL Express (default setting from Microsoft) as the database for Arcserve. An Express installation only applies to a local new installation. If the local machine already has Arcserve Backup products from a previous release, the Express option will not be available.

Note: An Express installation only supports non-cluster machines.

During an Express installation, the following products and components are installed by default, however you can de-select unnecessary components during the Installation Wizard:

Product/Component	Default Installation Location (x86)	Default Installation Location (x64)
Stand-alone Server	c:\program files\CA\ARCserve Backup	c:\program files (x86)\CA\ARCserve Backup
Manager (Console)	c:\program files\CA\ARCserve Backup	c:\program files (x86)\CA\ARCserve Backup
Tape Library Option	c:\program files\CA\ARCserve Backup	c:\program files (x86)\CA\ARCserve Backup
Enterprise Module	c:\program files\CA\ARCserve Backup	c:\program files (x86)\CA\ARCserve Backup
Global Dashboard	c:\program files\CA\ARCserve Backup\GlobalDashboard	c:\program files (x86)\CA\ARCserve Backup\GlobalDashboard
Disaster Recovery Option	c:\program files\CA\ARCserve Backup	c:\program files (x86)\CA\ARCserve Backup
Client Agent for Windows	c:\program files\CA\ARCserve Backup Client Agent for Windows	c:\program files\CA\ARCserve Backup Client Agent for Windows

Product/Component	Default Installation Location (x86)	Default Installation Location (x64)
Agent for Open Files for Windows, including the BAOF Server and BAOF Console	c:\program files\CA\ARCserve Backup Agent for Open Files	c:\program files (x86)\CA\ARCserve Backup Agent for Open Files
Agent Deployment Setup Files	c:\program files\CA\ARCserve Backup\Packages\AgentDeploy	c:\program files (x86)\CA\ARCserve Backup\Packages\AgentDeploy
Application Agents that setup detects in your environment (for example, Agent for Microsoft Exchange Server or Agent for Microsoft SQL Server)	c:\program files\CA\ARCserve Backup Agent for Microsoft Exchange c:\program files\CA\ARCserve Backup Agent for Microsoft SQL Server	c:\program files\CA\ARCserve Backup Agent for Microsoft Exchange c:\program files\CA\ARCserve Backup Agent for Microsoft SQL Server
Diagnostic Utility	c:\program files\CA\ARCserve Backup Diagnostic	c:\program files (x86)\CA\ARCserve Backup Diagnostic

Custom

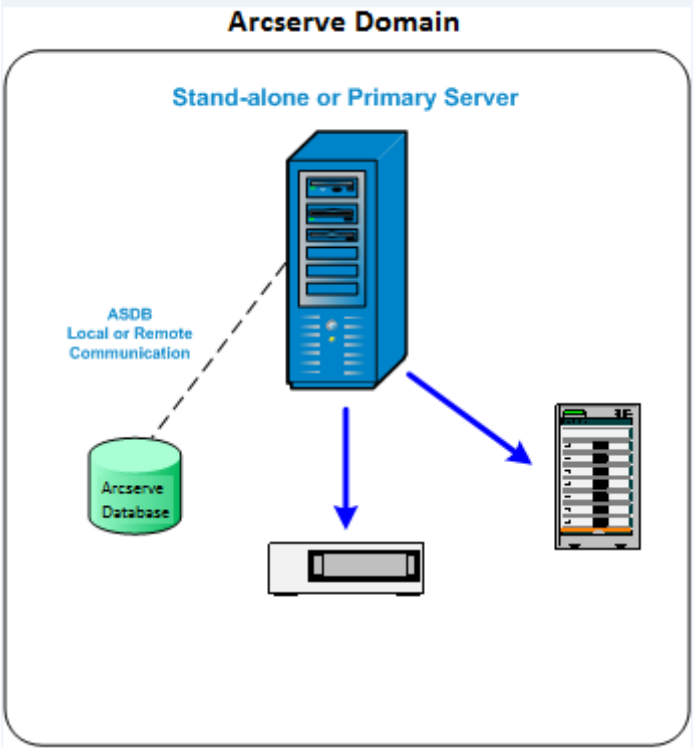
Lets you specify individual components, agents, and options that you want to install.

Arcserve Manager Console

Consists of a graphical user interface (GUI) that lets you manage operations that run on any Arcserve stand-alone, primary, and member server in your environment.

Arcserve Stand-alone Server

Consists of a single-server that lets you run, manage, and monitor jobs that run locally to the server.



Arcserve Primary Server

Consists of a single, centralized server in a Arcserve Backup domain that lets you submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

With a primary server, you can manage devices and licenses associated with member servers, create reports, alert notifications, and view Activity Log data for all servers in a domain.

You can attach storage devices, such as tape libraries, to primary servers. You can deploy the Arcserve Backup database on the primary server or on a remote system.

To enable centralized management capabilities, you must install and license the Central Management Option.

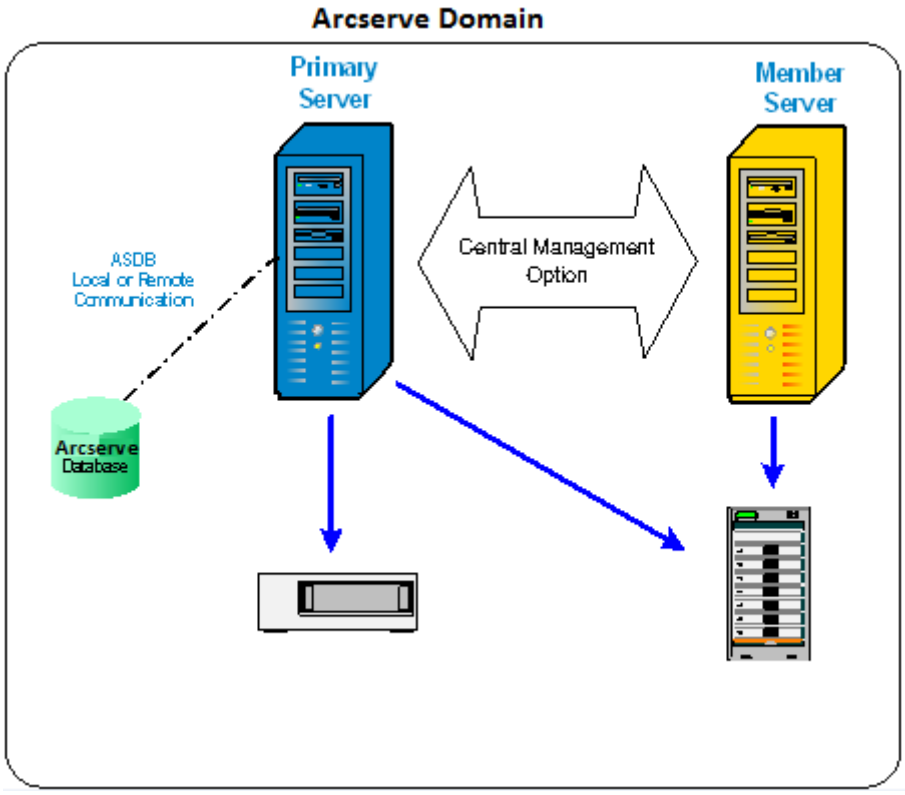
Note: For information about using primary servers to manage daily activities, see Central Management.

Arcserve Member Server

Consists of a server in a Arcserve Backup domain that receives instructions about jobs and devices from the primary server. Member servers send information about jobs in progress, job history, and Activity Log data to the primary server so that the information can be stored in the Arcserve Backup database.

You can attach storage devices, such as tape libraries, to member servers.

To enable centralized management capabilities, you must designate the server as a member server and then add it to the domain managed by the primary server.



Note: For information about using member servers to manage daily activities, see Central Management.

Other

This option lets you customize the installation of Arcserve Backup Servers, Agents, and Options.

Arcserve Backup Server Options

The following table describes the Arcserve Backup options that you can install on each type of Arcserve Backup server.

Option	Stand-alone Server	Primary Server	Member Server
Central Management Option		Available	
Tape Library Option	Available	Available	
Storage Area Network (SAN) Option		Available	
Enterprise Module	Available	Available	Available
Disaster Recovery Option	Available	Available	Available
Global Dashboard	Available	Available	Available
NDMP NAS Option	Available	Available	

Note: To install or uninstall Arcserve Backup server-based options after you install Arcserve Backup, use the Server Admin Manager to complete the task. For more information, see the *Administration Guide*.

caroot User Account

Arcserve Backup uses its own authentication mechanism for management purposes. It creates a default user named 'caroot' when you install Arcserve Backup. You can log in to the Arcserve Backup Manager Console using caroot.

The default caroot user account has root privileges for all Arcserve Backup functions. You can set a password for the caroot user profile during the configuration of the software, or after configuration using the User Profile Manager. You can also create additional user profiles using the User Profile Manager.

The caroot password can consist of any combination of alphanumeric and special characters, but may not exceed 15 bytes. A password totaling 15 bytes equates to approximately 7 to 15 characters.

Note: Arcserve Backup user names control access to only Arcserve Backup functions, and should not be confused with the operating system-required login name and password.

Database Requirements

To manage your storage environment, Arcserve Backup requires one of the following database applications:

- Microsoft SQL Server 2008 Express Edition (see page 46)
- Microsoft SQL Server (see page 48)

If you are upgrading to this release of Arcserve Backup, you can migrate data from a previous Arcserve database to Microsoft SQL Server Express Edition or Microsoft SQL Server.

Note: For a complete list of Arcserve products that you can upgrade from, see Supported Upgrades (see page 55).

Microsoft SQL Server 2008 Express Edition Considerations

Microsoft SQL Server 2008 Express Edition is a free, lightweight version of Microsoft SQL Server and is packaged with Arcserve Backup. Review the following information if you are considering using Microsoft SQL Server 2008 Express Edition to support the Arcserve Backup database:

- Ensure that the Arcserve system account has administrative privileges on Microsoft SQL Server 2008 Express Edition databases.
- Microsoft SQL Server 2008 Express Edition does not support remote operations. You must install the Arcserve database locally to your Arcserve Backup server.
- Microsoft does not recommend running Microsoft SQL Server 2008 Express Edition as a Local System account, a Local Service account, or Network Service account on Windows Server 2003 and Windows Server 2008 systems that function as domain controllers. When you install Arcserve Backup on a system that functions as a domain controller, Setup configures the Arcserve Backup database (ARCSERVE_DB) to communicate using a Local System account, and all other services to communicate using a Network Service account. To ensure that the Arcserve Backup database can communicate on Windows Server 2003 and Windows Server 2008 systems that function as a domain controller, you must change the Microsoft SQL Server 2008 Express Edition account to a Windows domain user account after you install Arcserve Backup.

  Note: For information about how to change the Microsoft SQL Server 2008 Express Edition account to a Windows domain user account, see the Microsoft SQL Server documentation.
- To function properly, Microsoft SQL Server 2008 Express Edition requires that .NET Framework 3.5 SP1 be installed on your system. Microsoft .NET Framework 3.5 SP1 is packaged with Arcserve Backup and is provided for you on the Arcserve Backup installation media.

- If you determine that Microsoft SQL Server 2008 Express Edition does not meet the needs of your Arcserve Backup environment, you can use the Server Configuration Wizard to convert the Arcserve Backup database to Microsoft SQL Server and then migrate your existing data to the new database after the conversion is complete. You can convert the database at any time after you install or upgrade Arcserve Backup.

  Note: For information about upgrading from Microsoft SQL Server 2008 Express Edition to Microsoft SQL Server, see the *Administration Guide*.

- Arcserve Backup does not support migrating data from a Microsoft SQL Server database to a Microsoft SQL Server 2008 Express database. Therefore, if you are currently running Microsoft SQL Server in your environment, you must deploy Microsoft SQL Server for the Arcserve Backup database.

- For Global Dashboard, you cannot configure the Arcserve Backup database for the Central Primary Server with Microsoft SQL Server Express installed. Microsoft SQL Server 2005, or later, must be installed on the Central Primary Server.

- You can download and install the latest updates, security patches, and service packs that apply to the version of Microsoft SQL Server 2008 Express Edition that is running in your environment. The Compatibility Matrix on the Arcserve support web site can help you determine the applicable updates for your implementation.

  Important! You should always check the Compatibility Matrix on the Arcserve support website before you apply Microsoft SQL Server 2008 Express Edition service packs to your Arcserve Backup implementation. After determining the compatible service packs, you should apply the updates and security patches based on the recommendations of Microsoft.

- Consider the following upgrade scenarios:

  - You are using Microsoft SQL Server 2005 Express Edition to host the Arcserve Backup database. The name of the Arcserve Backup database instance is ARCSERVE_DB (default). This scenario also includes situations where a previous release of Arcserve Backup may **not** be installed on the target system, however, Microsoft SQL Server 2005 Express Edition is installed on the target system and you are using an instance named ARCSERVE_DB for other applications.

  - You are using Microsoft SQL Server 2005 Express Edition to host the Arcserve Backup database. The name of the Arcserve Backup database instance is not ARCSERVE_DB.

  When you upgrade to this release, Setup searches for the default Arcserve Backup database instance. If Setup detects an instance named ARCSERVE_DB, Setup upgrades the instance to Microsoft SQL Server 2008 Express Edition, and Arcserve Backup continues using the instance, and data, from the previous release. However, if Setup cannot detect an instance named ARCSERVE_DB, Setup creates a new instance called ARCSERVE_DB. If Setup creates a new database instance, the information from the previous Arcserve Backup release is not retained in the new instance.

Microsoft SQL Server Database Considerations

Review the following information if you are considering using Microsoft SQL Server for the Arcserve Backup database:

- If you are upgrading to this release and currently running Microsoft SQL Server for the Arcserve Backup database, you must continue using Microsoft SQL Server for the Arcserve Backup database.
- Arcserve Backup does not support using Microsoft SQL Server 7.0 for the Arcserve Backup database.
- By default, Arcserve Backup creates the Arcserve Backup database (ASDB) using a simple recovery model. You should retain this model for proper operation.
- Microsoft SQL Server supports local and remote communication. This capability lets you configure the Arcserve Backup database to run locally or remotely to your Arcserve Backup server.

  Note: For more information, see Remote Database Considerations.
- By default, Arcserve Backup stores information about the backed up files and directories in the Catalog Database. This behavior causes the Catalog Database to grow in size at a faster rate than the Arcserve Backup database. Given this behavior and the needs of your organization, you should plan to have a sufficient amount of free disk space to support the growth of the Catalog Database.
- For Global Dashboard, the Central Primary Server, Arcserve Backup database (ASDB) must have Microsoft SQL Server 2005 or later installed (does not support Microsoft SQL Server 2008 Express Edition or Microsoft SQL Server 2000 as its database).

  Note: For a Branch Primary Server, no additional hardware or software is required beyond the minimum requirements for any Arcserve Backup primary server.
- To install Arcserve Backup with Microsoft SQL Server support, an administrative account such as the sa account, which has the right to create devices, is required for proper installation.

  You should use the *sa* account when prompted for the Arcserve Backup Database (SQL) System Account during installation of Arcserve Backup with Microsoft SQL support.
- Set the database security mode to SQL security in the SQL Enterprise Manager. This applies when using SQL security as the authentication mode and the systems that you want to back up reside inside or outside the Windows domain.
- If you specify Microsoft SQL Server 2000, Microsoft SQL Server 2005, Microsoft SQL Server 2008, or Microsoft SQL Server 2012 as the Arcserve Backup database during setup, you can use Windows authentication or SQL Server authentication to communicate with the Microsoft SQL database.
- If the Microsoft SQL Server account is changed, you must make the corresponding changes using the Server Configuration Wizard.

- The Arcserve Backup Database Engine periodically polls the status of the Microsoft SQL Server database. If Microsoft SQL Server does not respond in a timely fashion, the Database Engine assumes that the Microsoft SQL Server is unavailable and shuts down (red light). To avoid this situation, you can set the registry key to an appropriately longer value to increase the wait time for Arcserve Backup Database Engine, as follows:

  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Arcserve Backup\Base\Database\MSSQL\SQLLoginTimeout

- Arcserve Backup does not support local Microsoft SQL Server installations on Arcserve Backup servers in NEC CLUSTERPRO environments. In NEC CLUSTERPRO environments, you must install the Arcserve Backup database instance on a remote system.
- If the ODBC driver is configurable, the System Data Source "ASNT" under System DSN, in the ODBC Data Source Administrator should have the Client Configuration set to utilize TCP/IP communication.

Remote Database Considerations

Using a remote database provides a simple and transparent method of sharing a single database as if the database resides locally. When you use this configuration, you do not need a database on the local machine because all information is saved to the remote database. This configuration is best under the following conditions:

- There is not enough space locally for the database.
- There is no organizational requirement and you want to take advantage of the ease of management that comes with having a single location for the database.
- You require a separate server that is not a Arcserve Backup server to function as a dedicated as a Microsoft SQL Server machine.
- To protect SQL Server instances in a cluster-aware environment, you must manually install the Agent for Microsoft SQL Server on all of the cluster nodes.

  Note: For information about backing up and restoring Microsoft SQL Server Databases, see the *Agent for Microsoft SQL Server Guide*.

- Use the Server Configuration Wizard to configure ODBC communication between a remote Arcserve database and the Arcserve primary or stand-alone server. This wizard lets you configure efficient communication between servers, especially when you have more than one Arcserve Backup server in your environment.
- To ensure that Arcserve Backup can communicate with the system that is hosting the Arcserve database instance, you should enable TCP/IP communication between the SQL Server database instance and the Arcserve server.

  Note: For more information, see How to Enable TCP/IP Communication on Microsoft SQL Server Databases (see page 50).

Important! Microsoft SQL Server 2008 Express Edition does not support remote database communication.

Note: For information about configuring devices and modifying the database protection job, see the *Administration Guide*.

How to Enable TCP/IP Communication on Microsoft SQL Server Databases

If you are hosting the Arcserve database instance using Microsoft SQL Server 2000 or later and the Arcserve Backup database will reside on a remote system, the installation wizard may not be able to communicate with the database on the remote system.

To help ensure that the installation wizard can communicate with the remote system, you should enable TCP/IP communication between the Arcserve Backup server and the server that will host the Arcserve Backup database before you install Arcserve Backup.

- Microsoft SQL Server 2000--To enable TCP/IP communication on Microsoft SQL Server 2000 systems, run the SQL Server Network utility and ensure that TCP/IP appears in the Enabled Protocols. If TCP/IP does not appear in the Enabled Protocols list, add TCP/IP to the list and click OK. To apply TCP/IP communication, restart all Microsoft SQL Server services.
- Microsoft SQL Server 2005 and later--To enable TCP/IP communication on Microsoft SQL Server 2005 and later systems, run the SQL Server Configuration Manager and enable TCP/IP communication for the SQL Server instance. To apply TCP/IP communication, restart all Microsoft SQL Server services.

  Note: For Microsoft SQL Server 2008, you must use the SQL Server Native Client 10.0 driver.

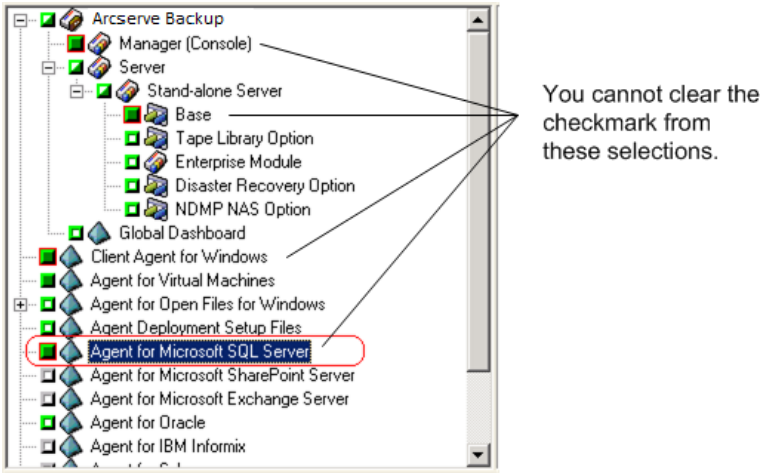
Agent for Arcserve Database

The Arcserve Backup Agent for Arcserve Database is a form of the Arcserve Backup Agent for Microsoft SQL Server. The agent is either installed automatically when you install Arcserve Backup, or manually using a special utility, either after the location of the Arcserve Backup database is changed, or on multiple nodes of a cluster.

This utility, named SQLAgentRmtInst.exe, is placed in the Packages sub-folder of the Arcserve Backup home directory, in a folder named ASDBSQLAgent, when you install Arcserve Backup. If you need to install the agent on a computer that is not a Arcserve Backup server, you must copy the ASDBSQLAgent folder to the system where you are installing the agent, and run the SQLAgentRmtInst.exe utility on that machine.

By itself, the Agent for Arcserve Database allows you to back up and restore the Arcserve Backup database, and the system databases and Disaster Recovery Elements from the Microsoft SQL Server instance that contains the Arcserve Backup database. When installed with the Agent for Microsoft SQL Server, it allows the Agent for Microsoft SQL Server to recognize the presence of a Arcserve Backup database, and to work with Arcserve Backup to provide the special recovery mechanisms that are available for the Arcserve Backup database.

When upgrading from a previous release of Arcserve Backup, you must upgrade the Agent for Arcserve Database. This behavior is designed to help ensure that the current version of the Arcserve Backup database is protected by the current version of the agent. As a result, you cannot clear the check box next to Agent for Microsoft SQL Server in the product selection tree on the Components dialog.



Because the Agent for Arcserve Database is a form of the Agent for Microsoft SQL Server, it will appear as the Arcserve Backup Agent for Microsoft SQL Server in the system's installed programs list. If both are present, only a single entry will appear. If you need to uninstall one or the other, the installation sequence will prompt you to select which variant to remove.

You can use the stand-alone utility that installs the Agent for Arcserve Database in any of the following situations:

- When the Arcserve Backup database is moved
- To re-install the agent if it is accidentally uninstalled
- To install the agent to additional nodes of a cluster
- To install the agent on a remote computer, if the Arcserve Backup installer is unable to do so directly

Installation Progress Logs

After you install Arcserve Backup and any agents and options, Arcserve Backup creates installation progress logs that you can refer to in the event that an interactive, silent, or unattended installation fails. Installation progress logs can be useful to Arcserve Customer Support personnel if you need to contact us about an installation problem.

- **Interactive installations--**If installation of the Arcserve Backup base product or any agent or option fails, you access the installation progress log from the Install Summary dialog. To open the installation progress log, double-click the error icon next to the application on the Install Summary dialog.
- **Silent and unattended installations--**You can access the installation progress logs from the following directory:

  <system drive>:\WINDOWS\Temp\CA_*.tmp

  For each installation session, Arcserve Backup creates a unique CA_*.tmp directory (where * represents a random number). Within this directory you will find a directory labeled *MACHINENAME* and a text file labeled ProdWiz.log. *MACHINENAME* is the machine name of the computer where you installed Arcserve Backup.

  - ProdWiz.log—Master Setup log.
  - *MACHINENAME* directory—Includes log files created when you installed Arcserve Backup and any agents and options.

    For example, ARCSERVE.log is the log file created when you installed the Arcserve Backup base product. If you installed the Tape Library Option, you can access the installation progress log labeled OPTTLO.LOG, in the *MACHINENAME* directory.

Global Dashboard Considerations

The Arcserve Backup base product includes support for Global Dashboard operations.

Configuration of Global Dashboard can be performed during or after installation of Arcserve Backup. However, before you configure Global Dashboard, consider the following:

- Which server within your Global Dashboard environment will be configured as the Central Primary Server?

  There can only be one Central Primary Server in a Global Dashboard environment.

  - When selecting the Central Primary Server, the main consideration should be database size. Ensure the selected Central Primary Server is capable of storing dashboard data received from all registered Branch Primary Servers.
  - Server performance should also be considered when selecting the Central Primary Server to help ensure fast, efficient, and reliable data interface between the Central Primary Server and all associated Branch Primary Servers.
  - Database type should also be considered when selecting the Central Primary Server.

    For Global Dashboard, the Central Primary Server only supports Microsoft SQL Server 2005/2008/2008 R2/2012. It does not support Microsoft SQL Server 2005/2008/ Express and Microsoft SQL Server 2000.

- Which servers within your Global Dashboard environment will be configured as Branch Primary Servers?

  At each server location, the Branch Primary Server must be a primary/stand-alone server within the Arcserve Backup domain (not a domain member server).

- During the configuration process, the Arcserve Backup database engine will be shut down for a few minutes. Plan your installation at a convenient and non-intrusive time when there are no Arcserve Backup jobs scheduled.

- In a Global Dashboard domain, if you are demoting a Branch Primary Server to a member server or changing which primary server will be configured as the Central Primary Server, you may want to continue to use the collected information from the old primary server. Global Dashboard lets you export (and save) this information from the old primary server and import it into the new primary server.

License Requirements:

- To enable Global Dashboard capabilities, you must have a valid Arcserve Backup Global Dashboard license at the Central Primary Server, with multiple license counts to include all registered Branch Primary Servers. (Branch Primary Servers do not need to install a Global Dashboard license).
- Each registered Branch Primary Server will then occupy one count of the Global Dashboard license. If the registered branch count exceeds the maximum limit of the license, new branch sites will not be allowed to register to that Central Primary Server.
- A license status check will then be performed for each of the following scenarios
  - When registering a branch site
  - When re-registering a branch site
  - When performing full data synchronization
  - When performing incremental synchronization
- If the license status check fails, you will need to obtain additional licenses or re-allocate your existing licenses, to enable data synchronization to the Central Primary Server. (The status of each branch site license is displayed on the Central Manager dialog).
- **Note:** Deleting a branch server from the Central Manager will release the license count occupied by that branch and allow you to re-assign that license count to a different branch server.

Upgrade Considerations

The following sections include information you should review before upgrading Arcserve Backup.

This section contains the following topics:

Supported Upgrades (see page 55)
Backward Compatibility (see page 56)
Global Dashboard Upgrades (see page 56)
Data Migration from a Previous Release (see page 57)

Supported Upgrades

If you are currently using one of the following releases of Arcserve Backup, you can upgrade to this release from the following products:

- Arcserve Backup r16 for Windows--Includes the General Availability (GA) release and all of the latest service packs.
- Arcserve Backup r15 for Windows--Includes the General Availability (GA) release and all of the latest service packs.
- Arcserve Backup r12.5 for Windows--Includes the General Availability (GA) release and all of the latest service packs.

Important! If you want to upgrade from <bab> v9, BrightStor Enterprise Backup v10.5, <bab> r11.1, <bab> r11.5, or Arcserve Backup r12 you must uninstall the previous release and then install this release of Arcserve Backup. However, if you wish to retain the database information from your previous implementation, you must upgrade the previous implementation to Arcserve Backup r12.5 GA release (with no SP), and then upgrade from Arcserve Backup r12.5 to this release. To obtain Arcserve Backup r12.5 installation media, contact Arcserve Support. For all other previous releases of <bab> or BrightStor Enterprise Backup earlier than v9, you must uninstall the previous release before you install this release.

Backward Compatibility

This release of the Arcserve Backup server component supports the following backward compatibilities:

- **Agents--**Using the Arcserve Backup r16 server component you can manage agents from the releases that follow:
  - Arcserve Backup r16--includes the General Availability (GA) release and the latest service packs.
  - Arcserve Backup r15--includes the General Availability (GA) release and the latest service packs.
  - Arcserve Backup r12.5--includes the General Availability (GA) release and the latest service packs.

  Be aware of the following:
  - When backing up agent computers, the version of the Arcserve Backup server component must be equal to or greater than the release of the agent you want to back up. You cannot use agents from this release of Arcserve Backup with any previous release of the Arcserve Backup server component.
  - For optimal performance, you should upgrade all Arcserve Backup agents and options installed in your backup environment to this release.
  - All Arcserve Backup products installed on a computer must be the same release.

    Example: The Arcserve Backup server component, the Agent for Microsoft SQL Server, and the Agent for Virtual Machines are installed on a computer. When you upgrade the Arcserve Backup server component to this release, you must also upgrade Agent for Microsoft SQL Server and the Agent for Virtual Machines to this release.
- **Arcserve Backup Domains--**All Arcserve Backup servers in a domain must be running the same version of the Arcserve Backup Server component. Arcserve Backup servers with different versions of the Arcserve Backup server component must reside in different Arcserve Backup domains.
- **Job Scripts--**You can restore data from backup tapes and load job scripts created using all previous versions BrightStor Arcserve Backup and BrightStor Enterprise Backup.

Global Dashboard Upgrades

When upgrading from a previous release of Global Dashboard, and the configuration consists of a central primary server and at least one registered branch primary server, the best practice is to upgrade the central primary server before you upgrade the branch primary servers.

Data Migration from a Previous Release

When you upgrade Arcserve Backup from a previous release, you can retain most of your current settings and migrate the information stored in the previous Arcserve Backup database to the new Arcserve Backup database.

After the upgrade is complete, Arcserve Backup migrates the following types of data to the new Arcserve Backup database:

- **Authentication**--The upgrade process migrates all Arcserve Backup System Account data from the previous database to the new database, such as user names, passwords, and so on.

  Note: For upgrades to member servers, Arcserve Backup does not migrate user accounts and passwords if they already exist in the domain that the member server joins.

- **Jobs**--The upgrade process migrates all job scripts, such as rotation jobs, GFS rotations, and custom jobs from the previous database to the new database.

  Note: The upgrade process does not migrate Database pruning job settings from your previous installation. For information about specifying Database pruning job settings, see the *Administration Guide*.

- **Core database data**--The upgrade process migrates all core data from the previous database to the new database. Core data can consist of information about jobs, media, sessions, devices, media pools, file path names, file names, and so on.

- **Log data**--The upgrade process migrates Activity Log data from the previous database to the new database.

- **Session data**--The upgrade process lets you migrate the session data from the previous database to the new database.

  Note: The process of migrating session data can take a lot of time. However, you can perform file-level and session-level restores immediately after the upgrade and migration process is complete.

- **Catalog data**--The upgrade process lets you migrate the catalog database data from the previous database to the new database.

  Note: The process of migrating catalog data can take a lot of time. A progress dialog does not display.

Product License Requirements

Arcserve Backup requires you to license your product to receive authorized and uninterrupted access to the components, options, and agents. If you do not license Arcserve Backup, it stops working 31 days after you begin using it.

There are different methods for entering license information, depending on how you purchased Arcserve Backup. You can easily determine the method you must use based on where your licensing information is located. You can find licensing information in one of the following locations:

- Inside the product installation media sleeve
- On a certificate received from the Arcserve License Program
- On an ALP Key Certificate

The method you use to enter your licensing information differs depending on where your licensing information is located. If your licensing information is on the product DVD sleeve or certificate from the Arcserve License Program, you must use one method. If your license information is on an ALP Key Certificate, you must use another method. The following sections include information about each method.

ALP Key Certificate

If you receive an ALP Key Certificate, your licensing information is an Execution Key found in the certificate that must be placed in the ca.olf file on each of the machines that are running your Arcserve software. To simplify the process, you can obtain your current ca.olf file by going to www.arcserve.com and downloading the license file. Otherwise, you must manually edit your ca.olf files. For more information, see your ALP Key Certificate.

To use Arcserve Backup client agents, you need to enter the licenses for these agents into the ca.olf file on the backup server you use to protect remote servers. The backup server checks to make sure client agents are licensed.

Arcserve Backup File System Agents Release Levels

File system agents let you protect the files that reside on computers running various operating systems.

The table that follows identifies the file system agents that are packaged with this release of Arcserve Backup, and the release level of each agent:

File System Agent	Release Level
Arcserve Backup Client Agent for UNIX	r16.5
Arcserve Backup Client Agent for Linux	r16.5
Arcserve Backup Client Agent for Mainframe Linux OS/390	r16.5
Arcserve Backup Client Agent for Windows	r16.5

File System Agent	Release Level
Arcserve Backup Client Agent for Mac OS X (Supported on Windows Only)	r16.5
Arcserve Backup Agent for Oracle (UNIX)	r16.5
Arcserve Backup Agent for Oracle (Linux)	r16.5
Arcserve Backup Agent for Oracle (Windows)	r16.5
Arcserve Backup Enterprise Option for SAP R/3 for Oracle for Linux	r16.5
Arcserve Backup Enterprise Option for SAP R/3 for Oracle for UNIX	r16.5
Arcserve Backup Enterprise Option for SAP R/3 for Oracle for Windows	r16.5
BrightStor Arcserve Backup Client Agent for OpenVMS (Supported on Windows Only)	r11.5 SP3
BrightStor Arcserve Backup Enterprise Option for AS400	r11.5 SP3

How the Installation Process Affects Operating Systems

The Arcserve Backup installation process updates various Windows operating system components using an installation engine called the Microsoft Installer Package (MSI). The components included in the MSI let Arcserve Backup perform custom actions that let you install, upgrade, and uninstall Arcserve Backup. The following table describes the custom actions and the affected components.

Note: All Arcserve Backup MSI packages call the components listed in this table when you install and uninstall Arcserve Backup.

Component	Description
CallAllowInstall	Lets the installation process check for conditions relating to the current Arcserve Backup installation.
CallPreInstall	Lets the installation process read and write MSI properties. For example, read the Arcserve Backup installation path from the MSI.
CallPostInstall	Lets the installation process perform various tasks relating to installation. For example, registering Arcserve Backup into the Windows Registry.

Component	Description
CallAllowUninstall	Lets the uninstallation process check for conditions relating the current Arcserve Backup installation.
CallPreUninstall	Lets the uninstallation process perform various tasks relating to uninstallation. For example, un-registering Arcserve Backup from the Windows Registry.

Directories Updated

The installation process installs and updates Arcserve Backup files in the following directories by default:

Arcserve Backup (base product)

- C:\Program Files\CA\ARCserve Backup (x86 operating systems)
- C:\Program Files (x86)\CA\ARCserve Backup (x64 operating systems)
- C:\Program Files\CA\SharedComponents\ARCserve Backup
- C:\Program Files\CA\SharedComponents\ScanEngine
- C:\Program Files\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CA_LIC

Client Agent for Windows

- C:\Program Files\CA\ARCserve Backup Client Agent for Windows
- C:\Program Files\CA\SharedComponents\ARCserve Backup
- C:\Program Files\CA\SharedComponents\ScanEngine
- C:\Program Files\CA\SharedComponents\CAPKI

Client Agent for Windows for x64-Based Systems

- C:\Program Files (x86)\CA\ARCserve Backup Agent for Open Files
- C:\Program Files\CA\SharedComponents\CAPKI
- C:\Program Files (x86)\CA\SharedComponents\CAPKI
- C:\Program Files (x86)\CA\SharedComponents\ARCserve Backup
- C:\Program Files (x86)\CA\SharedComponents\ScanEngine

Agent for Virtual Machines

- C:\Program Files\CA\ARCserve Backup Client Agent for Windows
- C:\Program Files (x86)\CA\SharedComponents\ARCserve Backup

Agent for Virtual Machines for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Client Agent for Windows
- C:\Program Files (x86)\CA\SharedComponents\ARCserve Backup

Agent for Open Files for Windows

- C:\Program Files\CA\ARCserve Backup Agent for Open Files\
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Open Files for Windows for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Agent for Open Files\
- C:\Program Files\CA\SharedComponents\CAPKI
- C:\Program Files (x86)\CA\SharedComponents\CAPKI

Agent Deployment Setup Files

- C:\Program Files\CA\ARCserve Backup\

Agent for Microsoft SQL Server

- C:\Program Files\CA\ARCserve Backup Agent for Microsoft SQL Server\
- C:\Program Files \CA\SharedComponents\ARCserve Backup
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Microsoft SQL Server for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Agent for Microsoft SQL Server\
- C:\Program Files \CA\SharedComponents\ARCserve Backup
- C:\Program Files (x86)\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Microsoft SharePoint Server

- C:\Program Files\CA\ARCserve Backup Agent for Microsoft SharePoint Server
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Microsoft SharePoint Server for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Agent for Microsoft SharePoint Server
- C:\Program Files (x86)\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Microsoft Exchange Server

- C:\Program Files\CA\ARCserve Backup Agent for Microsoft Exchange Server
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Microsoft Exchange Server for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Agent for Microsoft Exchange Server
- C:\Program Files (x86)\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Oracle

- C:\Program Files\CA\ARCserve Backup Agent for Oracle\
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Oracle for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Agent for Oracle\
- C:\Program Files (x86)\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Lotus Domino

- C:\Program Files\CA\ARCserve Backup Agent for Lotus Domino\
- C:\Program Files\CA\SharedComponents\CAPKI

Agent for Sybase

- C:\Program Files\CA\ARCserve Backup Agent for Sybase
- C:\Program Files\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CA_LIC

Agent for IBM Informix

- C:\Program Files\CA\C:\Program Files\CA\CA ARCserve Backup Agent for Informix
- C:\Program Files\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CA_LIC

Diagnostic Utility

- C:\Program Files\CA\ARCserve Backup Diagnostic\
- C:\Program Files\CA\SharedComponents\CAPKI

Enterprise Option for SAP R/3 for Oracle

- C:\Program Files\CA\ARCserve Backup Enterprise Option for SAP R3 for Oracle\
- C:\Program Files\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CA_LIC

Enterprise Option for SAP R/3 for Oracle for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Enterprise Option for SAP R3 for Oracle\
- C:\Program Files (x86)\CA\SharedComponents\CAPKI
- C:\Program Files\CA\SharedComponents\CAPKI
- C:\Program Files (x86)\CA\SharedComponents\CA_LIC

Arcserve Backup installs the following Arcserve Backup products in the same directory folder as the Arcserve Backup base product:

- Enterprise Module
- Disaster Recovery Option
- NDMP NAS Option
- Microsoft Windows EBS Option

You can install Arcserve Backup into the default installation directory or install Arcserve Backup into an alternate directory. The installation process copies various system files to the following directory:

C:\Windows\system

Arcserve Backup copies configuration files to the following directory:

C:\Documents and Settings\<user name>

Note: To view a list of Arcserve Backup unsigned files, see Unsigned Arcserve Backup Files (see page 65).

Windows Registry Keys Updated

The installation process updates the following Windows registry keys:

- Default registry keys:

  HKLM\SOFTWARE\Computer Associates

- The installation process creates new registry keys and modifies various other registry keys, based on your system's current configuration.

Applications Installed

The installation process installs the following applications into your computer:

- Arcserve Licensing
- Arcserve CAPKI (encryption)
- Microsoft Visual C++ 2005 SP1 Redistributable
- Scan Engine 8.1 (eTrust Antivirus)
- If you are installing Arcserve Backup server, the installation process also installs these applications:
  - Microsoft .NET Framework 3.5 SP1
  - Java Runtime Environment (JRE) 1.7.0.
  - Microsoft XML 6.0
- If you are installing Microsoft SQL Express Edition as the Arcserve Backup database, the following applications are also installed:
  - Microsoft SQL Server 2008 Express Edition SP3
  - Microsoft Windows Installer 4.5 Redistributable
- If you are installing the Arcserve Backup Agent for Oracle (x86/x64) or Enterprise Option for SAP R/3 for Oracle (x86/x64), the following applications are also installed:
  - Microsoft XML 6.0
  - Java Runtime Environment (JRE) 1.7.0.

Data Mover Servers, Oracle Agents, and SAP Agents

The installation process installs the following applications into your computer when you are installing UNIX and Linux Data Mover on a UNIX and Linux server, Agent for Oracle (UNIX and Linux), and Agent for SAP R3 for Oracle (UNIX and Linux):

- For Sun, HPUX, and Linux operating systems, Arcserve Backup installs Java Runtime Environment (JRE) into the following directory on your computer:

  /opt/CA/SharedComponents/jre

- For AIX operating systems, Arcserve Backup installs IBM Java Runtime Environment (IBM JRE) and Sun into the following directories on your computer:

  /opt/CA/SharedComponents/jre
  /opt/CA/SharedComponents/jre.sun

The following table describes the version of JRE that will be installed on your operating system:

JRE 1.6.0	JRE 1.7.0
RHEL 4.x through RHEL 5.5	RHEL 5.5 and later
SLES 9.x through SLES 10 SP2	SLES 10 SP2 and later
Solaris 9 SPARC	Solaris 10 and later

Note: Computers running the AIX and HP-UX operating systems will retain JRE 1.6.0.

Unsigned Binary Files

Arcserve Backup installs binary files developed third parties and Arcserve Backup that are not signed. The following table describes the binary files.

Binary Name	Source
ansiatl.dll	Microsoft
ATL80.dll	Microsoft
CALicense.msi	CA License
Cazipxp.exe	CA License
ccme_base.dll	EMC (RSA)
ccme_ecc.dll	EMC (RSA)
ccme_eccaccel.dll	EMC (RSA)
ccme_eccnistaccel.dll	EMC (RSA)
cdcdrom.sys	Microsoft
cdrom.sys	Microsoft
CFX2032.DLL	ChartFX
COMPRESS.EXE	Microsoft
cryptocme2.dll	EMC (RSA)

Binary Name	Source
dbghelp.dll	Microsoft
GX1142R.dll	Classworks
icudt34.dll	IBM
icuin34.dll	IBM
icuio34.dll	IBM
icule34.dll	IBM
iculx34.dll	IBM
icutest.dll	IBM
icutu34.dll	IBM
icuuc34.dll	IBM
libeay32.dll	OpenSSL
libetpki_openssl_crypto.dll	EMC (RSA)
LogSet_rwtest13-vm22_20121025_163425.cab	Microsoft
mfc80.dll	Microsoft
mfc80CHS.dll	Microsoft
mfc80CHT.dll	Microsoft
mfc80DEU.dll	Microsoft
mfc80ENU.dll	Microsoft
mfc80ESP.dll	Microsoft
mfc80FRA.dll	Microsoft
mfc80ITA.dll	Microsoft
mfc80JPN.dll	Microsoft
mfc80KOR.dll	Microsoft
mfc80u.dll	Microsoft
mfcm80.dll	Microsoft
mfcm80u.dll	Microsoft
msdia80.dll	Microsoft
msi.dll	Microsoft
msstkprp.dll	Microsoft

Binary Name	Source
msvcm80.dll	Microsoft
msvcp80.dll	Microsoft
msvcr71.dll	Microsoft
msvcr80.dll	Microsoft
Msvcrt40.dll	Microsoft
roboex32.dll	Blue Sky Software Corporation
sqlite3.dll	SQLite software
ssleay32.dll	Arcserve Backup
System.EnterpriseServices.Wrapper.dll	Microsoft
tpcdrom.sys	Microsoft
txf_wrapper.dll	Arcserve RHA
unzip.exe	Info-ZIP
vcomp.dll	Microsoft
Vim25Service2005.dll	Arcserve Backup
Vim25Service2005.XmlSerializers.dll	Vmware
VimService2005.dll	Arcserve Backup
VimService2005.XmlSerializers.dll	Vmware
xalan_messages_1_10.dll	Apache Software Foundation
xalan-c_1_10.dll	Apache Software Foundation
xerces-c_2_7.dll	Apache Software Foundation
xsec_1_2_0.dll	Apache Software Foundation
zlib1.dll	Zlib Compression Library

Binary Files Containing Incorrect File Version Information

Arcserve Backup installs binary files developed by third parties, other Arcserve products, and Arcserve Backup that contain incorrect file version information. The following table describes the binary files.

Binary Name	Source
ABFuncWrapperTypeLib.dll	Arcserve Backup

Binary Name	Source
casmgmtsvc.exe	Tanuki Software
Cazipxp.exe	CA License
cryptocme2.dll	EMC (RSA)
decora-d3d.dll	Java Runtime Environment
decora-sse.dll	Java Runtime Environment
fxplugins.dll	Java Runtime Environment
glass.dll	Java Runtime Environment
glib-lite.dll	Java Runtime Environment
gstreamer-lite.dll	Java Runtime Environment
gvmomi.dll	Vmware
icutest.dll	IBM
icutu34.dll	IBM
inocboot.exe	CA AVEngine
javafx-font.dll	Java Runtime Environment
javafx-iio.dll	Java Runtime Environment
jfxmedia.dll	Java Runtime Environment
jfxwebkit.dll	Java Runtime Environment
libcurl.dll	Vmware
libeay32.dll	OpenSSL
libetpki_openssl_crypto.dll	EMC (RSA)
liblber.dll	Vmware
libldap.dll	Vmware
libldap_r.dll	Vmware
libxml2.dll	Java Runtime Environment
libxslt.dll	Java Runtime Environment
MSClusterLib.dll	Microsoft
mxvfdwyr.dll	Microsoft
prism-d3d.dll	Java Runtime Environment
sqlite3.dll	SQLite software
TroubleTicketUtil.exe	CA Alert

Binary Name	Source
unzip.exe	Info-ZIP
Vim25Service2005.dll	Arcserve Backup
Vim25Service2005.XmlSerializers.dll	Vmware
VimService2005.dll	Arcserve Backup
VimService2005.XmlSerializers.dll	Vmware
WindowsServer2003-KB942288-v4-x86.exe	Microsoft
WindowsXP-KB942288-v3-x86.exe	Microsoft
wrapper.dll	Tanuki Software
xalan_messages_1_10.dll	Apache Software Foundation
zlib1.dll	Zlib Compression Library

Binary Files that do not Comply with Windows Security Requirements

Arcserve Backup installs binary files developed by third parties, other Arcserve products, and Arcserve Backup that do not comply with Windows security requirements. The following table describes the binary files.

Binary Name	Source
Acslsrdc.dll	Arcserve Backup
AGUIEXC.dll	Arcserve Backup
Albuild.dll	CA Alert
AlertPackage.exe	CA Alert
AMS_Plugin.dll	CA ScanEngine
AMS_Update.dll	CA ScanEngine
arclib.dll	CA ScanEngine
ARCserve.dll	Arcserve Backup
ARCserveMgr.exe	Arcserve Backup
Asbrdcst.dll	Arcserve Backup
ASCORE.dll	Arcserve Backup
ASDBEXP.dll	Arcserve Backup
asdbsql_exp.dll	Arcserve Backup

Binary Name	Source
asdcen.dll	Arcserve Backup
ASETUPRES.dll	Arcserve Backup
Asm_db.dll	Arcserve Backup
asm_dt.dll	Arcserve Backup
Asm_mm.dll	Arcserve Backup
ASREMSVC.EXE	Arcserve Backup
Asvctl.dll	Arcserve Backup
asycfilt.dll	Microsoft
BaseLicInst.exe	CA License
bdaemon2.exe	Arcserve Backup
bdelobj.exe	Arcserve Backup
brand.dll	Arcserve Backup
CAPatchManager.dll	Arcserve Backup
careports.exe	Arcserve Backup
casmgmtsvc.exe	Tanuki Software
CAUConfig.dll	CAUpdate
CAUConnect.dll	CAUpdate
CAUMessage.dll	CAUpdate
CAUpdate.dll	CAUpdate
Cazipxp.exe	CA License
ccme_base.dll	EMC (RSA)
ccme_ecc.dll	EMC (RSA)
ccme_eccaccel.dll	EMC (RSA)
cdcdrom.sys	Microsoft
Cdict32.dll	Microsoft
CFX2032.DLL	ChartFX
cheyprod.dll	Arcserve Backup
comcat.dll	Microsoft
CommandBase.dll	Arcserve Backup
COMPRESS.EXE	Microsoft

Binary Name	Source
Configencr.exe	Arcserve Backup
crux_1_0.dll	CA ScanEngine
cruxcrypto_1_0.dll	CA ScanEngine
cryptintf.dll	Arcserve Backup
cryptocme2.dll	EMC (RSA)
CryptoWrapperDll.dll	Arcserve Backup
cstool.dll	Arcserve Backup
Ctl3d32.dll	Microsoft
Dbaxchg2.dll	Arcserve Backup
DeleteMe.exe	Arcserve Backup
demo32.exe	Flexera Software
diskLibPlugin.dll	Vmware
dotnetfx35.exe	Microsoft
e55userupd.dll	Arcserve Backup
etpki_setup.exe	CA ETPKI
EtpkiCrypt.dll	Arcserve Backup
exchenum.dll	Arcserve Backup
fcrinst.dll	Arcserve Backup
fsminst.dll	Arcserve Backup
glib-2.0.dll	Vmware
gobject-2.0.dll	Vmware
gthread-2.0.dll	Vmware
gvmomi.dll	Vmware
GX1142R.dll	Classworks
HBMINST.DLL	Arcserve Backup
iconv.dll	Vmware
icudt34.dll	IBM
icuin34.dll	IBM
icuio34.dll	IBM
icule34.dll	IBM

Binary Name	Source
iculx34.dll	IBM
icutest.dll	IBM
icutu34.dll	IBM
icuuc34.dll	IBM
inocboot.exe	CA AVEngine
Interop.COMAdmin.dll	Microsoft
intl.dll	Vmware
libcaopenssl_crypto.dll	CA ETPKI
libcaopenssl_ssl.dll	CA ETPKI
libcapki.dll	CA ETPKI
libcapki_ipthread.dll	CA ETPKI
libcapki_thread.dll	CA ETPKI
libcurl.dll	Vmware
libeay32.dll	OpenSSL
libetpki_openssl_crypto.dll	EMC (RSA)
liblber.dll	Vmware
libldap.dll	Vmware
libldap_r.dll	Vmware
libxml2.dll	Vmware
licreg.dll	CA License
licregres.dll	CA License
MalwareAPI.dll	Arcserve Backup
MAPISis.dll	Arcserve Backup
MasterSetup.exe	Arcserve Backup
MasterSetup_Main.exe	Arcserve Backup
mfc42.dll	Microsoft
mfc42u.dll	Microsoft
MFC71u.dll	Microsoft
mfc80.dll	Microsoft
mfc80u.dll	Microsoft

Binary Name	Source
mfcm80.dll	Microsoft
mfcm80u.dll	Microsoft
mscomct2.ocx	Microsoft
MSetupRes.dll	Arcserve Backup
MSetupResEx.dll	Arcserve Backup
msi.dll	Microsoft
msstkprp.dll	Microsoft
msvcirt.dll	Microsoft
msvcm80.dll	Microsoft
msvcp60.dll	Microsoft
msvcp71.dll	Microsoft
msvcp80.dll	Microsoft
msvcr71.dll	Microsoft
msvcr80.dll	Microsoft
msvcrt.dll	Microsoft
MSVCRT40.DLL	Microsoft
msxml3.dll	Microsoft
msxml3a.dll	Microsoft
msxml3r.dll	Microsoft
msxml4.dll	Microsoft
msxml4a.dll	Microsoft
msxml4r.dll	Microsoft
NotesUI.dll	CA Alert
ofawin.dll	Arcserve Backup
oleaut32.dll	Microsoft
olepro32.dll	Microsoft
PatchManagerLog.dll	Arcserve Backup
PatchManagerService.exe	Arcserve Backup
PatchManagerUI.exe	Arcserve Backup
PMGUI.dll	Arcserve Backup

Binary Name	Source
psapi.dll	Microsoft
roboex32.dll	Blue Sky Software Corporation
SDRegister.exe	CA DSM
setup.exe	Arcserve Backup
SetupCLS.dll	Arcserve Backup
setupdd.351	Microsoft
setupdd.40	Microsoft
setupddf.351	Microsoft
setupddf.40	Microsoft
Signatures_Plugin.dll	Arcserve Backup
silent.exe	CA License
sps15adp.dll	Arcserve Backup
SQLEXPR.EXE	Microsoft
sqlite3.dll	SQLite software
ssleay32.dll	Vmware
stdole2.tlb	Microsoft
sysimgbase.dll	Vmware
tpcdrom.sys	Microsoft
types.dll	Vmware
unzip.exe	Info-ZIP
UpgradePatchManager.dll	Arcserve Backup
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
vete.dll	CA ScanEngine
vixDiskLib.dll	Vmware
vixDiskLibVim.dll	Vmware
vixMntapi.dll	Vmware
vmacore.dll	Vmware
vmomi.dll	Vmware
vmware-mount.exe	Vmware

Binary Name	Source
vmware-vdiskmanager.exe	Vmware
VService.exe	Arcserve Backup
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
wrapper.dll	Tanuki Software
ws_backup.dll	Arcserve RHA
xalan_messages_1_10.dll	Apache Software Foundation
xalan-c_1_10.dll	Apache Software Foundation
xerces-c_2_7.dll	Apache Software Foundation
xoctl.dll	Arcserve RHA
xsec_1_2_0.dll	Apache Software Foundation
zlib1.dll	Zlib Compression Library

Binary Files that are not Uninstalled Completely

Arcserve Backup installs binary files developed by third parties, other Arcserve products, and Arcserve Backup that cannot be uninstalled completely. The following table describes the binary files.

Binary Name	Source
C:\Program Files (x86)\CA\SharedComponents\CAPKI\Windows\x86\32\uninstaller.exe	Arcserve Backup
C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.dat	CA License
C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.log	CA License
C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98-port	CA License
C:\Windows\Downloaded Installations\{3D52BE33-2E8C-4A39-BECF-878DD4D58252}\CALicense.msi	CA License

Binary Name	Source
C:\Program Files (x86)\CA\SharedComponents\Jre	Java Runtime Environment
C:\$Mft	Microsoft
C:\inetpub\temp\appPools\APC47F.tmp	Microsoft
C:\msdia80.dll	Microsoft
C:\Program Files (x86)\Common Files\microsoft shared\	Microsoft
C:\Program Files (x86)\Microsoft SQL Server\	Microsoft
C:\Program Files (x86)\Microsoft Visual Studio 9.0\	Microsoft
C:\Program Files (x86)\Microsoft.NET\	Microsoft
C:\Program Files\Microsoft Logo\Software Certification Toolkit\Data\	Microsoft
C:\Program Files\Microsoft SQL Server\	Microsoft
C:\Users\Administrator\	Microsoft
C:\Windows\AppCompat\Programs\RecentFileCache.bcf	Microsoft
C:\Windows\assembly\NativeImages_v2.0.50727_32\	Microsoft
C:\Windows\bootstat.dat	Microsoft
C:\Windows\debug\PASSWD.LOG	Microsoft
C:\Windows\Downloaded Installations\{3D52BE33-2E8C-4A39-BECF-878DD4D58252}\1041.MST	Microsoft
C:\Windows\inf\	Microsoft
C:\Windows\Microsoft.NET\	Microsoft
C:\Windows\ODBC.INI	Microsoft
C:\Windows\PFRO.log	Microsoft
C:\Windows\rescache\rc0002\ResCache.hit	Microsoft
C:\Windows\ServiceProfiles\NetworkService\AppData\	Microsoft

Binary Name	Source
C:\Windows\SoftwareDistribution\DataStore\	Microsoft
C:\Windows\System32\	Microsoft
C:\Windows\SysWOW64\	Microsoft
C:\Windows\Tasks\	Microsoft
C:\Windows\WindowsUpdate.log	Microsoft
C:\Windows\winsxs\	Microsoft

Binary Files that do not Contain an Embedded Manifest

Arcserve Backup installs binary files developed by third parties, other Arcserve products, and Arcserve Backup that do not contain an embedded manifest and do not contain a text manifest. The following table describes the binary files.

Binary Name	Source
ASDBCom.exe	Arcserve Backup
ca_vcbpopulatedb.exe	Arcserve Backup
DBBAFAgentWrapper.exe	Arcserve Backup
VCBUI.exe	Arcserve Backup
inocboot.exe	CA AVEngine
authtool.exe	CA eTrust
ConfigTool.exe	CA eTrust
eavdisc.exe	CA eTrust
eITMURL.exe	CA eTrust
igateway.exe	CA eTrust
Inocmd64.exe	CA eTrust
InoDist.exe	CA eTrust
InoRpc.exe	CA eTrust
InoRT.exe	CA eTrust
InoTask.exe	CA eTrust
ITMDist.exe	CA eTrust
phonhome.exe	CA eTrust

Binary Name	Source
SigCheck.exe	CA eTrust
spar.exe	CA eTrust
spintool.exe	CA eTrust
transtool.exe	CA eTrust
UnITMEng.exe	CA eTrust
BaseLicInst.exe	CA License
UpdateData.exe	CA License
unzip.exe	Info-ZIP
java.exe	Java Runtime Environment
javac.exe	Java Runtime Environment
javacpl.exe	Java Runtime Environment
java-rmi.exe	Java Runtime Environment
javaw.exe	Java Runtime Environment
javaws.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment
keytool.exe	Java Runtime Environment
kinit.exe	Java Runtime Environment
klist.exe	Java Runtime Environment
ktab.exe	Java Runtime Environment
orbd.exe	Java Runtime Environment
pack200.exe	Java Runtime Environment
policytool.exe	Java Runtime Environment
rmid.exe	Java Runtime Environment
rmiregistry.exe	Java Runtime Environment
servertool.exe	Java Runtime Environment
tnameserv.exe	Java Runtime Environment
unpack200.exe	Java Runtime Environment
COMPRESS.EXE	Microsoft
DTSWizard.ni.exe	Microsoft
SQLEXPR.EXE	Microsoft

Binary Name	Source
SQLPS.ni.exe	Microsoft
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
WindowsServer2003-KB942288-v4-x64.exe	Microsoft
WindowsServer2003-KB942288-v4-x86.exe	Microsoft
WindowsXP-KB942288-v3-x86.exe	Microsoft
casmgmtsvc.exe	Tanuki Software
BAB_060706_SETUP_ALPHA.EXE	Virtual Memory System
BAB_060706_SETUP_VAX.EXE	Virtual Memory System

Arcserve Backup installs binary files developed by other Arcserve products and Arcserve Backup that contain a text manifest and do not contain an embedded manifest. The following table describes the binary files.

Binary Name	Source
setuprd.exe	Arcserve Backup
Cazipxp.exe	CA License

Arcserve Backup MSI Installer Package Identification

Windows MSI installer packages should contain a Property table and an Upgrade table. Various Arcserve Backup MSI installers do not contain an Upgrade table. The following list identifies the affected Arcserve Backup installer packages:

- ARCserve.msi
- BaofNtNw.msi
- BrightStorSAK.msi
- CADiag.msi
- DBAExch.msi
- DBAExch12.msi
- DBAIFX.msi
- DBANotes.msi
- DBASQL.msi
- DBASYB.msi

- EBSAgent.msi
- msxml.msi
- NASAgent.msi
- NTAgent.msi
- OPTDRO.msi
- OPTEO.msi
- OPTIO.msi
- OPTSBO.msi
- PM.msi
- RMANAgent.msi
- SAPAgent.msi
- SP2K7Agent.msi

Chapter 4: Installing and Upgrading Arcserve Backup

This section contains the following topics:

How to Complete Prerequisite Tasks (see page 81)
Install Arcserve Backup (see page 86)
Upgrade Arcserve Backup from a Previous Release (see page 94)
Create a Silent Installation Response File (see page 101)
Upgrade Arcserve Backup Agents Silently to the Current Release (see page 107)
Deploy Agents to Remote Computers from the Primary Server (see page 110)
How to Install Arcserve Backup Using Unicenter Software Delivery (see page 120)
Post-Installation Tasks (see page 126)

How to Complete Prerequisite Tasks

Before you install or upgrade Arcserve Backup, complete the following tasks:

Installation and System Requirements

Review the Arcserve Backup readme file. The readme file contains the operating system requirements, hardware and software prerequisites, last-minute changes, and known issues with Arcserve Backup. The readme file is provided in HTML format and is located at root level on the installation media.

Installation Servers

Compile a list of servers where you are installing Arcserve Backup and identify the following:

- The names of the Arcserve Backup domains
- The names of the servers where you are installing Arcserve Backup

  Note: Arcserve Backup server names and Arcserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.
- Determine the type of Arcserve Backup servers you are installing.

  Note: For more information, see Types of Arcserve Backup Server Installations (see page 41).
- If you are installing Arcserve Backup, agents, and options on remote systems, you must specify the host names of the target systems. Arcserve Backup does not support specifying IP addresses when you are performing a remote installation or upgrade.

Arcserve Backup Database

Determine the database application that you will use for your Arcserve Backup installation. For more information, see Database Requirements (see page 46).

Administrative Privileges

Ensure that you have administrator privileges or the proper authority to install software on the servers where you are installing Arcserve Backup.

Upgrades

If you are upgrading your current BrightStor Arcserve Backup installation to this release, review the information about upgrades, backwards compatibility, and data migration in Upgrade Considerations (see page 54).

Primary Server Installations

You must install and license the Arcserve Backup Central Management Option to install a primary server.

Note: To install a Arcserve Backup domain consisting of a primary server and one or more member servers, you must install the primary server before you install the member servers. After you install the primary server, you allow the member servers to join the domain that was created when you installed the primary server.

Member Server Installations

You must specify Arcserve Backup authentication credentials to allow the member servers to join the primary servers' domain (for example, *caroot* and the Arcserve Backup password that you specified when you installed the primary server). The process of allowing a member server to join a Arcserve Backup domain does support using Windows authentication.

Global Dashboard Installations

Before installing Global Dashboard, verify the following prerequisites:

License Requirements

- To enable Global Dashboard capabilities, you must have a valid Arcserve Backup Global Dashboard license at the Central Primary Server, with multiple license counts to include all registered Branch Primary Servers. (Branch Primary Servers do not need to install a Global Dashboard license).

Central Primary Server

- Arcserve Backup (Primary or Stand-alone server) installed.

  Note: You can install Global Dashboard on member servers; however, member servers cannot function as Central Primary Servers.

- Arcserve Backup database must have Microsoft SQL Server 2005 or later installed (does not support Microsoft SQL Express or Microsoft SQL Server 2000 as its database).

- Sufficient Arcserve Backup database capacity for your Global Dashboard environment. For more information about estimated database capacity for the Central Primary Server, see Global Dashboard Data Storage Requirements (see page 25).

Branch Primary Servers

- Arcserve Backup (Primary or Stand-alone server) installed.

- Arcserve Backup database must have Microsoft SQL Server 2000 or later installed or SQL Server Express 2008 or later installed.

Global Dashboard Console

- Arcserve Backup Primary server, Stand-alone server, or Manager Console component installed.

  Note: You can install the Global Dashboard Console on member servers; however, member servers cannot function as Branch Primary Servers.

Ports Configuration

To ensure that primary servers and member servers can communicate in a secure environment, all communication ports must be allowed to remain in an open state while you install Arcserve Backup. For more information, see Primary Server and Member Server Communication Ports (see page 231).

Cluster Installations

When you install Arcserve Backup, the installation wizard detects the following cluster applications:

- Microsoft Cluster Server (MSCS)
- NEC Cluster Server (CLUSTERPRO/ExpressCluster)

Before you start the installation wizard, ensure that these cluster applications are installed, properly configured, and running.

Note: Arcserve Backup does not support remote installations in a cluster environment.

Remote Installations

You must disable simple file sharing on Windows XP systems to ensure that you can successfully install Arcserve Backup, agents, and options on remote systems. Use the steps that follow to disable simple file sharing on remote systems:

1. Log in to the remote Windows XP system.

   From the Windows desktop, double-click My Computer.

   My Computer opens.

2. From the Tools menu, click Folder Options.

   The Folder Options dialog opens.

3. Click the View tab.

   Locate Use simple file sharing (recommended).

   Clear the check box next to Use simple file sharing (recommended) and click OK.

   Simple file sharing is disabled.

Storage Devices

Connect your storage devices to the systems that you designate as Arcserve Backup primary servers and member servers, and the SAN. Arcserve Backup detects and configures libraries that are connected directly to the Arcserve Backup servers and the SAN the first time the Tape Engine starts. You do not need to run a wizard or other external application to enable Arcserve Backup to detect and configure supported libraries. For all other types of devices (for example, NAS devices, IBM 3494 libraries, Sun StorageTek ACSLS libraries, ARCserve Tape RAID libraries, and ARCserve virtual libraries), you must configure the devices manually after you install Arcserve Backup using Device Configuration or Enterprise Module Configuration.

Note: For more information, see the *Administration Guide*.

If you are using a fibre or SCSI device, ensure that your Arcserve Backup server has a SCSI/Fibre controller or adapter supported by both Windows and Arcserve Backup. Arcserve Backup can support most installed SCSI controllers.

Note: To ensure that your hardware devices are compatible and that Arcserve Backup can communicate with your system, you can get the latest Certified Device List from www.arcserve.com.

Storage Area Network Installations

In a multiple-server SAN environment, you must designate a server that is connected to the shared library to function as a primary server before you install and license the Arcserve Backup server component and the Arcserve Backup Central Management Option on the domain primary server. You must then designate all other servers connected to the shared library to function as member servers. The member servers must reside in the same Arcserve Backup domain as the primary server. When you are finished, the primary server automatically detects your SAN infrastructure - manual configuration is not required.

Note: If you are upgrading from a previous release, you must install the Arcserve Backup primary server on the system that is functioning as the SAN primary and you must install the Arcserve Backup Member Server on the systems that are functioning as SAN distributed servers.

Antivirus

If you are installing Arcserve Backup database backup agents on a system where you are running CA Antivirus, you must apply the following driver update to both the Arcserve Backup server and the client machine:

https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/156/ildrvupdate.html

DNS Communication

Ensure that domain name system (DNS) communication is configured to optimize communication between the Arcserve Backup Manager Console and the remote systems in your environment. For example, you should configure DNS to perform reverse lookups efficiently. For more information about configuring DNS communication, see the Microsoft Help and Support website.

Cross-platform Agents

To install or upgrade a cross-platform agent, you must have the Arcserve Backup installation media available to you while you run the installation wizard.

Install Arcserve Backup

You can install Arcserve Backup on local or remote computers and on computers running Windows Server Core using the installation wizard.

To install Arcserve Backup

1. Insert the Arcserve Backup installation media into your computer's optical drive.

   Note: If the Arcserve Backup Installation Browser does not appear, run Setup.exe from the root directory on the installation media.

   From the right column on the Product Installation Browser, click Install Arcserve Backup for Windows.

   The Prerequisite Components dialog opens.

2. Click Install to install the Prerequisite Components.

   Be aware of the following behavior:

   - The Prerequisite Components dialog opens only if Setup does not detect Arcserve Backup Prerequisite Components installed on the target computer.
   - On Windows Server 2003 systems, you must restart your computer and repeat the previous steps if Setup installs Microsoft SQL Server 2008 Express Edition.

     Note: If you are installing Arcserve Backup on the active node in a cluster-aware environment, the cluster resources are transferred from the active node to the passive node while the active node restarts. After the active node restarts, you should transfer the cluster resources back to the original active node.

3. On the License Agreement dialog, accept the terms of the Licensing Agreement and click Next.

4. Follow the prompts and complete all required information on the subsequent dialogs.

   The following list describes dialog-specific information about installing Arcserve Backup.

   Select Install/Upgrade Type dialog

   When you select the remote installation option, you can install Arcserve Backup on multiple systems.

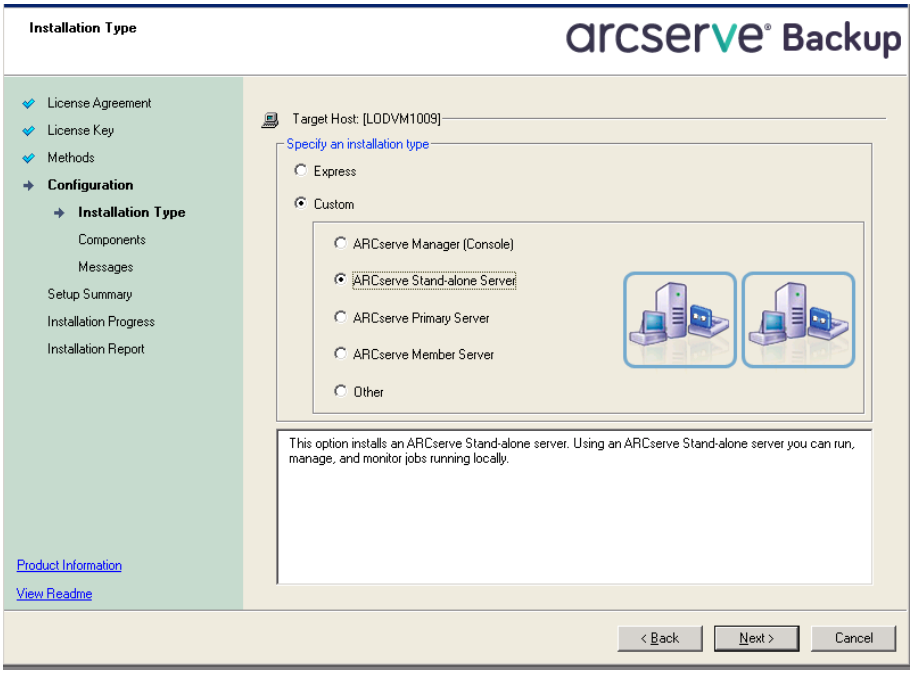
   With remote installations, the target remote systems can consist of different Arcserve server types, different Arcserve Backup agents and options, or both.

   Note: The setup program for cluster machines does not support remote installation of the Arcserve Backup base product or the Arcserve Backup agents. This remote install limitation for the Arcserve Backup agents (for example, the Agent for Microsoft SQL Server and the Agent for Microsoft Exchange Server) only applies if you use a virtual host. Remote installation of Arcserve Backup agents using the physical hosts of clusters is supported.

   Installation Type dialog

   Lets you specify the type of Arcserve Backup components that you want to install, by selecting either the Express or Custom installation type.

   Note: When you upgrade from a previous release, the installation wizard detects your current Arcserve configuration and selects the Installation/Upgrade type that is appropriate for your new installation. For more information, see Types of Arcserve Backup Server Installations (see page 41) and Arcserve Backup Server Options (see page 45).



Components dialog

Lets you specify the Arcserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the Arcserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and primary server name in your network. Therefore, you should complete at least one primary server installation before you perform member server installations.
- When you click the Arcserve Backup object or the Server object on the Select Products dialog, the installation wizard specifies the default Stand-alone Server installation components, regardless of the installation type that you specified on the Select Install/Upgrade Type dialog. To ensure that you are installing the correct components, expand the Server object, expand the object for the type of Arcserve Backup server that you want to install, and check the check boxes corresponding to the components that you want to install.
- Agent Deployment is a wizard-like application that lets you install or upgrade Arcserve Backup agents on multiple remote systems, after you install Arcserve Backup. To support this capability, Setup must copy Setup source files to the Arcserve Backup server. To copy the contents of the installation media to the Arcserve Backup server, you must select Agent Deployment on the Components dialog. When you select Agent Deployment, the length of time required to install or upgrade Arcserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the Arcserve Backup Client Agent for Windows into the same directory as the Arcserve Backup base product.
- Global Dashboard can be installed on primary servers, stand-alone servers, and member servers. However, you cannot configure member servers to function as Central Primary Servers and Branch Primary Servers. For more information about Central Primary Servers and Branch Primary Servers, see the *Dashboard User Guide*.
- On computers running Windows Server Core, you can install only the following Arcserve Backup products:

  - Member Server and supported options

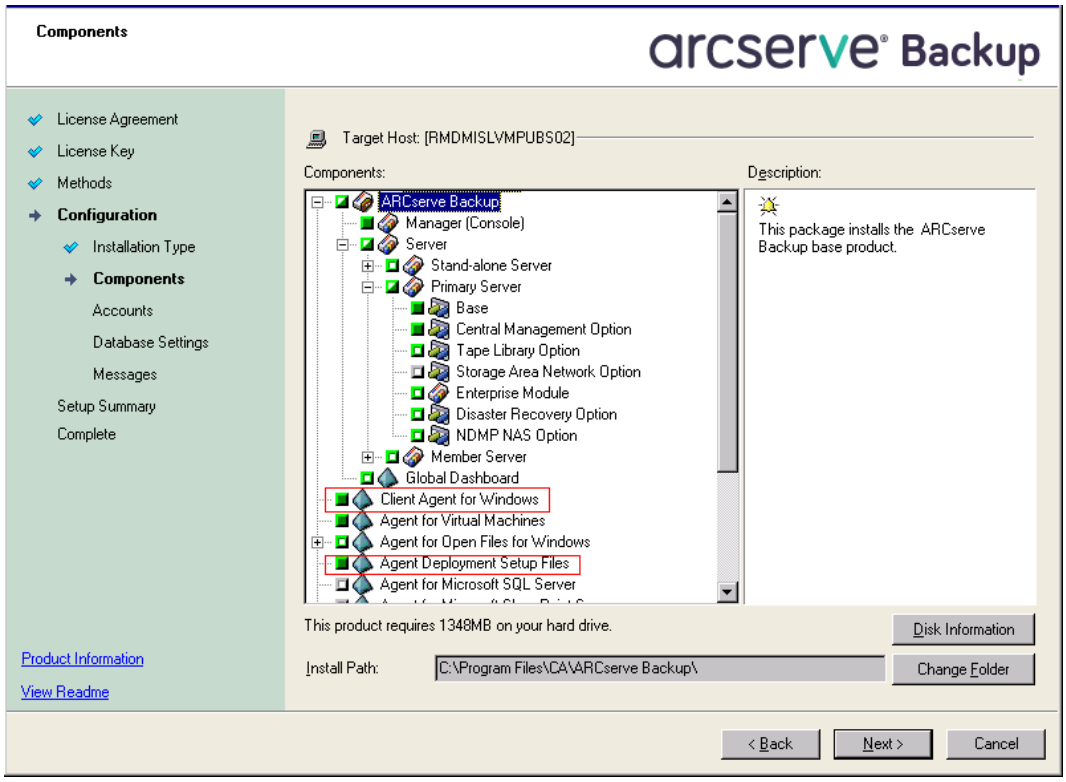
  - Agent for Open Files

  - Agent for Virtual Machines

  - Client Agent for Windows

  - Disaster Recovery Option

The following diagram illustrates the default installation path for the Client Agent for Windows and Agent Deployment is specified:

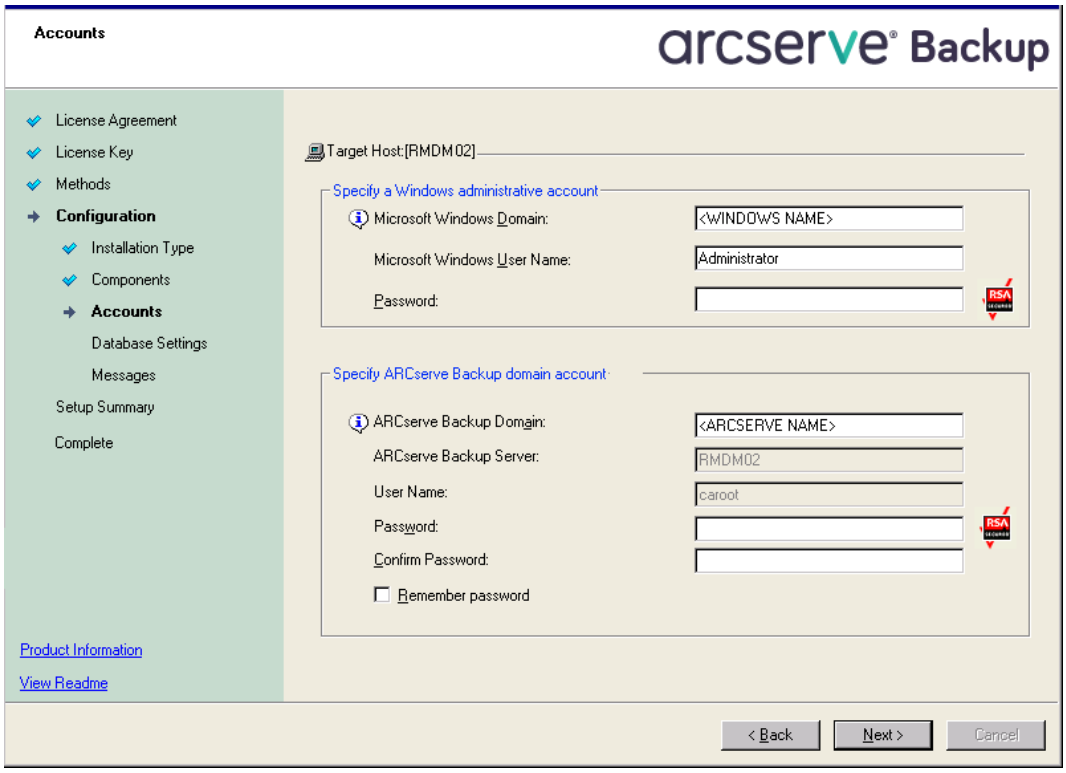


Accounts dialog

Lets you set up your Arcserve Backup accounts.

If Setup detects a cluster-aware application running in your environment, and you want to install Arcserve Backup in the cluster-aware environment, check the Cluster Environment Installation option and specify the path to the shared disk where you want to install Arcserve Backup.

Note: Arcserve Backup server names and Arcserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

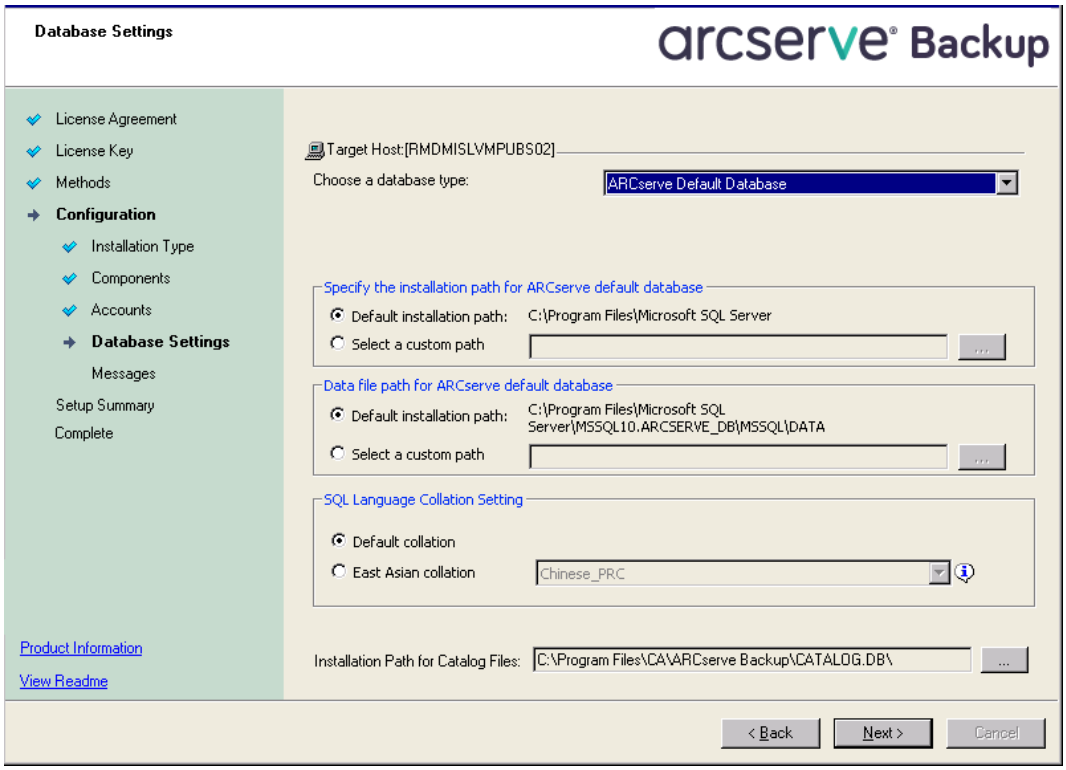


Database Settings dialog

Lets you configure the Arcserve Backup database.

After you specify a database application (ARCserve Default Database or Microsoft SQL Server) complete the required fields on this dialog and click Next.

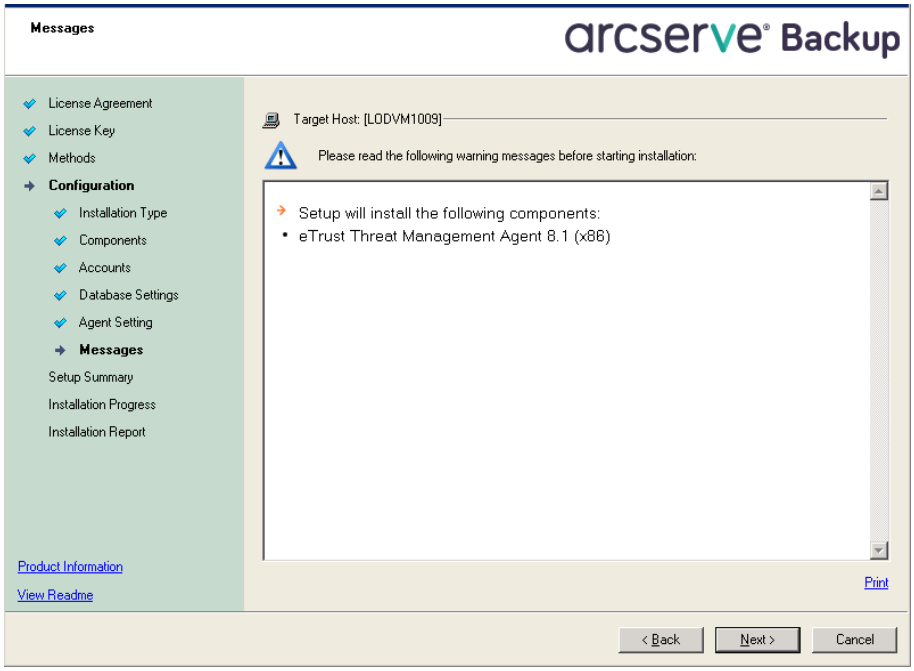
Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that Arcserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



Messages dialog

As you review the messages in the Messages dialog, you should attempt to resolve the problems at this time.

The following graphic illustrates the Important Warning Messages dialog:



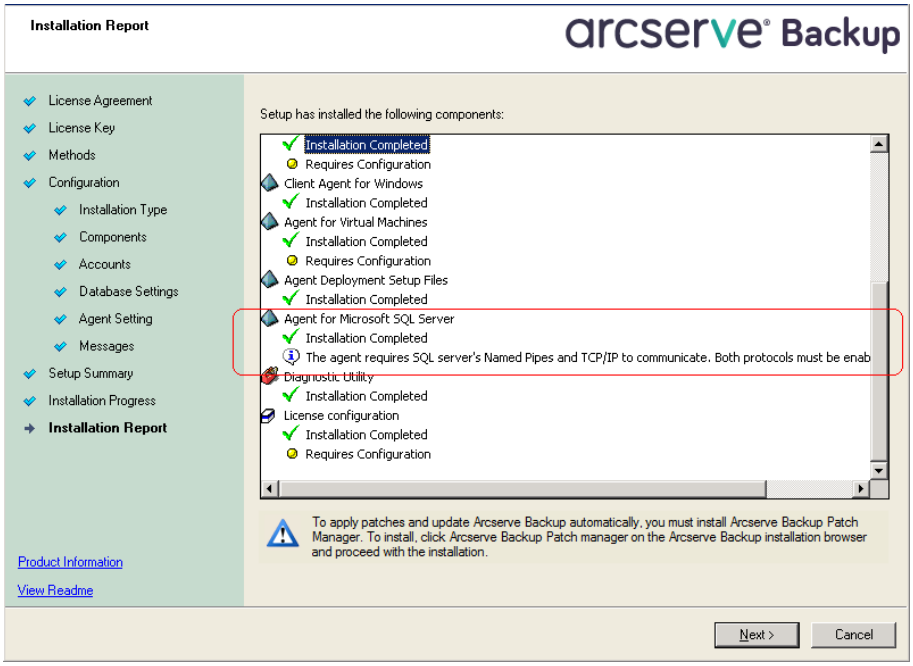
Setup Summary dialog

To modify the components that you want to install, click Back as often as necessary to return to the dialog containing the installation options that you want to change.

Installation Report dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

The diagram that follows illustrates the Installation Report dialog. The Agent for Microsoft SQL Server requires configuration.



Note: You may be required to restart the server after you install Arcserve Backup. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.

Installation Summary dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

License Verification dialog

To enter license keys, locate the components, agents, and options that you are installing, select the Use License Key option, and enter the license key for the component.

Click Continue to close the License Verification dialog.

5. Click Finish on the Installation Summary dialog to complete the installation.

Upgrade Arcserve Backup from a Previous Release

You can upgrade Arcserve Backup on local or remote computers and on computers running Windows Server Core using the installation wizard. To upgrade an installation means to reinstall features or components to higher release or build number without uninstalling the older release. The upgrade process lets you retain most of your current settings and migrate the information stored in the previous Arcserve Backup database to the new database.

If you are currently using one of the following releases of Arcserve Backup, you can upgrade to this release from the following products:

- Arcserve Backup r16 for Windows--Includes the General Availability (GA) release and all of the latest service packs.
- Arcserve Backup r15 for Windows--Includes the General Availability (GA) release and all of the latest service packs.
- Arcserve Backup r12.5 for Windows--Includes the General Availability (GA) release and all of the latest service packs.

Important! If you want to upgrade from <bab> v9, BrightStor Enterprise Backup v10.5, <bab> r11.1, <bab> r11.5, or Arcserve Backup r12 you must uninstall the previous release and then install this release of Arcserve Backup. However, if you wish to retain the database information from your previous implementation, you must upgrade the previous implementation to Arcserve Backup r12.5 GA release (with no SP), and then upgrade from Arcserve Backup r12.5 to this release. To obtain Arcserve Backup r12.5 installation media, contact Arcserve Support. For all other previous releases of <bab> or BrightStor Enterprise Backup earlier than v9, you must uninstall the previous release before you install this release.

For more information about upgrading to this release, see Upgrade Considerations (see page 54).

To upgrade Arcserve Backup from a previous release

1. Insert the Arcserve Backup installation media into your computer's optical drive.

   Note: If the Arcserve Backup Installation Browser does not appear, run Setup.exe from the root directory on the installation media.

   From the right column on the Product Installation Browser, click Install Arcserve Backup for Windows.

   The Prerequisite Components dialog opens.

2. Click Next to install the Prerequisite Components.

   Note: The Prerequisite Components dialog opens only if Setup does not detect Arcserve Backup Prerequisite Components installed on the target computer.

3. On the License Agreement dialog, accept the terms of the Licensing Agreement and complete the fields on the Customer and Information dialog.

4. Follow the prompts on the subsequent dialogs and complete all required information.

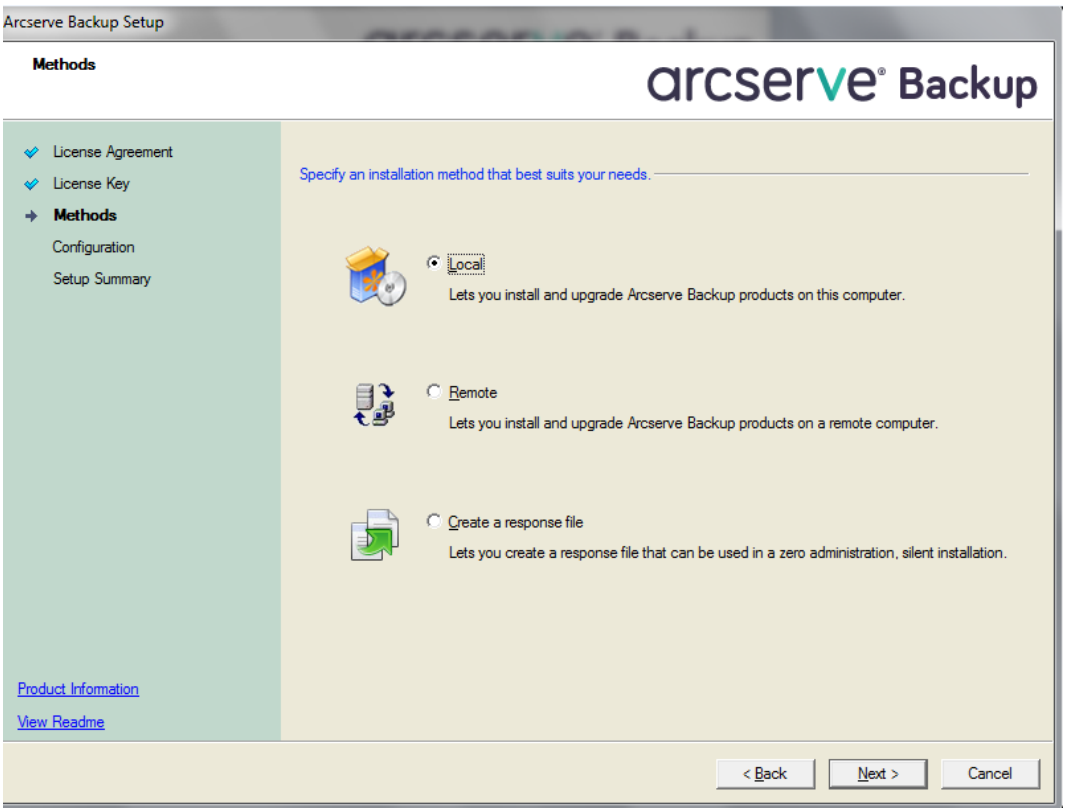
   The following list describes dialog-specific information about upgrading Arcserve Backup from a previous release.

Methods dialog

If you are upgrading from a previous release to an Arcserve Primary Server, you must select the Local Installation/Upgrade option. Arcserve Backup does not support the following types of upgrades:

- Upgrade from a previous release to an Arcserve Primary Server on a remote system.
- Silent upgrade from a previous release to an Arcserve Primary Server on a system using a response file.

For all other types of upgrades, select the option corresponding to the task that you want to perform.



Components dialog

Lets you specify the Arcserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the Arcserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and primary server name in your network. Therefore, you should complete at least one primary server installation before you perform member server installations.
- When you click the Arcserve Backup object or the Server object on the Select Products dialog, the installation wizard specifies the default Stand-alone Server installation components, regardless of the installation type that you specified on the Select Install/Upgrade Type dialog. To ensure that you are installing the correct components, expand the Server object, expand the object for the type of Arcserve Backup server that you want to install, and check the check boxes corresponding to the components that you want to install.
- Agent Deployment is a wizard-like application that lets you install or upgrade Arcserve Backup agents on multiple remote systems, after you install Arcserve Backup. To support this capability, Setup must copy Setup source files to the Arcserve Backup server. To copy the contents of the installation media to the Arcserve Backup server, you must select Agent Deployment on the Components dialog. When you select Agent Deployment, the length of time required to install or upgrade Arcserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the Arcserve Backup Client Agent for Windows into the same directory as the Arcserve Backup base product.
- Global Dashboard can be installed on primary servers, stand-alone servers, and member servers. However, you cannot configure member servers to function as Central Primary Servers and Branch Primary Servers. For more information about Central Primary Servers and Branch Primary Servers, see the *Dashboard User Guide*.
- On computers running Windows Server Core, you can install only the following Arcserve Backup products:

  - Member Server and supported options

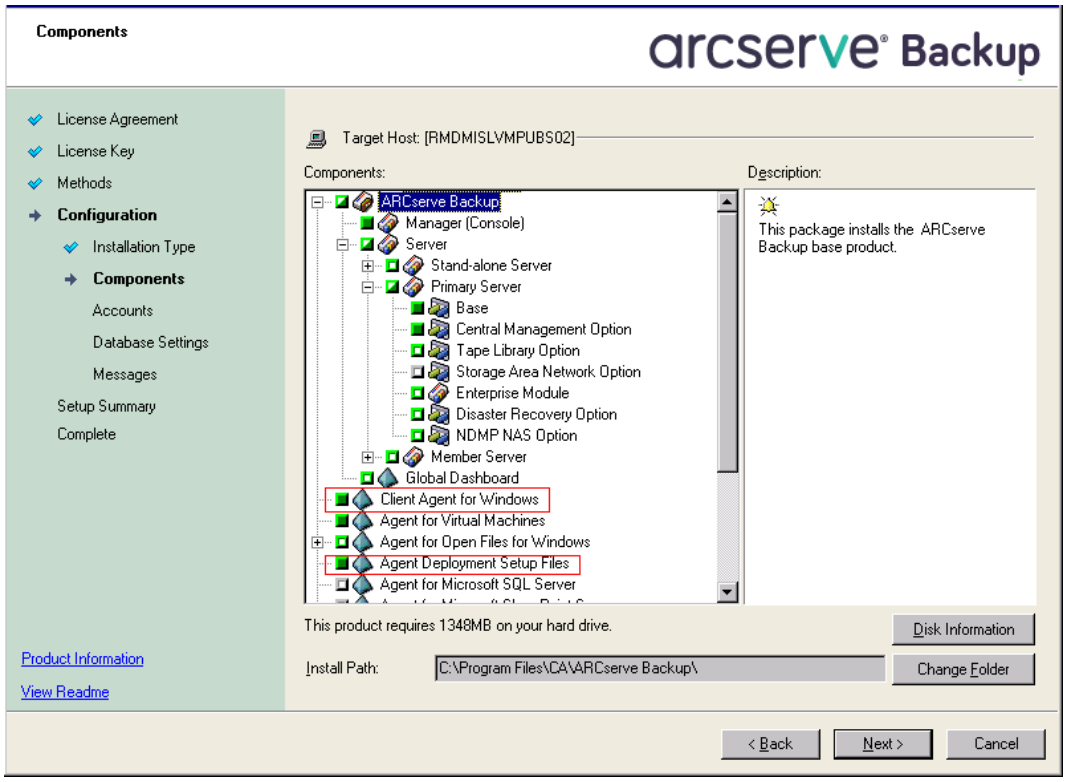
  - Agent for Open Files

  - Agent for Virtual Machines

  - Client Agent for Windows

  - Disaster Recovery Option

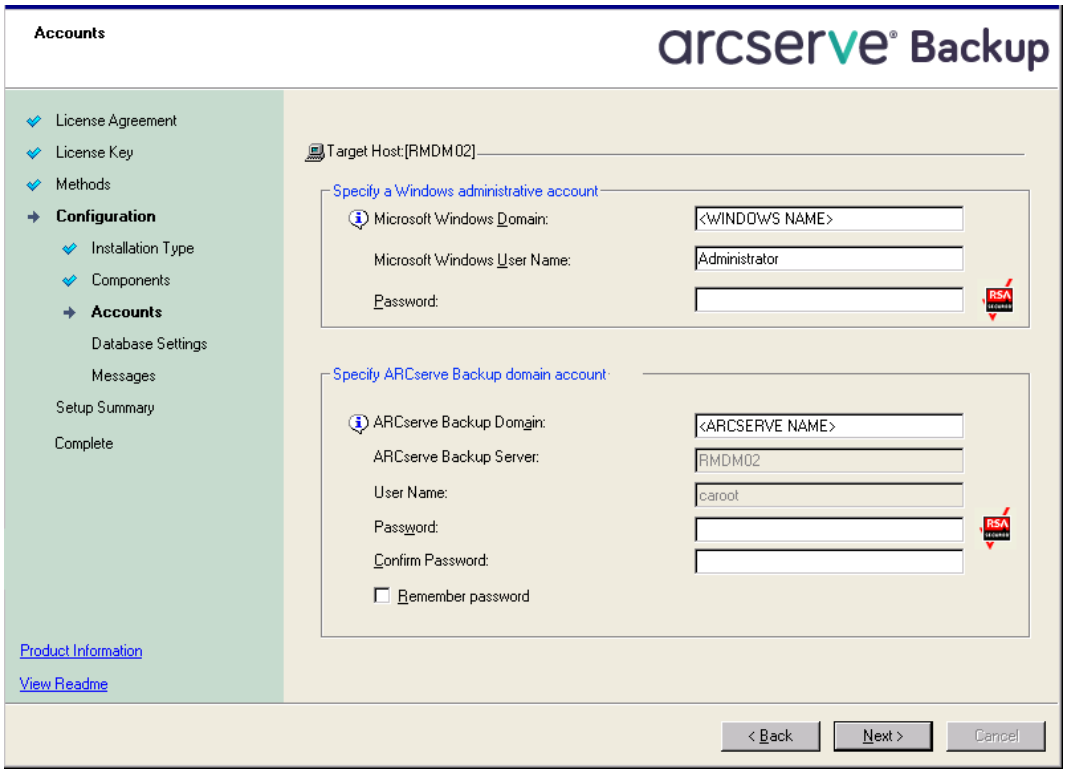
The following diagram illustrates the default installation path for the Client Agent for Windows and Agent Deployment is specified:



Accounts dialog

If Setup detects a cluster-aware application running in your environment, and you want to install Arcserve Backup in the cluster-aware environment, check the Cluster Environment Installation option and specify the path where you want to install Arcserve Backup.

Note: Arcserve Backup server names and Arcserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

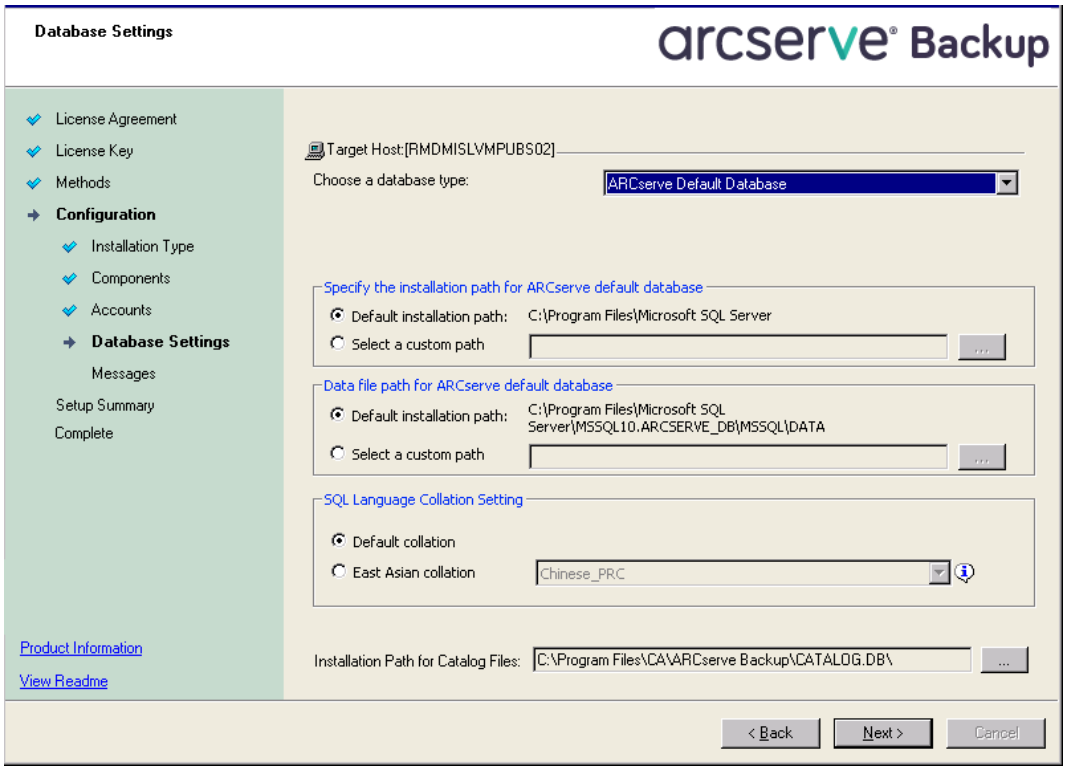


Database Settings dialog

Lets you configure the Arcserve Backup database.

After you specify a database application (Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition) complete the required fields on this dialog.

Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that Arcserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



Messages dialog

After you review the messages in the Important Warning Messages dialog, you should attempt to resolve the problems at this time.

Setup Summary dialog

To modify the components that you want to install, click Back as often as necessary to return to the dialog containing the installation options that you want to change.

Installation Summary dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

License Verification dialog

To enter license keys, locate the components, agents, and options that you are installing, select the Use License Key option, and enter the license key for the component.

Click Continue to close the License Verification dialog.

Click Finish on the Installation Summary dialog to open the Arcserve Backup Server Migration dialog.

Arcserve Backup Server Data Migration dialog

Specify the data that you want to migrate. For more information about data migration, see Data Migration from a Previous Release (see page 57).

Important! The Arcserve Backup Server Data Migration dialog does not appear when you upgrade from Arcserve Backup for Windows r12 SP1 and Arcserve Backup for Windows r12.5 to this release.

5. Click OK on the Arcserve Backup Server Data Migration dialog to complete the upgrade.

Be aware of the following limitations and considerations:

- Arcserve Backup does not support recovering the Arcserve Backup database when the last backup was before you upgraded to this release. As a best practice, you should back up the Arcserve Backup as soon as possible after the upgrade is complete.
- You may be required to restart the server after the upgrade process is complete. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.
- To ensure that all Arcserve Backup services start properly in a cluster-aware environment, you must execute the cstop and cstart scripts on the Arcserve Backup server before you open the Arcserve Backup Manager Console. You must complete this task when you upgrade from Arcserve Backup r12.5 (includes the GA release and the latest service packs) to this release.

Create a Silent Installation Response File

During an interactive installation, many Arcserve Backup components require you to enter configuration information (for example, installation directory, user name, and password). During a silent installation, (a non-interactive installation) this information is read from a previously created response file. The default response file name is setup.icf, but can be renamed to suit your needs.

To create a silent installation response file

1. Insert the Arcserve Backup installation media into your computer's optical drive.

   Browse to the \Install directory.

   Double-click MasterSetup.exe to start MasterSetup, and click Next on the Welcome to Arcserve Backup dialog.

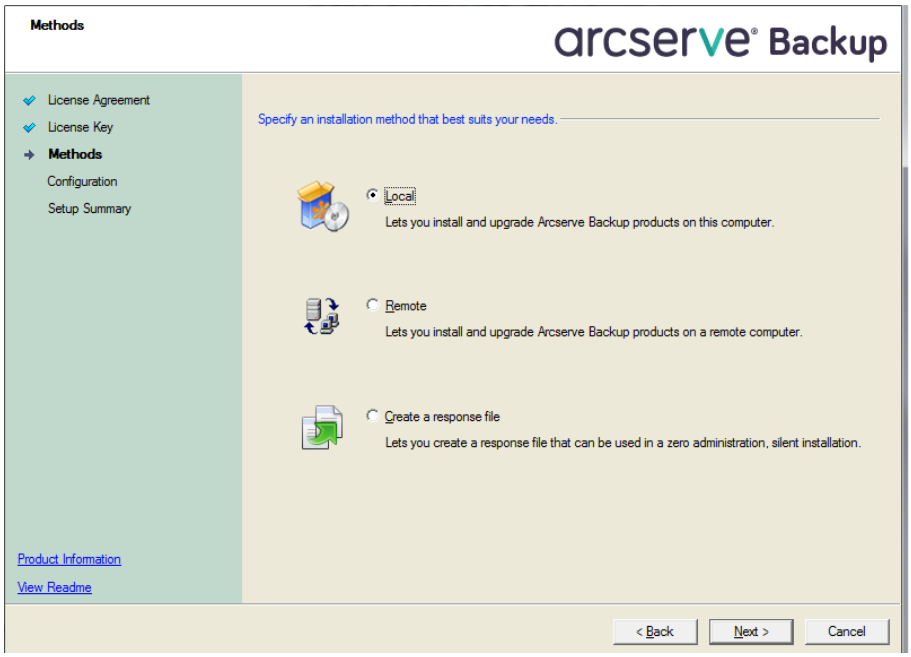
2. On the License Agreement dialog, accept the terms of the Licensing Agreement and complete the fields on the Customer and Information dialog.

3. Follow the prompts on the subsequent dialogs and complete all required information.

   The following list describes dialog-specific information about creating a response file.

   Methods dialog

   You must select Create a response file to create the response file.



Components dialog

Lets you specify the Arcserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the Arcserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and primary server name in your network. Therefore, you should complete at least one primary server installation before you perform member server installations.
- When you click the Arcserve Backup object or the Server object on the Select Products dialog, the installation wizard specifies the default Stand-alone Server installation components, regardless of the installation type that you specified on the Select Install/Upgrade Type dialog. To ensure that you are installing the correct components, expand the Server object, expand the object for the type of Arcserve Backup server that you want to install, and check the check boxes corresponding to the components that you want to install.
- Agent Deployment is a wizard-like application that lets you install or upgrade Arcserve Backup agents on multiple remote systems, after you install Arcserve Backup. To support this capability, Setup must copy Setup source files to the Arcserve Backup server. To copy the contents of the installation media to the Arcserve Backup server, you must select Agent Deployment on the Components dialog. When you select Agent Deployment, the length of time required to install or upgrade Arcserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the Arcserve Backup Client Agent for Windows into the same directory as the Arcserve Backup base product.
- Global Dashboard can be installed on primary servers, stand-alone servers, and member servers. However, you cannot configure member servers to function as Central Primary Servers and Branch Primary Servers. For more information about Central Primary Servers and Branch Primary Servers, see the *Dashboard User Guide*.
- On computers running Windows Server Core, you can install only the following Arcserve Backup products:

  - Member Server and supported options

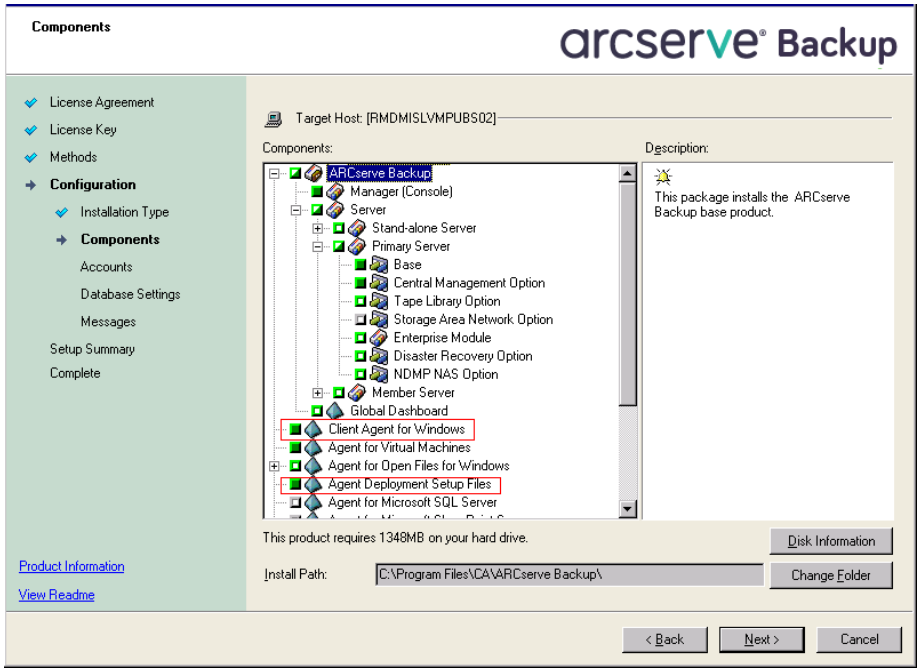
  - Agent for Open Files

  - Agent for Virtual Machines

  - Client Agent for Windows

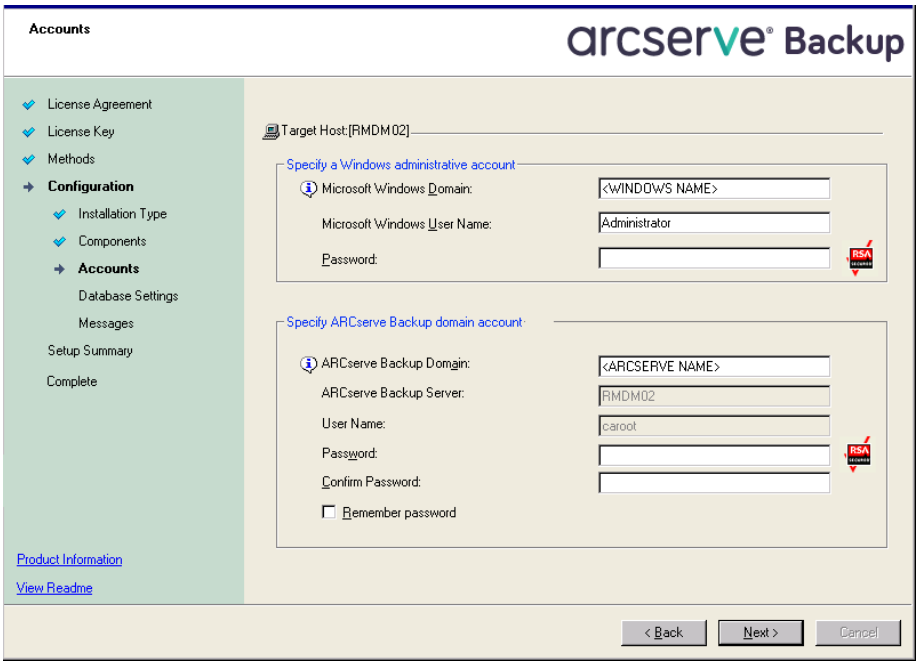
  - Disaster Recovery Option

The following diagram illustrates the default installation path for the Client Agent for Windows and Agent Deployment is specified:



Accounts dialog

Arcserve Backup domain names and Arcserve Backup server names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

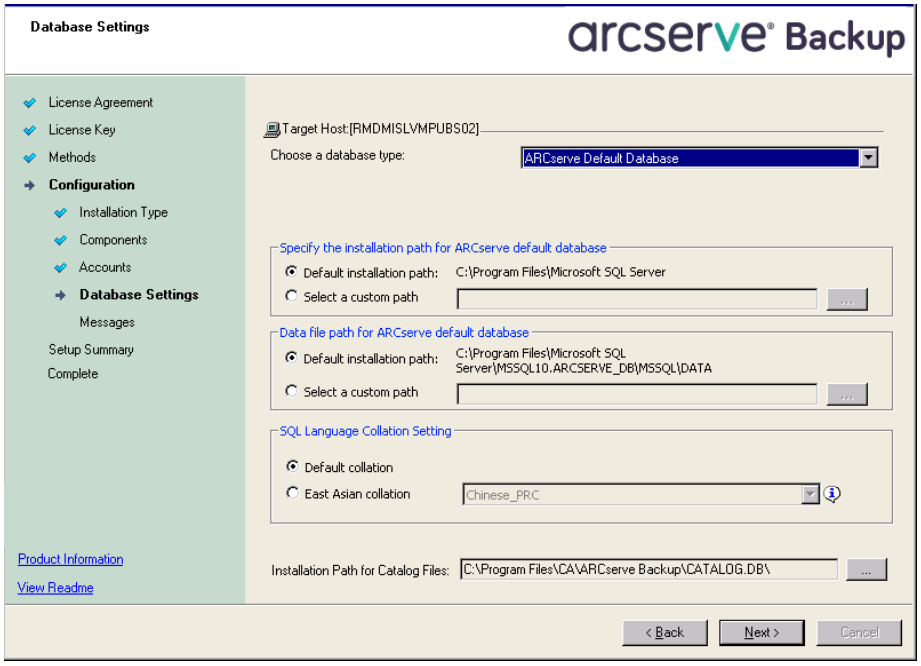


Note: If you do not retain the domain name from your previous installation, Arcserve Backup changes your previous caroot password to a blank password. You can change the blank password after the installation is complete.

The caroot password can consist of any combination of alphanumeric and special characters, but may not exceed 15 bytes. A password totaling 15 bytes equates to approximately 7 to 15 characters.

Database Settings dialog

If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that you can search and sort the data. To do this, click Language Support Options on the SQL Server Express Instance dialog and follow the on-screen instructions to complete the configuration. (If you are hosting the Arcserve Backup database with Microsoft SQL Server, you click Language Support Options on the Select Database Installation Path dialog.)



Setup Summary dialog

To modify the components that you want to install, click Back as often as necessary to return to the dialog containing the installation options that you want to change.

License Verification dialog

To enter license keys, locate the components, agents, and options that you are installing, select the Use License Key option, and enter the license key for the component.

4. After you generate the response file, you can use it with MasterSetup.exe, to silently install the Arcserve Backup components that you selected.

   By default, Arcserve Backup saves the response file in the following directory:

   - **Windows Server 2003 platforms:**

     C:\Documents and Settings\Administrator\My Documents\Setup.icf

   - **All other Windows platforms:**

     C:\Users\Administrator\Documents\Setup.icf

   You can specify a different location by clicking the ellipsis button on the Setup Summary dialog.

5. After Setup competes the response file, click Finish.

To view full details about the required parameters, open the Windows Command Line and execute the following command:

```
mastersetup /?
```

Example: Execute a Response File

The following example describes the syntax for executing a response file. The response file is labeled setup.icf and is located in c:\temp.

```
mastersetup.exe /I:"c:\temp\setup.icf"
```

You can edit the setup.icf file to change the InstallScanEng setting from 1 to 0 to indicate that the Scan Engine should not be installed.

Note: You may have to restart the target system after the installation completes. To determine if you have to restart your machine, check the ProdWiz.log for a restart message.

For more information about using a response file to install Arcserve Backup, see Upgrade Arcserve Backup Agents Silently to the Current Release (see page 107).

Upgrade Arcserve Backup Agents Silently to the Current Release

Situations may arise where you want to upgrade agents from different Arcserve releases installed on a system to the current release. The process of identifying the agents, their release numbers, and the process of performing the upgrade itself, can take a lot of time.

To simplify this task, you can run MasterSetup silently from the Windows Command Line to upgrade all Arcserve Backup agents that are installed on a system to the current release.

There are several methods that you can use to complete this task.

- Execute MasterSetup directly from the installation media. Specify the syntax to upgrade all agents on the target (remote) system.
- Share the optical drive where the installation media is mounted on your network. Execute the command from the target (remote) system and specify the syntax to upgrade all agents on the local system.
- Create a network share and copy the entire contents of the installation media to the shared directory. Execute the command from the target (remote) system and specify the syntax to upgrade all agents on the local system.

When you run MasterSetup from the Command Line, you cannot upgrade the Arcserve Backup base product and Arcserve Backup options.

MasterSetup is installed in the following directory on the installation media:

<drive>\Install\mastersetup.exe

To upgrade Arcserve Backup agents to the current release

1. Complete the steps described in Upgrade Arcserve Backup from a Previous Release (see page 94).
2. Create a response file using the steps described in Create a Silent Installation Response File (see page 101).
3. After you complete the upgrade process and create a response file, open the Windows Command Line and browse to the directory where MasterSetup is accessible.

   Execute MasterSetup using the following syntax:

   MasterSetup [/?][/D][/H:<host name>][/U:<User Name>][/P:<Password>][/I:<Icf Path>][/AU][/O]

   Note: Square brackets [ ] indicate that the argument inside the brackets is optional. Angle brackets < > indicate that the argument inside the brackets is required.

   /?

   Displays the usage for this command.

   /D

   Displays the status of the installation.

   /H

   Specifies the host name of the target system.

   /U

   Specifies the user name for the target system.

/P

Specifies the password for the user name on the target system.

/I

Specifies the location of the response file.

/AU

Specifies to perform a silent upgrade.

Note: This argument lets you upgrade all agents installed on the local system.

/O

Specifies the location of the output file. To use this argument, you must specify the /AU argument.

After the execution is complete, all agents installed on the specified systems are upgraded to this release.

Note: If MasterSetup detects that the Arcserve Backup base product is installed on the target system, the upgrade process fails.

Examples: MasterSetup Syntax

The following example describes the syntax required to upgrade all agents installed on computer001 to this release. The user is logged in to a primary server, the user name is administrator, and the password is test-001.

```
mastersetup /h:computer001 /u:administrator /p:test-001 /au
```

The following example describes the syntax required to upgrade all agents that are installed on the local system. The user must be logged in to the target system with user account that has administrative privileges.

```
mastersetup /au
```

Deploy Agents to Remote Computers from the Primary Server

Arcserve Backup lets Backup Administrators and Backup Managers install and upgrade a collection of Arcserve Backup agents on remote computers simultaneously using the Agent Deployment wizard application. Agent Deployment verifies that you are running the most current version of a selected group of Arcserve Backup agents in your backup environment.

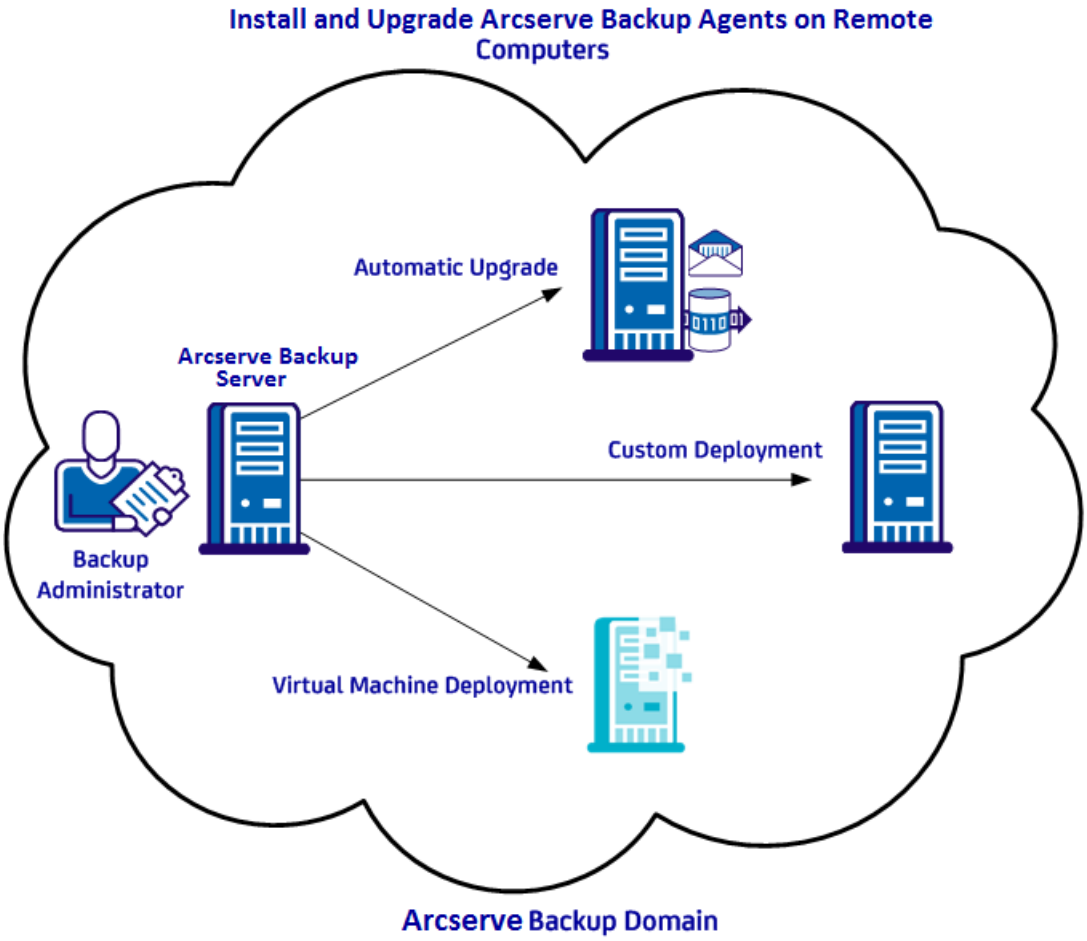
You can deploy agents to remote computers from primary servers and stand-alone servers.

Agent Deployment lets you deploy the following Arcserve Backup products:

- Arcserve Backup Agent for Microsoft Exchange Server
- Arcserve Backup Agent for Open Files
- Arcserve Backup Agent for Virtual Machines
- Arcserve Backup Client Agent for Windows
- Arcserve Backup Diagnostic Utility

Note: If Agent Deployment detects agents installed on remote computers other than the products listed above, the deployment process terminates.

The following diagram illustrates how to install and upgrade agents on remote computers:



Using Agent Deployment, you can deploy agents using the methods described in the following table:

Deployment Method	More Information
Automatic upgrade	Deploy Agents to Remote Computers Using Automatic Upgrade (see page 113)
Custom deployment	Deploy Agents to Remote Computers Using Custom Deployment (see page 115)
Virtual machine deployment	Deploy Agents to Virtual Machines Using Virtual Machine Deployment (see page 117)

Remote Deployment Considerations

Review the following before using Agent Deployment:

- Agent Deployment requires installation files that you can install on the Arcserve Backup server. This approach eliminates the need to provide the Arcserve Backup installation media when you run Agent Deployment. Agent Deployment requires approximately 1.3 GB of hard disk space and can significantly increase the length of time required to install Arcserve Backup. To eliminate the need to provide the installation media, you must explicitly select Agent Deployment Setup Files when you install Arcserve Backup.
- Do *not* use Agent Deployment to install the Agent for Microsoft Exchange Server on Exchange Client Access Servers and Hub Transport Servers.
- Agent Deployment requires that you specify the host names of the target systems. Arcserve Backup does *not* support specifying IP addresses when deploying agents to remote systems.
- Agent Deployment installs agents using their default installation path. For example, Agent Deployment installs or upgrades the Client Agent for Windows in this path (x86 systems):

  C:\Program Files\CA\ARCserve Backup Client Agent for Windows
- You must log into your computer with an account that has administrative privileges to deploy agents to remote computers.
- Verify that the administrative share on the remote computers (for example, C$, Admin$, and so on) is accessible from the server that pushes the agents.
- Verify that the firewall exception rule for File and Printing Service on the remote computers is enabled. This task is required on Windows Server 2008 systems because, by default, Windows Server 2008 firewall policy blocks File and Printing Service communication.
- To prevent the Windows firewall from blocking File and Print Sharing communication, use Domain level group policy to enable an exception to File and Print Sharing communication on all servers in your backup environment.
- On Windows XP systems, follow these steps to disable simple file sharing and verify that you can install agents on remote computers successfully:

  1. Log in to the remote Windows XP computer.

     Double-click My Computer on the desktop.
  2. Click Folder Options on the Tools menu.
  3. Click the View tab.

     Locate Use simple file sharing (recommended).

     Clear the check box next to Use simple file sharing (recommended), and click OK.

Deploy Agents to Remote Computers Using Automatic Upgrade

Arcserve Backup Agent Deployment lets Backup Administrators and Backup Managers install and upgrade Arcserve Backup agents on remote computers. Automatic upgrade lets you deploy agents to detected computers with agents that require an upgrade to this release. This method helps ensure that the release numbers of all agents running in your Arcserve Backup environment are the same as the Arcserve Backup base product.

Note: When using Automatic upgrade, you cannot specify the host name of the remote computers manually.

The Automatic upgrade method lets you deploy these agents and components:

- Arcserve Backup Agent for Microsoft Exchange Server
- Arcserve Backup Agent for Microsoft SQL Server
- Arcserve Backup Agent for Microsoft SharePoint Server
- Arcserve Backup Agent for Open Files
- Arcserve Backup Agent for Oracle
- Arcserve Backup Agent for Virtual Machines
- Arcserve Backup Client Agent for Windows
- Arcserve Backup Diagnostic Utility

Automatic upgrade must detect an agent from a previous release installed on the target computer to upgrade the agents to this release. If an agent is not detected, use the Custom deployment method to install the agents on the target computer.

Note: Before you complete the following task, see Remote Deployment Considerations (see page 112).

To deploy agents to remote computers using Automatic Upgrade

1. Open the Arcserve Backup Manager Console.

   From the Quick Start Menu, select Administration, and click Agent Deployment.

   Arcserve Backup Agent Deployment starts and the Login Server dialog opens.

2. Complete the required fields in the Login Server dialog, and click Next.

3. In the Methods dialog, click Automatic upgrade, and click Next.

   The Components dialog displays a list of computers detected by Agent Deployment that are running Arcserve Backup agents from a previous release.

4. Click Next to populate the Host Information dialog with host names, user names, and passwords for the detected computers.

5. To modify the user name and password for a remote computer, do the following:

   a. Click the check box next to a host name to select it.

   b. Click the UserName field next to the host name and type the user name in the format <*domain*>\<*user name*>.

   c. Click the Password field and type the password.

   Note: When the user name and password are the same for all remote computers, select all of the computer check boxes. Under For all selected hosts, type the user name in the User field in the format <*domain*>\<*user name*>, type the password in the Password field, then click Apply Credentials.

6. Click the Allow the Remote Registry service to run for the duration of the remote installation process option. This option lets Agent Deployment retrieve information about the target computers and verify that credentials specified are correct.

   Note: This option lets the Remote Registry service run only during the remote installation process.

7. (Optional) To remove computers from the Host and Credentials list, click the check box next to the host you want to remove, and click Remove.

8. Click Next.

   Agent Deployment validates the information specified for all specified hosts. If no authentication errors are detected, pending appears in the Status field. If an authentication error is detected, click Failed in the Status field to discover the reason. You must correct all Failed messages to continue.

9. When the Status field for all remote hosts displays Verified, click Next.

10. In the Setup Summary dialog, verify the components and the host names specified, and click Next.

11. In the Installation Status dialog, click Install, and click Next.

    Agent Deployment installs or upgrades the Arcserve Backup agents on the specified computers.

    After all upgrades are complete, the Installation Report dialog opens.

12. In the Restart dialog, click the check box next to the remote computer that you want to restart now, and click Restart.

    Optionally, click the All check box to restart all remote computers now.

    Agent Deployment restarts all of the computers.

    Note: To create a list of remote computers that require a restart, click Export Restart Report.

13. After the Status field for all remote computers displays complete, click Finish.

Deploy Agents to Remote Computers Using Custom Deployment

Arcserve Backup Agent Deployment lets Backup Administrators and Backup Managers install and upgrade Arcserve Backup agents on remote computers. Custom deployment lets you specify the agents that you want to install and upgrade on remote computers. Computers of this type may or may not have a previous version of an agent installed. This method helps ensure that the release number of all agents running in your Arcserve Backup environment are the same release number as the Arcserve Backup base product.

Using the Custom deployment method, you can deploy the following agents and components:

- Arcserve Backup Agent for Microsoft Exchange Server
- Arcserve Backup Agent for Open Files
- Arcserve Backup Agent for Virtual Machines
- Arcserve Backup Client Agent for Windows
- Arcserve Backup Diagnostic Utility

Note: Before you complete the following task, see Remote Deployment Considerations (see page 112).

To deploy agents to remote computers using Custom Deployment

1. Open the Arcserve Backup Manager Console.

   From the Quick Start Menu, select Administration, and click Agent Deployment.

   Arcserve Backup Agent Deployment starts and the Login Server dialog opens.

2. Complete the required fields in the Login Server dialog, and click Next.
3. In the Methods dialog, click Custom installation, and click Next.
4. In the Components dialog, select the agents to install on all remote computers, and click Next.

5. In the Host Information dialog, specify the names of remote hosts by doing one of the following:

   - Click Import to import a list of remote computers from a text file.

     Note: The host names must be separated the new line delimiter. You can import multiple text files, however, the total number of remote computers must be less than or equal to 1000.

   - Specify the remote host name in the Host Name field, and click Add. Repeat this step as necessary until all required host names appear in the Host column.

   Note: You can specify up to 1000 remote computers. To deploy agents to more than 1000 remote computers, restart Agent Deployment and repeat this task, or run Agent Deployment from an alternate Arcserve Backup primary server or stand-alone server.

6. Specify the user name and password for each remote host by doing the following:

   a. Click the check box next to a host name to select it.

   b. Click the UserName field next to the host name and type the user name in the format <*domain*>\<*user name*>.

   c. Click the Password field and type the password.

   Note: If the user name and password are the same for *all* remote computers, select all of the check boxes. Under For all selected hosts, type the user name in the User field in the format <*domain*>\<*user name*>, type the password in the Password field, then click Apply Credentials.

7. Click the Allow the Remote Registry service to run for the duration of the remote installation process option. This option lets Agent Deployment retrieve information about the target computers and verify that credentials specified are correct.

   Note: This option lets the Remote Registry service run only during the remote installation process.

8. (Optional) To remove a host from the Host and Credentials list, click the check box next to the host name, and click Remove.

9. Click Next.

   Agent Deployment validates the information for all specified hosts. If no authentication errors are detected, pending appears in the Status field. If an authentication error is detected, click Failed in the Status field to discover the reason. You must correct all Failed messages to continue.

10. After the Status field for all hosts displays Pending or Verified, click Next.

11. In the Setup Summary dialog, verify the components and the host names specified, and click Next.

12. In the Installation Status dialog, click Install.

    Agent Deployment installs or upgrades the Arcserve Backup agents on the specified hosts.

    After all installations and upgrades are complete, the Installation Report dialog opens.

13. Do one of the following:

    - If there are remote computers that require a restart, click Next.

      The Restart dialog opens to identify the remote computers that require a restart, and click Restart.

      Continue to the next step.

    - If there are no remote computers that require a restart, click Finish.

14. In the Restart dialog, click the check box next to the remote host that you want to restart now.

    Optionally, you can click the All check box to restart all remote computers now.

    Click Restart.

    Agent Deployment restarts all remote computers now.

    Note: To create a list of remote computers that require a restart, click Export Restart Report.

15. After the Status field for all remote computers displays complete, click Finish.

Deploy Agents to Virtual Machines Using Virtual Machine Deployment

Arcserve Backup Agent Deployment lets Backup Administrators and Backup Managers install and upgrade Arcserve Backup agents on local or remote virtual machines (VMs). The target VMs may or may not have a previous version of an agent installed. This method helps ensure that the release numbers of all agents running on the VMs in your Arcserve Backup environment are the same release number as the Arcserve Backup base product.

Using the Virtual Machine deployment method you can deploy the following agents and components:

- Arcserve Backup Agent for Open Files
- Arcserve Backup Agent for Virtual Machines
- Arcserve Backup Client Agent for Windows
- Arcserve Backup Diagnostic Utility

Be aware of the following:

- To install or upgrade an agent on a VM, the VM must be powered on.
- Agent Deployment installs or upgrades agents on all VMs that reside in the ESX/ESXi Server system and the Hyper-V host system.

Note: Before you complete the following task, see Remote Deployment Considerations (see page 112).

To deploy agents to virtual machines using Virtual Machine Deployment

1. Open the Arcserve Backup Manager Console.

   From the Quick Start Menu, select Administration and click Agent Deployment.

   Arcserve Backup Agent Deployment starts and the Login Server dialog opens.

2. Complete the required fields in the Login Server dialog, and click Next.
3. From the Methods dialog, select Virtual Machine deployment, and click Next.
4. From the Components dialog, select the agents that you want to install on all remote computers, and click Next.
5. Specify the names of remote computers that contain the VMs in the Host Information dialog by doing one of the following:

   - Click Import to import a list of remote computers from a text file.

     Note: The host names must be separated the new line delimiter. You can import multiple text files, however, the total number of remote computers must be less than or equal to 1000.

   - Click Refresh to import the existing VMs from the Arcserve Backup database.
   - Specify the remote host name in the Host Name field and click Add. Repeat this step as necessary until all required host names appear in the Host column.

   After the host names appear in the Host column, continue to the next step.

   Note: You can specify up to 1000 remote computers. To deploy agents to more than 1000 remote computers, you can restart Agent Deployment and repeat this task, or, run Agent Deployment from an alternate Arcserve Backup primary server or stand-alone server.

6. Specify the user name and password for each remote host by doing the following:

   a. Click the check box next to a host name to select it.

   b. Click the UserName field next to the host name and type the user name in the format <*domain*>\<*user name*>.

   c. Click the Password field and type the password.

   Note: If the user name and password are the same for *all* remote computers, select all of the check boxes. Under For all selected hosts, type the user name in the User field in the format <*domain*>\<*user name*>, type the password in the Password field, then click Apply Credentials.

7. Click the Allow the Remote Registry service to run for the duration of the remote installation process option. This option lets Agent Deployment retrieve information about the target computers and verify that credentials specified are correct.

   Note: This option lets the Remote Registry service run only during the remote installation process.

8. To remove a host from the Host and Credentials list, click the check box next to the host name, and click Remove.

9. Click Next.

   Agent Deployment validates the information for all specified hosts. If no authentication errors are detected, pending appears in the Status field. If an authentication error is detected, click Failed in the Status field to discover the reason. You must correct all Failed messages to continue.

10. After the Status field for all hosts displays Pending or Verified, click Next.

11. In the Setup Summary dialog, verify the components and the host names specified, and click Next.

12. In the Installation Status dialog, click Install.

    Agent Deployment installs or upgrades the Arcserve Backup agents on the specified hosts.

    After all installations and upgrades are complete, the Installation Report dialog opens.

13. Do one of the following:

    - If there are remote computers that require a restart, click Next, then click Restart.
    - If there are no remote computers that require a restart, click Finish.

14. In the Restart dialog, click the check box next to the remote host that you want to restart now, and click Restart.

    Optionally, click the All check box to restart all remote computers now.

    Note: To create a list of remote computers that require a restart, click Export Restart Report.

15. After the Status field for all remote computers displays complete, click Finish.

    The Arcserve Backup agents are deployed on the VMs.

How to Install Arcserve Backup Using Unicenter Software Delivery

MasterSetup is the main installation program for Arcserve Backup. As an alternative to using MasterSetup, you can perform a silent installation or use Unicenter Software Delivery to install Arcserve Backup components. The following sections include information about each of these alternate installation methods.

Important! You cannot install the Arcserve Backup server component (primary server, member server, and data mover server) using Unicenter Software Delivery.

This section contains the following topics:

Register Arcserve Backup on the Unicenter Software Delivery Server (see page 120)
Components and Prerequisites (see page 121)
Install Arcserve Backup Components Using Unicenter Software Delivery (see page 125)

Register Arcserve Backup on the Unicenter Software Delivery Server

Unicenter Software Delivery is a flexible tool for distributing, installing, verifying, updating, and uninstalling software from a central location. If you have Unicenter Software Delivery, you can use this tool to distribute and install Arcserve Backup. For more information on configuring and using Unicenter Software Delivery, see the Unicenter Software Delivery documentation.

Before you can use Unicenter Software Delivery to distribute and install Arcserve Backup, you must register the software on the Unicenter Software Delivery server. The following procedure describes how to register Arcserve Backup on the Unicenter Software Delivery server.

To register Arcserve Backup on the Unicenter Software Delivery server

1. Insert the Arcserve Backup installation media into your optical drive and browse to the SD Packages folder.
2. Double-click SDRegister.exe

   The Choose Product to Register dialog appears.
3. Select the individual package that you want to register.

   The License Agreement dialog appears.

   Note: You must agree to the license agreement for each product selected to continue with the registration.
4. After you select the products that you want to register, click Next to continue.

   The Unicenter Software Delivery User Details dialog appears.
5. Specify the required information in the following fields:
   - USD Server
   - User ID
   - Domain
   - Password

   Note: If you leave the above fields blank, Unicenter will attempt to register the selected products using your current system account credentials.
6. Click Next.

   All selected packages are registered and added to the Unicenter Software Delivery explorer.

Components and Prerequisites

The following tables list the components and prerequisites for the Arcserve Backup components you can register with Unicenter Software Delivery.

Arcserve Backup Client Agents for Windows

Component	Prerequisites
Windows Client Agent	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ Arcserve Installer Assistance Utility

Component	Prerequisites
Windows 64-bit Client Agent	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ Arcserve Installer Assistance Utility

Arcserve Backup Agents

Component	Prerequisites
Arcserve Backup Agent for Open Files	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Open Files 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Microsoft Exchange Server	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Microsoft Exchange Server 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility

Component	Prerequisites
Arcserve Backup Agent for Informix	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Lotus Domino	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Oracle	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Oracle 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup for Microsoft SQL Server	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup for Microsoft SQL Server 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility

Component	Prerequisites
Arcserve Backup Agent for Sybase	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Microsoft SharePoint Server	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Microsoft SharePoint Server 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility

Arcserve Backup Options

Component	Prerequisites
Arcserve Backup Enterprise Option for SAP R/3	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Enterprise Option for SAP R/3 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility

Component	Prerequisites
Arcserve Backup Agent for Virtual Machines	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility
Arcserve Backup Agent for Virtual Machines 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ Arcserve Installer Assistance Utility

The installed components have various procedures defined. Most include the following:

- Local Install: Installs the component
- Local Uninstall: Uninstalls the component

Important! Many of these components have prerequisites you must fulfill before they can be installed. You must ensure that the target computer contains the proper configuration to install and run the component. This information is available in the documentation for the individual agents and options.

Install Arcserve Backup Components Using Unicenter Software Delivery

To install Arcserve Backup components, the previously generated response file must be specified when the Unicenter Software Delivery Job is created.

Note: For information about creating a response file, see Create a Silent Installation Response File (see page 101).

To install Arcserve Backup components using Unicenter Software Delivery

1. In Unicenter Software Delivery Explorer, right-click the installation procedure you want to use.

   Drag it to the computer or group of computers you want to install it on, and select the Schedule Jobs option from the displayed menu.

   The Setup Jobs dialog appears.

2. Specify the response file in the User Parameters field on the Job Options tab, using the following syntax and arguments:

   ICFPATH={fullpath to the response file}

   Example:

   ICFPATH=\\sdo-server\sdlib$\responsefiles\setup.icf.

   sdo-server

   Specifies the Unicenter Software Delivery server.

   setup.icf

   Specifies the name of the response file that was created using MasterSetup.exe.

   When the job runs the installation program on the target computer, it reads the configuration information from the response file stored on the Unicenter Software Delivery server.

   Note: If the CA ETPKI for Windows installation fails, double-click the job to view the returns codes. If the return code is 1 or 2, you must restart the target system and then repeat this procedure.

Post-Installation Tasks

After you install or upgrade Arcserve Backup ensure that you complete the following tasks:

- If you installed agents or options that require configuration, see the appropriate agent or option guide. You can access Arcserve Backup documentation from the installation media or from the Help menu on the Arcserve Backup Manager Console.
- To ensure that all jobs start on schedule, synchronize the system time between the primary server and all of its member servers.

  Note: Use Windows Time Service to synchronize the time on all Arcserve Backup servers in your domain.
- Set up the Arcserve Backup Database Protection Job. For more information, see Start the Arcserve Backup Database Protection Job (see page 207), or the *Administration Guide*.

Chapter 5: Installing and Upgrading Arcserve Backup in a Cluster-aware Environment

This section contains the following topics:

Introduction to Cluster-aware Installations (see page 127)
Deployment Considerations (see page 127)
Plan Your Arcserve Backup HA Deployment (see page 128)
Deploy Arcserve Backup Server on MSCS (see page 130)
Deploy Arcserve Backup Server on NEC Cluster (see page 150)
How to Verify a Cluster-aware Installation and Upgrade (see page 180)

Introduction to Cluster-aware Installations

Installation of Arcserve Backup in a cluster environment with job failover capability is supported for the following cluster platforms:

- Microsoft Cluster Server (MSCS) in x86/x64 Windows Server
- CLUSTERPRO/ExpressCluster X 2.1 for Windows
- CLUSTERPRO/ExpressCluster X 3.0 for Windows
- CLUSTERPRO/ExpressCluster X 3.1 for Windows

Deployment Considerations

Before you begin to deploy Arcserve Backup into a cluster environment, you need to be aware of the following considerations:

- **Supported operating systems--**For information about supported operating systems, see the Arcserve Backup Readme file.
- **Required Cluster Resource Considerations--**As with other cluster-aware applications, the Arcserve Backup HA server needs to bind itself with some cluster resources, including a shared disk and a virtual name/IP address. Clusters resources can be grouped together to allow you to install Arcserve Backup into an existing group and bind it with the existing cluster resources already established for that group, or to create a dedicated group for Arcserve Backup deployment.

- **Special Installation/Configuration Considerations--**To deploy Arcserve Backup into all cluster nodes, you need install the same Arcserve Backup components on all nodes, and each of these components must be configured in the same way. The Arcserve Backup system accounts must be the same for all Arcserve Backup servers installed on each of the cluster nodes.

  Note: The setup program for cluster machines does not support remote installation of the Arcserve Backup base product or the Arcserve Backup agents. This remote install limitation for the Arcserve Backup agents (for example, the Agent for Microsoft SQL Server and the Agent for Microsoft Exchange Server) only applies if you use a virtual host. Remote installation of Arcserve Backup agents using the physical hosts of clusters is supported.

- **Failover Trigger Mechanism Considerations--**Arcserve Backup has its own cluster resource Dynamic Link Library functions (DLL) and scripts to extend the cluster service capabilities to monitor and detect Arcserve Backup failures. The network name and IP address of a virtual server allows Arcserve Backup to appear as a single system and take advantage of the capabilities of cluster management tools.

- **Upgrade Considerations--**To ensure that all Arcserve Backup services start properly, you must execute the cstop and cstart scripts after you complete the upgrade process and before you open the Arcserve Backup Manager Console. You must perform this task when you upgrade from Arcserve Backup r12.5 (includes the GA release and all of the latest service packs), Arcserve Backup r15 (includes the GA release and all of the latest service packs), and r16 (includes the GA release and all of the latest service packs) to this release.

  The cstop and cstart batch files are stored in the Arcserve Backup installation directory on the Arcserve Backup server.

  Note: For more information about using cstop and cstart, see the *Administration Guide*.

Plan Your Arcserve Backup HA Deployment

High availability (HA) is often associated with fault-tolerant systems, meaning a system can continue to operate in the presence of a component failure or a planned shutdown. A single component failure in a fault-tolerant system will not cause a system interruption because the alternate component will take over the task transparently. With Arcserve Backup central management the need for high availability becomes more important to provide 24x7 data protection, especially for the primary server, which plays a key role as the centralized control center for the Arcserve Backup domain.

Prior to performing cluster-aware installation of a Arcserve Backup server, you should consider the following:

Which Arcserve Backup server(s) will be deployed as cluster-aware?

Usually in a central management environment, the Arcserve Backup primary server is considered a better candidate to protect by cluster to achieve HA capability. However, clustered member servers are also supported.

Note: The setup program for cluster machines does not support remote installation of the Arcserve Backup base product or the Arcserve Backup agents. This remote install limitation for the Arcserve Backup agents (for example, the Agent for Microsoft SQL Server and the Agent for Microsoft Exchange Server) only applies if you use a virtual host. Remote installation of Arcserve Backup agents using the physical hosts of clusters is supported.

Which cluster nodes will be deployed as a Arcserve Backup HA server?

A cluster system may include several cluster nodes. In a cluster environment, you must have one node that is configured as the active node and one or more that are configured as passive nodes. Usually you would have a "one active + one passive" solution; however, it is also possible to configure a "one active + multiple passive" solution.

Where to install Arcserve Backup?

In a production environment, a cluster system might be shared by multiple cluster-aware applications. Each cluster-aware application should have its own virtual name and IP address and a dedicated shared disk. You have three choices for Arcserve Backup deployment:

- Install Arcserve Backup into a dedicated group.

  The best practice is to create a dedicated group as the container for the virtual name/IP address and shared disk, and to deploy Arcserve Backup into the new created group. The benefit of this is that the risk of failover can be limited to the group level, and not to other applications. For example, a Arcserve Backup server failover will not impact a SQL Server.

- Install Arcserve Backup into an existing group created by other applications.

  Other cluster-aware applications (such as SQL Server Cluster) will create their own groups to manage application specified resources. It is possible for Arcserve Backup to share these groups with existing applications by installing Arcserve Backup into the shared disk in the same group.

Which Arcserve Backup database type to use?

Arcserve Backup primary server supports using a local Microsoft SQL Server 2008 Express Edition installation and a local or remote Microsoft SQL Server installation as the back-end database. However, a cluster-aware primary server only supports the following scenarios:

- Microsoft SQL Server 2008 Express Edition (SQLE)

  If you do not purchase a SQL Server cluster and can accept the limitations imposed by SQL Server 2008 Express, it is the best choice.

  Note: In a MSCS cluster environment, if the Arcserve database is SQLE, the Arcserve Backup the database summary (on the Database manager) will display the physical name of the install path instead of the virtual name.

- Local Microsoft SQL Server Cluster

  If there is existing SQL Server cluster in your production environment, you can use it as the database for Arcserve Backup.

  Note: Arcserve Backup does not support local installations of Microsoft SQL Server for the Arcserve Backup database in NEC CLUSTERPRO/ExpressCluster environments.

- Remote Microsoft SQL Server

  You can also select a remote SQL Server as the Arcserve Backup database, which should safely provide 24x7 stable services.

Deploy Arcserve Backup Server on MSCS

This section contains the following topics:

MSCS Hardware Requirements (see page 131)
MSCS Software Requirements (see page 131)
MSCS Cluster Resource Preparation (see page 131)
Prepare MSCS Cluster Resources on Windows Server 2008 Systems (see page 132)
Prepare MSCS Cluster Resources on Windows Server 2012 Systems (see page 133)
Install Arcserve Backup in an MSCS Cluster-aware Environment (see page 134)
Upgrade Arcserve Backup from r12.5, r15 and r16 to r16.5 in an MSCS Cluster Environment (see page 143)
Uninstall Arcserve Backup from an MSCS Cluster (see page 147)
Delete Arcserve Backup Cluster Resources (see page 148)

MSCS Hardware Requirements

To deploy Arcserve Backup on a MSCS cluster, your system must meet the following hardware requirements:

- All cluster nodes should have identical hardware configurations (SCSI adapters, Fiber Adapters, RAID Adapters, network adapters, disk drives, for example).
- You should use separate SCSI/Fiber adapters for disk and tape devices.

  Note: You should ensure that the hardware for all nodes is similar, if not identical, to make configuration easier and eliminate any potential compatibility problems.

MSCS Software Requirements

To deploy Arcserve Backup on a MSCS cluster, your system must meet the following software requirements:

- Arcserve Backup supports cluster-aware configurations on the following operating systems:
  - Windows Server 2003 x86
  - Windows Server 2003 x64
  - Windows Server 2008 x86
  - Windows Server 2008 x64
  - Windows Server 2008 R2
  - Windows Server 2012 x64
- HA platform is configured for a MSCS cluster

MSCS Cluster Resource Preparation

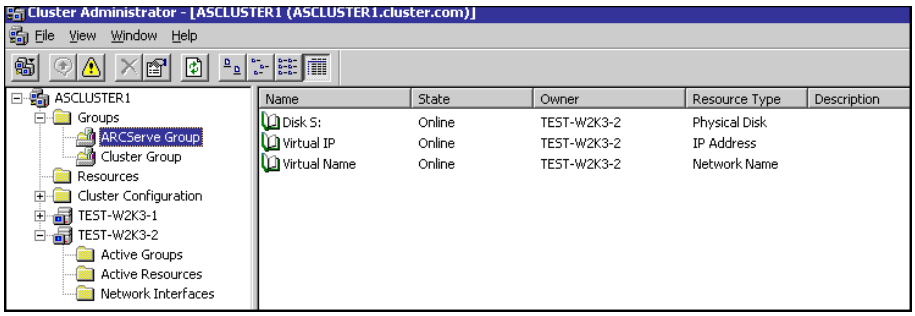
If you are installing Arcserve Backup into a dedicated group, you need to create the required resources into the new dedicated group, including a virtual IP address, virtual name, and a shared disk.

Note: Cluster Administrator (Windows Server 2003) and Failover Cluster Manager (Windows Server 2008 and Windows Server 2012) are utilities provided by Microsoft that are installed on servers that have MSCS installed. You perform most of the configuration and management tasks associated with clusters using these utilities.

In following screen example, a group named "ARCserve Group" is created for Arcserve Backup installation with three related resources on a Windows Server 2003 system:

- Shared Disk S:
- Virtual IP address
- Virtual Name

Later you can select to install Arcserve Backup into a path located in shared disk S:



If you want to share the same group with an existing application, you will not need to create new resources. In the same screen example, you can install Arcserve Backup into "Cluster Group", binding it with the quorum disk and management virtual IP address and virtual name.

Note: Cluster Group is the name of the default resource group created by MSCS during setup when the cluster is created. The Cluster Group contains a quorum disk resource, a virtual IP address, and virtual name and is used for cluster management purposes. The disk containing the quorum resource is called the quorum disk, and it must be a member of the default Cluster Group.

Prepare MSCS Cluster Resources on Windows Server 2008 Systems

On Windows Server 2008 systems, use the Failover Cluster Management utility to prepare MSCS cluster resources.

Note: On Windows Server 2008 systems, the utility is named Failover Cluster Management. On Windows Server 2008 R2 systems, the utility is named Failover Cluster Manager. The steps that follow describe how to prepare cluster resources on Windows Server 2008 systems.

To prepare MSCS cluster resources on Windows Server 2008 systems

1. From the Windows Start menu, open Failover Cluster Management.

   The High Availability Wizard, Before You Begin dialog opens.

2. Review the content on the Before You Begin dialog and click Next.

   The Failover Cluster Management window opens.

3. From the directory tree, right-click Services and applications and click Configure a server or application on the pop-up menu.

   The Select Service or Application dialog opens.

4. In the list of services and applications, click Other Server, and then click Next.

   The Client Access Point dialog opens.

5. Complete the required fields on the Client Access Point dialog. Verify that you provide the following information:

   - Name of the service
   - Public and private IP address for the location of the service

   Click Next.

   The Select Storage dialog opens.

6. Specify the the volume that you want to assign to the service or application.

   Click Next, and then click Finish.

   The cluster resource is prepared.

Prepare MSCS Cluster Resources on Windows Server 2012 Systems

On Windows Server 2012 systems, use the Failover Cluster Management utility to prepare MSCS cluster resources.

Follow these steps:

1. From the Windows Start menu, open Failover Cluster Management.
2. Right-click Roles and then click Configure Role.

   The High Availability Wizard, Before You Begin dialog opens.

3. Review the content on the Before You Begin dialog and click Next.
4. Click the Select Role option and click Other Server from the list of roles pop-up menu.

   The Client Access Point dialog opens.

5. Complete the required fields on the Client Access Point dialog. Verify that you provide the following information:

   - Name of cluster role
   - Public and private IP address for the location of the cluster role

   Click Next.

   The Select Storage dialog opens.

6. Specify the the volume that you want to assign to the cluster role.

   Click Next and the message "High availability was successfully configured for the role." appears.

   Click Finish.

   The cluster resource is prepared.

Install Arcserve Backup in an MSCS Cluster-aware Environment

You can install Arcserve Backup in an MSCS cluster-aware environment using the installation wizard.

To install Arcserve Backup in an MSCS cluster-aware environment

1. Insert the Arcserve Backup installation media into your computer's optical drive.

   Note: If the Arcserve Backup Installation Browser does not appear, run Setup.exe from the root directory on the installation media.

   From the right column on the Product Installation Browser, click Install Arcserve Backup for Windows.

   The Prerequisite Components dialog opens.

2. Click Install to install the Prerequisite Components.

   Be aware of the following behavior:

   - The Prerequisite Components dialog opens only if Setup does not detect Arcserve Backup Prerequisite Components installed on the target computer.
   - On Windows Server 2003 systems, you must restart your computer and repeat the previous steps if Setup installs Microsoft SQL Server 2008 Express Edition.

     Note: If you are installing Arcserve Backup on the active node in a cluster-aware environment, the cluster resources are transferred from the active node to the passive node while the active node restarts. After the active node restarts, you should transfer the cluster resources back to the original active node.

3. On the License Agreement dialog, accept the terms of the Licensing Agreement and click Next.

4. Follow the prompts and complete all required information on the subsequent dialogs.

   The following list describes dialog-specific information about installing Arcserve Backup.

   Select Install/Upgrade Type dialog

   When you select the remote installation option, you can install Arcserve Backup on multiple systems.

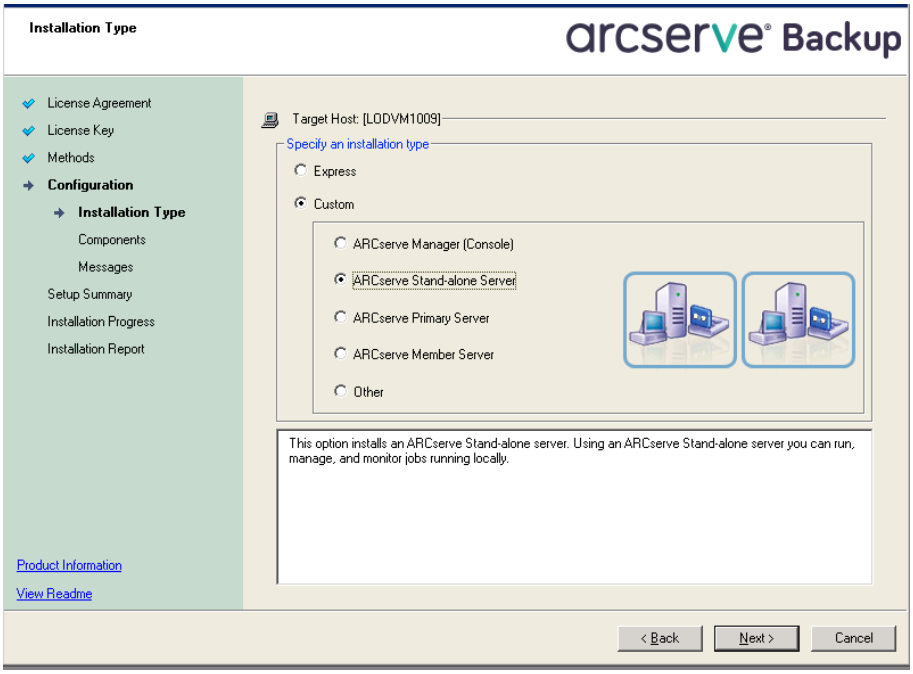
   With remote installations, the target remote systems can consist of different Arcserve server types, different Arcserve Backup agents and options, or both.

   Note: The setup program for cluster machines does not support remote installation of the Arcserve Backup base product or the Arcserve Backup agents. This remote install limitation for the Arcserve Backup agents (for example, the Agent for Microsoft SQL Server and the Agent for Microsoft Exchange Server) only applies if you use a virtual host. Remote installation of Arcserve Backup agents using the physical hosts of clusters is supported.

   Installation Type dialog

   Lets you specify the type of Arcserve Backup components that you want to install, by selecting either the Express or Custom installation type.

   Note: When you upgrade from a previous release, the installation wizard detects your current Arcserve configuration and selects the Installation/Upgrade type that is appropriate for your new installation. For more information, see Types of Arcserve Backup Server Installations (see page 41) and Arcserve Backup Server Options (see page 45).



Components dialog

Lets you specify the Arcserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the Arcserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and primary server name in your network. Therefore, you should complete at least one primary server installation before you perform member server installations.
- When you click the Arcserve Backup object or the Server object on the Select Products dialog, the installation wizard specifies the default Stand-alone Server installation components, regardless of the installation type that you specified on the Select Install/Upgrade Type dialog. To ensure that you are installing the correct components, expand the Server object, expand the object for the type of Arcserve Backup server that you want to install, and check the check boxes corresponding to the components that you want to install.
- Agent Deployment is a wizard-like application that lets you install or upgrade Arcserve Backup agents on multiple remote systems, after you install Arcserve Backup. To support this capability, Setup must copy Setup source files to the Arcserve Backup server. To copy the contents of the installation media to the Arcserve Backup server, you must select Agent Deployment on the Components dialog. When you select Agent Deployment, the length of time required to install or upgrade Arcserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the Arcserve Backup Client Agent for Windows into the same directory as the Arcserve Backup base product.
- Global Dashboard can be installed on primary servers, stand-alone servers, and member servers. However, you cannot configure member servers to function as Central Primary Servers and Branch Primary Servers. For more information about Central Primary Servers and Branch Primary Servers, see the *Dashboard User Guide*.
- On computers running Windows Server Core, you can install only the following Arcserve Backup products:

  - Member Server and supported options

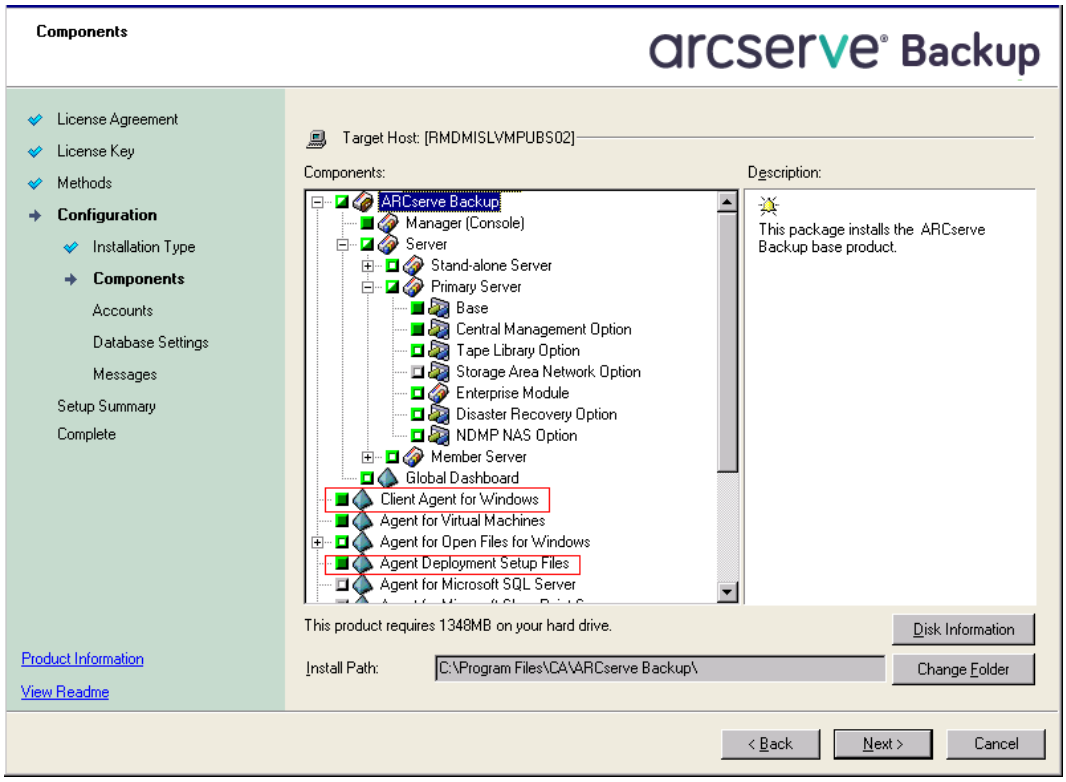
  - Agent for Open Files

  - Agent for Virtual Machines

  - Client Agent for Windows

  - Disaster Recovery Option

The following diagram illustrates the default installation path for the Client Agent for Windows and Agent Deployment is specified:

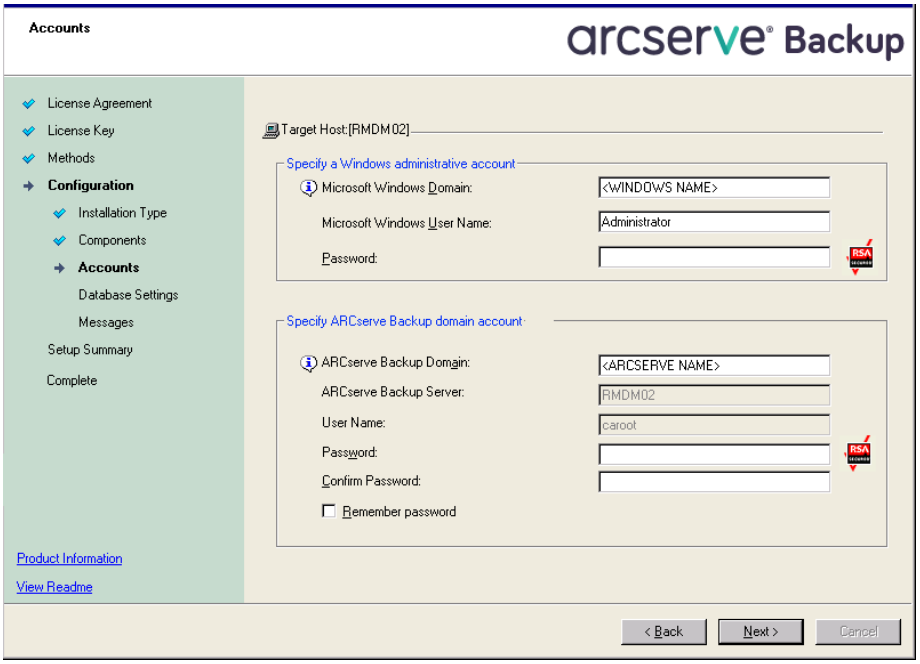


Accounts dialog

Lets you set up your Arcserve Backup accounts.

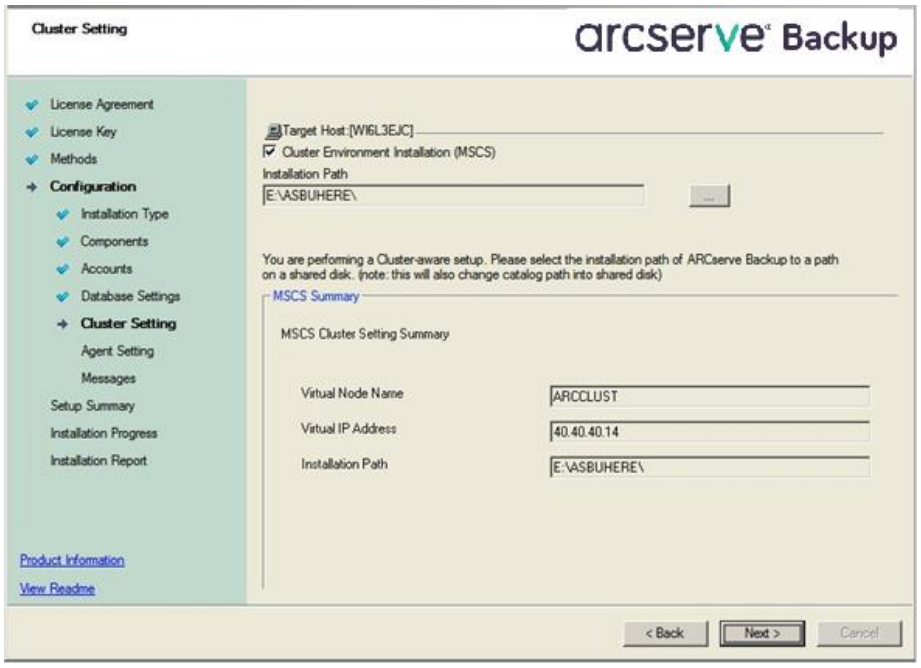
If Setup detects a cluster-aware application running in your environment, and you want to install Arcserve Backup in the cluster-aware environment, check the Cluster Environment Installation option and specify the path to the shared disk where you want to install Arcserve Backup.

Note: Arcserve Backup server names and Arcserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.



Cluster Setting dialog

The Cluster Setting dialog opens only if Setup detects that you are installing Arcserve Backup into a cluster-aware environment. You must complete all fields on this dialog to continue.



For Cluster Installations, be aware of the following database installation considerations:

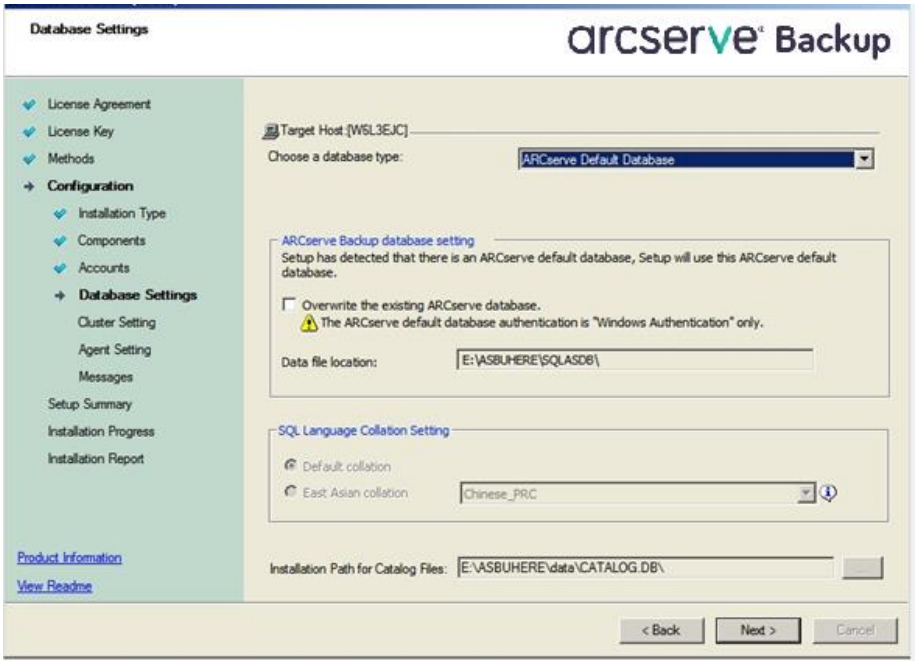
- Arcserve Backup does not support local Microsoft SQL Server installations on Arcserve Backup servers in NEC CLUSTERPRO environments. Therefore, you must install the Arcserve database instance on a remote system.
- You must specify the Remote SQL Server Type option if the Arcserve database instance and the Arcserve Backup installation will not reside in the same cluster.

Database Settings dialog

Lets you configure the Arcserve Backup database.

After you specify a database application (Arcserve Default Database or Microsoft SQL Server) complete the required fields on this dialog and click Next.

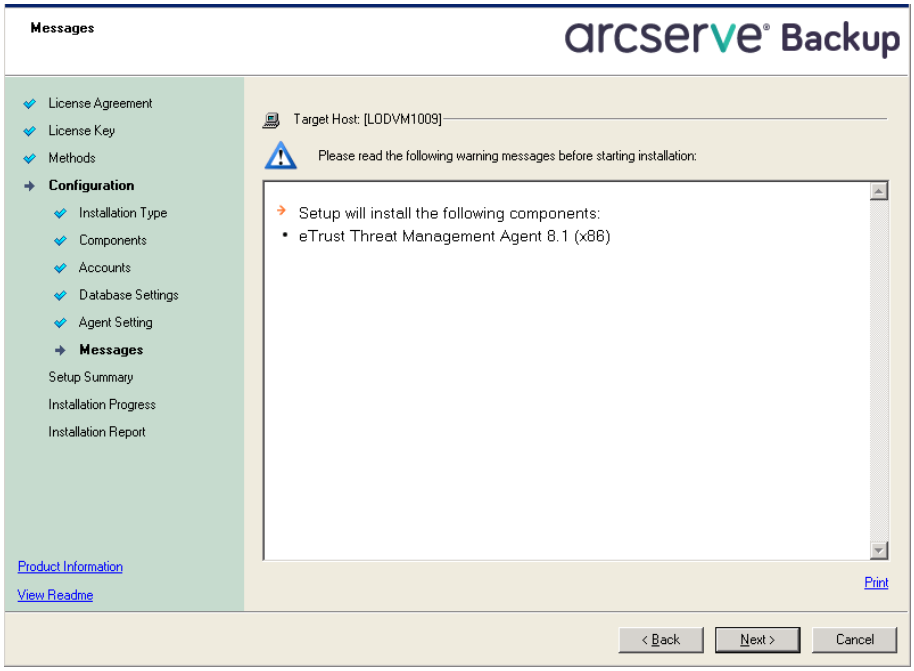
Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that Arcserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



Messages dialog

As you review the messages in the Messages dialog, you should attempt to resolve the problems at this time.

The following dialog illustrates the Messages dialog:



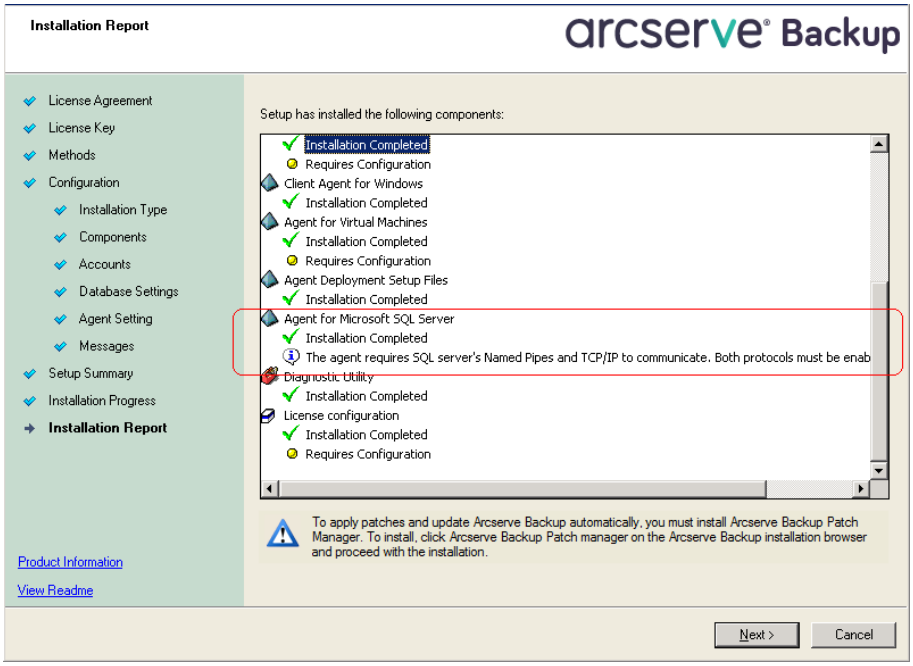
Setup Summary dialog

To modify the components that you want to install, click Back as often as necessary to return to the dialog containing the installation options that you want to change.

Installation Report dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

The diagram that follows illustrates the Installation Report dialog. The Agent for Microsoft SQL Server requires configuration.



Note: You may be required to restart the server after you install Arcserve Backup. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.

Installation Summary dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

License Verification dialog

To enter license keys, locate the components, agents, and options that you are installing, select the Use License Key option, and enter the license key for the component.

Click Continue to close the License Verification dialog.

5. Click Finish on the Installation Summary dialog to complete the installation.
6. Install Arcserve Backup on the passive node.

   Note: Repeat Steps 1 to 5 to install Arcserve Backup on the passive node.
7. Configure the cluster resources on the active and passive nodes.

   Be aware of the following:

   - On Windows Server 2003 systems, for each cluster node that Arcserve Backup will be deployed, you need to verify that the current node is set as the active node in the cluster so that it is capable of accessing the shared disk. If the current node is set as passive, you can change it to active by using the Move Group option from the Cluster Administrator.

     Cluster Administrator is a utility provided by Microsoft and is installed on servers that have MSCS installed. From the Cluster Administrator, you perform most of the configuration and management tasks associated with clusters.
   - When a cluster-aware installation is successfully finished, a post setup pop-up screen appears with an option to create HA resources. The option to create the HA resources is specified by default. You should perform this task only after Arcserve Backup is installed on the last node in the cluster.

Upgrade Arcserve Backup from r12.5, r15 and r16 to r16.5 in an MSCS Cluster Environment

This section describes the steps you must perform to upgrade Arcserve Backup r12.5, r15, r16 to r16.5 including the latest service packs, in an MSCS cluster-aware environment, to this release.

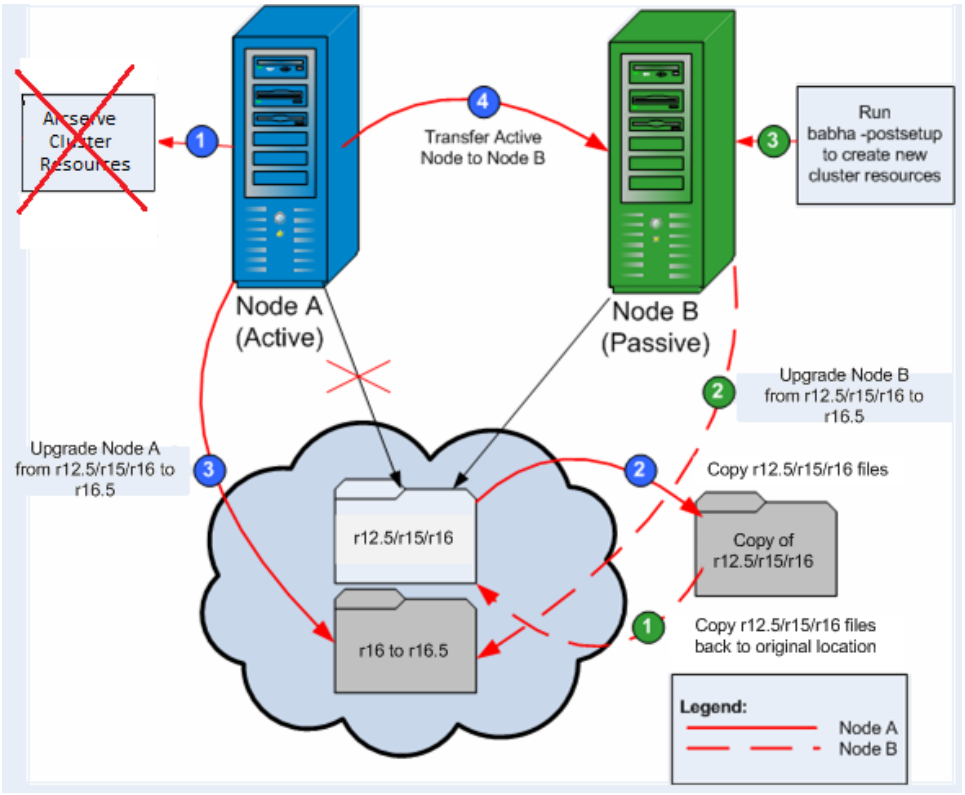
Before you begin, you should review the information in Upgrade Arcserve Backup from a Previous Release (see page 94).

When upgrading Arcserve Backup to r16.5 in an MSCS cluster environment, the following procedure must be performed to protect your clustered backup data. The procedure supports the following Arcserve Backup r12.5, r15, and r16 upgrade scenarios in an MSCS cluster environment:

- Primary server upgrade SQL Server to SQL Server
- Primary server upgrade SQL Server Express to SQL Server Express
- Member server upgrade to r16 Member server

This upgrade procedure assumes that you are operating in a two-node cluster environment, with Node A representing the initial Active Node and Node B representing the initial Passive Node.

In the diagram, the upgrade steps are illustrated.



To upgrade Arcserve Backup from r12.5, r15, r16 to r16.5 in an MSCS cluster environment

Important! Before you start the following procedure, verify that you synchronize the Arcserve Backup registry on the active node and the passive node. You can synchronize the registries using the Move Group option in the Cluster Administrator.

On Node A:

1. Delete the Arcserve cluster resources for r12.5/r15/r16 as follows:

   a. Access the Cluster Administrator.

      The Cluster Administrator dialog appears.

      Note: Cluster Administrator is a utility provided by Microsoft and is accessed from the Administrative Tools group of the Start menu.

   b. Select the Arcserve Group that the Arcserve server is deployed in, and locate the corresponding Arcserve cluster resources. Right-click on each Arcserve cluster resource and from the pop-up menu, select Delete.

   The Arcserve cluster resources for r12.5/r15/r16 are deleted.

2. Copy the Arcserve Backup r12.5/r15/r16 installation directory files into a temporary location.

   A backup copy of the Arcserve Backupr12.5/r15/r16 files is located in another location from the original files.

3. Perform Arcserve Backup r16.5 upgrade installation for Node A. See Upgrade Arcserve Backup from a Previous Release (see page 94).

   - The installation path location for Arcserve Backup r16 upgrade must be the same location where r12.5/r15/r16 is currently located.

   Arcserve Backup for Node A is upgraded from r12.5/r15/r16 to r16.5. Do not set up new Arcserve cluster resources at this time.

4. Move the active node from Node A to Node B, as follows:

   a. Access the Cluster Administrator. The Cluster Administrator opens.

   b. Select the Arcserve Group for Node A, right-click on the group name from the shortcut menu and select Move Group.

      - If there are only two nodes in the cluster, the active node status is automatically transferred from the initial active node (Node A) to the other node (Node B), making Node B the active node, and Node A the passive node.
      - If there are more than two nodes in the cluster, a pop-up screen opens, allowing you select the node to which you want to transfer the active status. When you select the node for transfer, the node you specified becomes active and the previously-selected node becomes passive. Repeat this procedure for each node in the cluster.

On Node B:

1. Copy the Arcserve Backupr12.5/r15/r16 installation directory files from the temporary location back into the original location.

   The Arcserve Backup r12.5/r15/r16 files are now located back in the original location.

2. Do one of the following:

   - Continue to the next step if you are upgrading a member server or a primary server that uses a remote deployment of Microsoft SQL Server to host the Arcserve Backup database.
   - For all other upgrades, do the following:

     a. Access the following directory on the shared disk in the cluster-aware environment:

     ARCserve_Home\SQLASDB\data

     Select all of the files in the above directory.

     Right-click the selected files and click Properties on the pop-up menu.

     The Properties dialog opens.

     b. Click the Security tab.

     Click Add and select the Network Service security group.

     Set the Network Service security group permissions to Allow Full Control.

     Click OK, and then click OK on the Properties dialog.

3. Perform Arcserve Backup r16.5 upgrade installation for Node B with the same settings selected for Node A (domain name, server type, installation path, installed options, and so on). For more information, see Upgrade Arcserve Backup from a Previous Release.

4. From the command line console, run the babha -postsetup utility to set up new Arcserve cluster resources. The babha -postsetup utility is located in the %bab_home% directory.

   The new Arcserve cluster resources (CA XOsoft WANSyncHA, Arcserve database, Arcserve Registry, and Arcserve Share) are created.

Note: Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

How to Verify a Cluster-aware Installation and Upgrade (see page 180)

Uninstall Arcserve Backup from an MSCS Cluster

Uninstalling Arcserve Backup from a cluster can only be made on the active node and must also be made for all nodes within the cluster.

To uninstall Arcserve Backup from an MSCS Cluster

1. Delete all cluster resources. For more information, see Delete Arcserve Backup Cluster Resources (see page 148).

   All Arcserve Backup cluster resources are deleted.

2. Unregister the ARCserveHA resource type by accessing the command line window and typing the following command:

   ```
   cluster restype "ARCserveHA"/delete/type
   ```

   Note: The cluster restype command is provided by Microsoft and embedded into the Windows system.

   The CA XOsoft WANSyncHA resource type is unregistered.

   For Windows Server 2012:

   Unregister the ARCserveHA resource type by accessing the Windows PowerShell and typing the following command:

   ```
   Remove-ClusterResourceType"ARCserveHA"
   ```

   Note: The Remove-clusterresourcetype command is provided by Microsoft and embedded into the Windows system.

   The CA XOsoft WANSyncHA resource type is unregistered.

3. In the active node, access the Arcserve Backup directory. Sort all files by type and then copy all the .dll files into a different location. (The recommended location for the copy is on the shared disk so that you do not have to do a network copy later).

   Note: If Arcserve Backup Global Dashboard is installed, you must also copy the directory named \GlobalDashboard and its contents to the temporary location.

   The dynamic link library (.dll) files for Arcserve Backup are copied to a different location. This lets you uninstall Arcserve Backup from each node in the cluster.

4. From the Windows Control Panel, access the Add or Remove Programs utility, and remove Arcserve Backup from the current node.

   Arcserve Backup is removed from the current (active) node.

5. Copy the .dll files back to the original location in the Arcserve Backup directory.

   Note: If you copied the directory named \GlobalDashboard and its contents to the temporary location, you must now copy this directory and its contents back to the original directory.

   The .dll files for Arcserve Backup are copied back into the Arcserve Backup directory.

6. From the Cluster Administrator, right-click on the group name and from the pop-up menu, select Move Group to change the active node.

   The status of the original node will be changed to "passive" and the status of the next node within the cluster will be changed to "active".

7. Repeat Steps 3 through 5 for all remaining nodes in the cluster.

   Arcserve Backup is removed from all nodes in the cluster.

Delete Arcserve Backup Cluster Resources

Before you can create new cluster resources, you must delete all existing cluster resources from the group where Arcserve Backup is deployed.

The available MSCS cluster resources are as follows:

- Windows Server 2003 Systems
  - CA XOsoft WANSyncHA
  - Arcserve database
  - Arcserve Registry
  - Arcserve Share
- Windows Server 2008 Systems
  - CA XOsoft WANSyncHA
  - Arcserve database
  - Arcserve Registry
- Windows Server 2012 Systems
  - CA XOsoft WANSyncHA
  - Arcserve database
  - Arcserve Registry

Follow these steps:

1. Do one of the following:

   Windows Server 2003 systems:

   - Open the Cluster Administrator.
   - Right-click the group name and click Take offline on the pop-up menu.

   Windows Server 2008 systems:

   - Open the Failover Cluster Manager.
   - Right-click the service or application name and click Take this service or application offline.

   The state of the Arcserve cluster resources is changed from Online to Offline.

   Windows Server 2012 systems:

   - Open the Failover Cluster Manager.
   - Right-click the cluster role and stop role.

   The state of the Arcserve cluster resources is changed from Online to Offline.

2. Based on the Windows Server system you use, perform one of the following options:

   - **For Windows Server 2003 or 2008 systems:**

     Select the Arcserve Group that the Arcserve server is deployed in.

   - **For Windows Server 2012 systems:**

     Select the Arcserve cluster role that the Arcserve server is deployed in.

   Locate the corresponding Arcserve cluster resources.

   Right-click each Arcserve cluster resource and click Delete on the pop-up menu.

   The selected Arcserve cluster resources are deleted.

Deploy Arcserve Backup Server on NEC Cluster

The following sections provide information about deploying Arcserve Backup on a NEC cluster. Arcserve Backup cluster support is provided for NEC CLUSTERPRO/ExpressCluster X 2.1 for Windows, NEC CLUSTERPRO/ExpressCluster X 3.0 for Windows, and NEC CLUSTERPRO/ExpressCluster X 3.1 for Windows.

Note: The following sections contain illustrations of NEC CLUSTERPRO/ExpressCluster screens that may not be up-to-date or correspond to the version of NEC CLUSTERPRO/ExpressCluster that is deployed in your environment. For more information, see the NEC CLUSTERPRO/ExpressCluster documentation.

This section contains the following topics:

NEC CLUSTERPRO/ExpressCluster Hardware Requirements (see page 150)
NEC CLUSTERPRO/ExpressCluster Software Requirements (see page 151)
NEC CLUSTERPRO/ExpressCluster Resource Preparation (see page 151)
Install Arcserve Backup in an NEC Cluster-aware Environment (see page 152)
Upgrade Arcserve Backup from r12.5, r15, and r16 to r16.5 in an NEC CLUSTERPRO Environment (see page 167)
Manage and Configure NEC CLUSTERPRO/ExpressCluster X 3.1 (see page 171)
Uninstall Arcserve Backup from an NEC CLUSTERPRO/ExpressCluster (see page 172)
Stop NEC Cluster Groups (see page 174)
Disable Arcserve Backup in NEC Cluster Scripts (see page 175)
Enable Arcserve Backup in NEC Cluster Scripts (see page 177)

NEC CLUSTERPRO/ExpressCluster Hardware Requirements

To deploy Arcserve Backup on NEC CLUSTERPRO/ExpressCluster, your system must meet the following hardware requirements:

- All cluster nodes should have identical hardware configurations (SCSI adapters, Fiber Adapters, RAID Adapters, network adapters, disk drives, for example).
- You should use separate SCSI/Fiber adapters for disk and tape devices.

  Note: You should ensure that the hardware for all nodes is similar, if not identical, to make configuration easier and eliminate any potential compatibility problems.

NEC CLUSTERPRO/ExpressCluster Software Requirements

To deploy Arcserve Backup on NEC CLUSTERPRO/ExpressCluster, your system must meet the following software requirements:

- Arcserve Backup supports cluster-aware configurations on the following operating systems:
  - Windows Server 2003 x86
  - Windows Server 2003 x64
  - Windows Server 2008 x86
  - Windows Server 2008 x64
  - Windows Server 2008 R2

The HA operating environment is configured for NEC CLUSTERPRO/ExpressCluster X 2.1 for Windows, NEC CLUSTERPRO/ExpressCluster X 3.0 for Windows, or NEC CLUSTERPRO/ExpressCluster X 3.1 for Windows.

NEC CLUSTERPRO/ExpressCluster Resource Preparation

If you are installing Arcserve Backup into a dedicated group, you need to create the required resources into the new dedicated group, including a virtual name with a floating IP address, and a shared (or mirrored) disk. To install Arcserve Backup in an NEC CLUSTERPRO/ExpressCluster environment, you must do the following:

- Before you install Arcserve Backup, create a definition and resource for the cluster. For more information about how to create a definition and resource for the cluster, see the *NEC CLUSTERPRO/ExpressCluster User's Guide*.
- After you install Arcserve Backup, add registry synchronization resources for the cluster. For more information about adding registry synchronization resources for the cluster, see Step 8 in the topic Install Arcserve Backup in an NEC Cluster-aware Environment (see page 152).

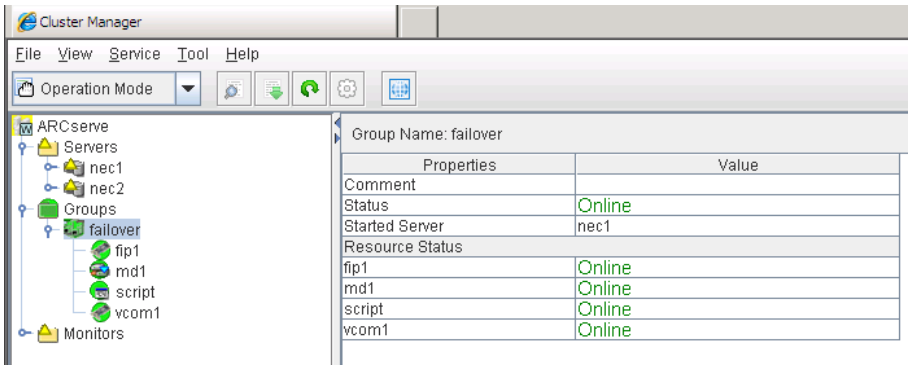
Cluster Manager and Task Manager are utilities provided by NEC and are installed on servers that have NEC CLUSTERPRO/ExpressCluster installed.

- From the Cluster Manager, you can perform most of the configuration and management tasks associated with clusters including stopping, starting, moving, and deleting cluster groups and configuring cluster properties and group resources.
- From the Task Manager, you can only stop and start each Service or Application and stop and start monitoring of each Service or Application.

In following screen example, a cluster named "ARCserve" is created for Arcserve Backup installation with four related resources:

- Floating IP address (fip1)
- Mirror disk resource (md1)
- Script (script)
- Virtual computer name (vcom1)

Later you can select to install Arcserve Backup into a path located in shared disk.



If you want to share the same group with an existing application, you will not need to create new resources.

Install Arcserve Backup in an NEC Cluster-aware Environment

You can install Arcserve Backup in an NEC cluster-aware environment using the installation wizard.

To install Arcserve Backup in an NEC cluster-aware environment

1. Insert the Arcserve Backup installation media into your computer's optical drive.

   Note: If the Arcserve Backup Installation Browser does not appear, run Setup.exe from the root directory on the installation media.

   From the right column on the Product Installation Browser, click Install Arcserve Backup for Windows.

   The Prerequisite Components dialog opens.

2. Click Install to install the Prerequisite Components.

   Be aware of the following behavior:

   - The Prerequisite Components dialog opens only if Setup does not detect Arcserve Backup Prerequisite Components installed on the target computer.
   - On Windows Server 2003 systems, you must restart your computer and repeat the previous steps if Setup installs Microsoft SQL Server 2008 Express Edition.

     Note: If you are installing Arcserve Backup on the active node in a cluster-aware environment, the cluster resources are transferred from the active node to the passive node while the active node restarts. After the active node restarts, you should transfer the cluster resources back to the original active node.

3. On the License Agreement dialog, accept the terms of the Licensing Agreement and click Next.

4. Follow the prompts and complete all required information on the subsequent dialogs.

   The following list describes dialog-specific information about installing Arcserve Backup.

   Select Install/Upgrade Type dialog

   When you select the remote installation option, you can install Arcserve Backup on multiple systems.

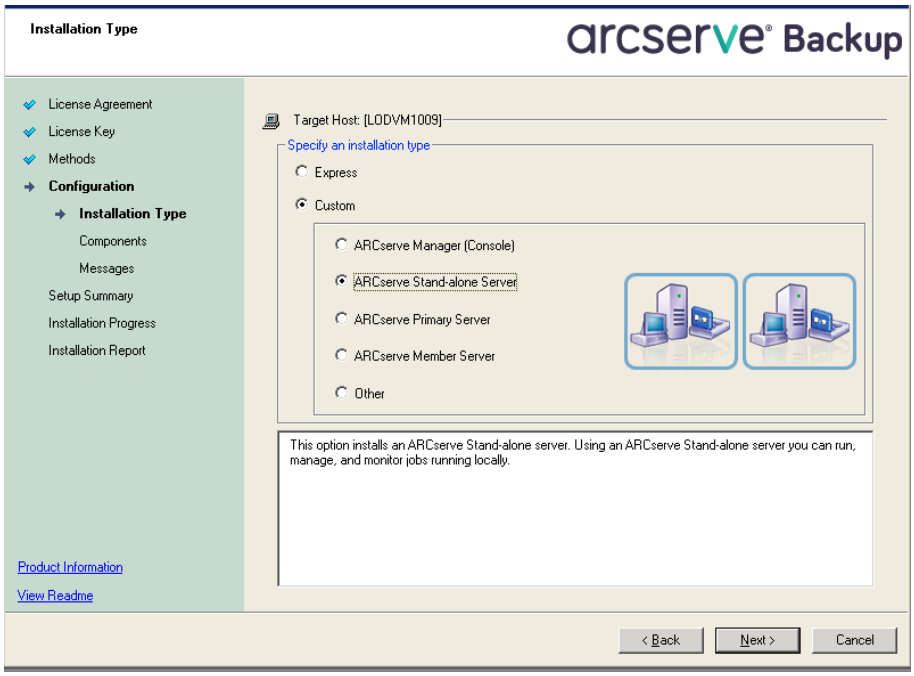
   With remote installations, the target remote systems can consist of different Arcserve server types, different Arcserve Backup agents and options, or both.

   Note: The setup program for cluster machines does not support remote installation of the Arcserve Backup base product or the Arcserve Backup agents. This remote install limitation for the Arcserve Backup agents (for example, the Agent for Microsoft SQL Server and the Agent for Microsoft Exchange Server) only applies if you use a virtual host. Remote installation of Arcserve Backup agents using the physical hosts of clusters is supported.

Installation Type dialog

Lets you specify the type of Arcserve Backup components that you want to install, by selecting either the Express or Custom installation type.

Note: When you upgrade from a previous release, the installation wizard detects your current Arcserve configuration and selects the Installation/Upgrade type that is appropriate for your new installation. For more information, see Types of Arcserve Backup Server Installations (see page 41) and Arcserve Backup Server Options (see page 45).



Components dialog

Lets you specify the Arcserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the Arcserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and primary server name in your network. Therefore, you should complete at least one primary server installation before you perform member server installations.

- When you click the Arcserve Backup object or the Server object on the Select Products dialog, the installation wizard specifies the default Stand-alone Server installation components, regardless of the installation type that you specified on the Select Install/Upgrade Type dialog. To ensure that you are installing the correct components, expand the Server object, expand the object for the type of Arcserve Backup server that you want to install, and check the check boxes corresponding to the components that you want to install.
- Agent Deployment is a wizard-like application that lets you install or upgrade Arcserve Backup agents on multiple remote systems, after you install Arcserve Backup. To support this capability, Setup must copy Setup source files to the Arcserve Backup server. To copy the contents of the installation media to the Arcserve Backup server, you must select Agent Deployment on the Components dialog. When you select Agent Deployment, the length of time required to install or upgrade Arcserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the Arcserve Backup Client Agent for Windows into the same directory as the Arcserve Backup base product.
- Global Dashboard can be installed on primary servers, stand-alone servers, and member servers. However, you cannot configure member servers to function as Central Primary Servers and Branch Primary Servers. For more information about Central Primary Servers and Branch Primary Servers, see the *Dashboard User Guide*.
- On computers running Windows Server Core, you can install only the following Arcserve Backup products:

  - Member Server and supported options

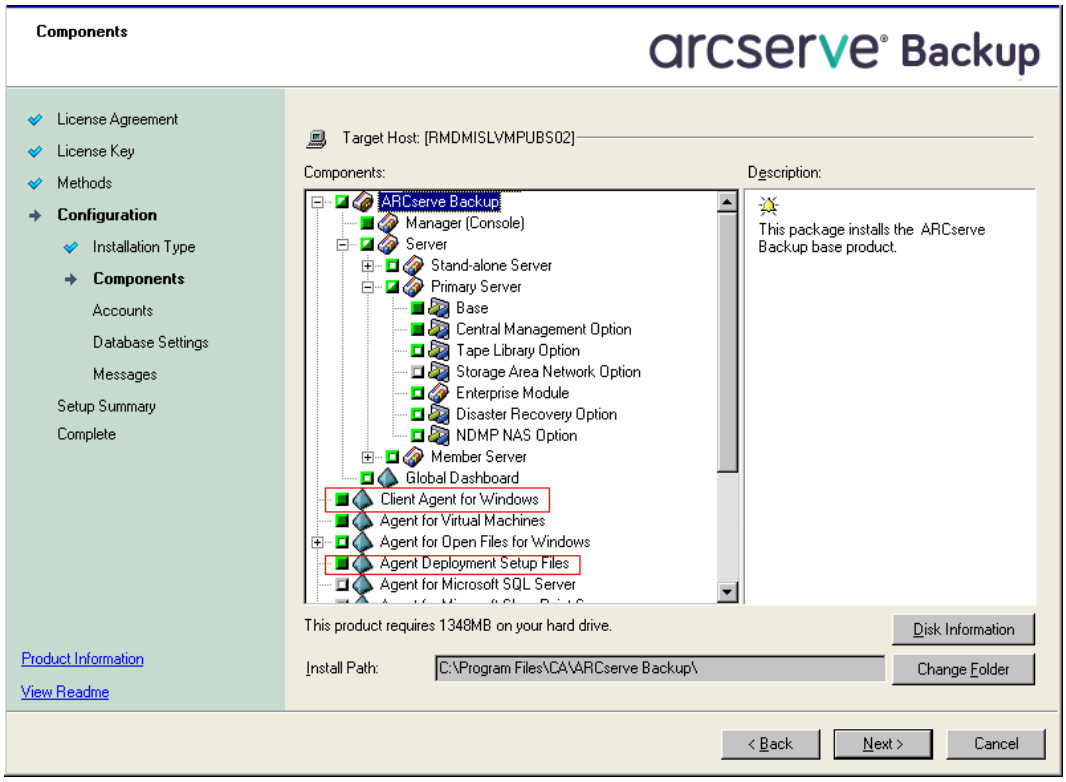
  - Agent for Open Files

  - Agent for Virtual Machines

  - Client Agent for Windows

  - Disaster Recovery Option

The following diagram illustrates the default installation path for the Client Agent for Windows and Agent Deployment is specified:

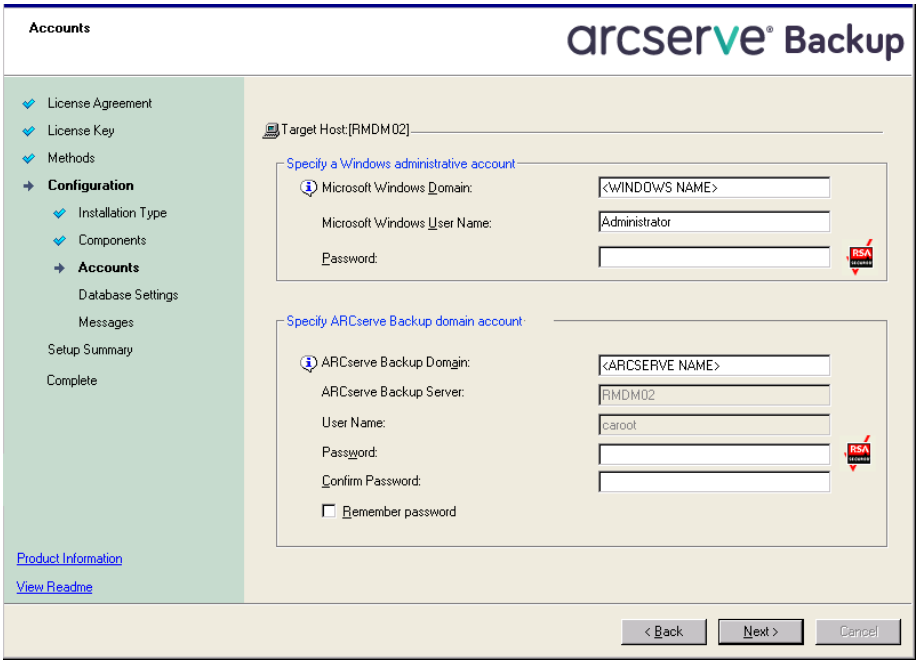


Accounts dialog

Lets you set up your Arcserve Backup accounts.

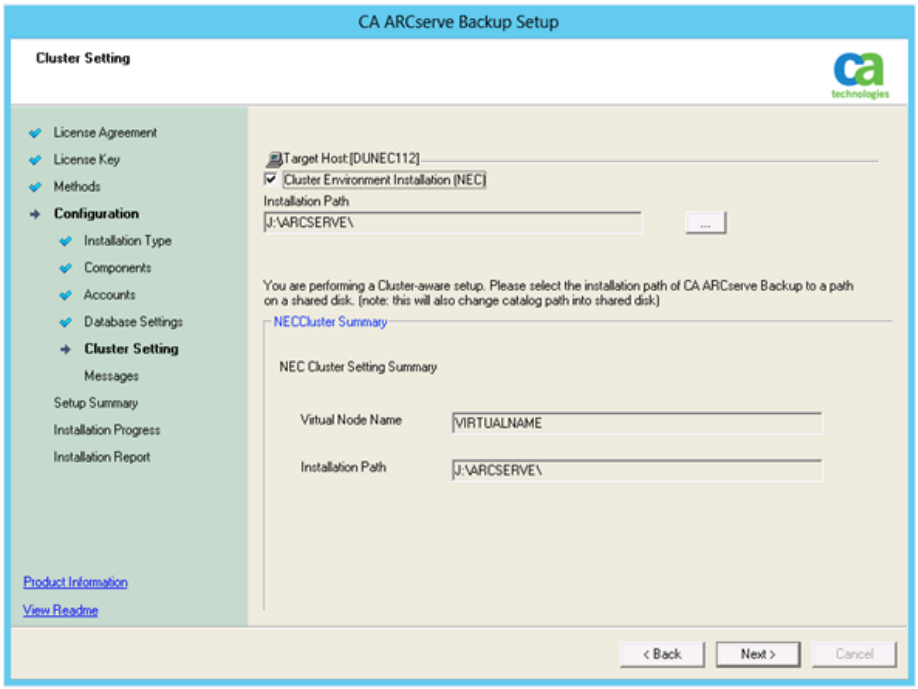
If Setup detects a cluster-aware application running in your environment, and you want to install Arcserve Backup in the cluster-aware environment, check the Cluster Environment Installation option and specify the path to the shared disk where you want to install Arcserve Backup.

Note: Arcserve Backup server names and Arcserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.



Cluster Setting dialog

The Cluster Setting dialog opens only if Setup detects that you are installing Arcserve Backup into a cluster-aware environment. You must complete all fields on this dialog to continue.

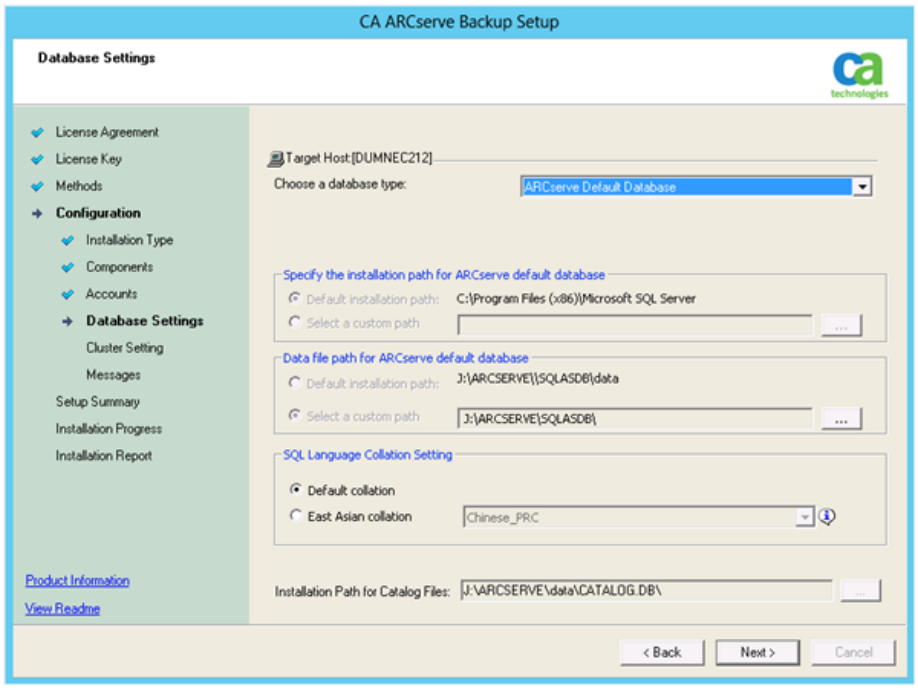


Database Settings dialog

Lets you configure the Arcserve Backup database.

After you specify a database application (ARCserve Default Database or Microsoft SQL Server) complete the required fields on this dialog and click Next.

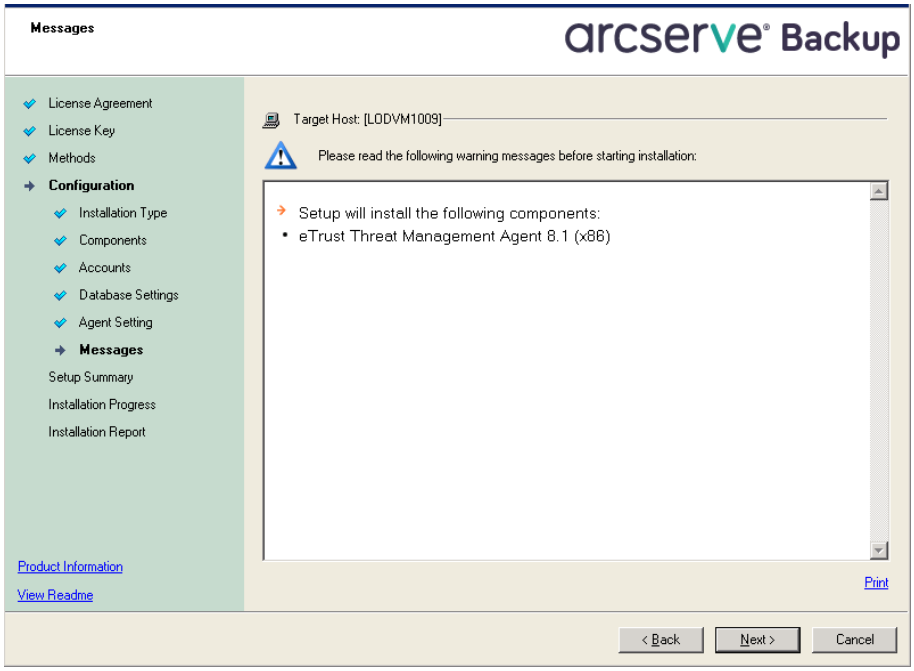
Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that Arcserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



Messages dialog

As you review the messages in the Messages dialog, you should attempt to resolve the problems at this time.

The following dialog illustrates the Messages dialog:



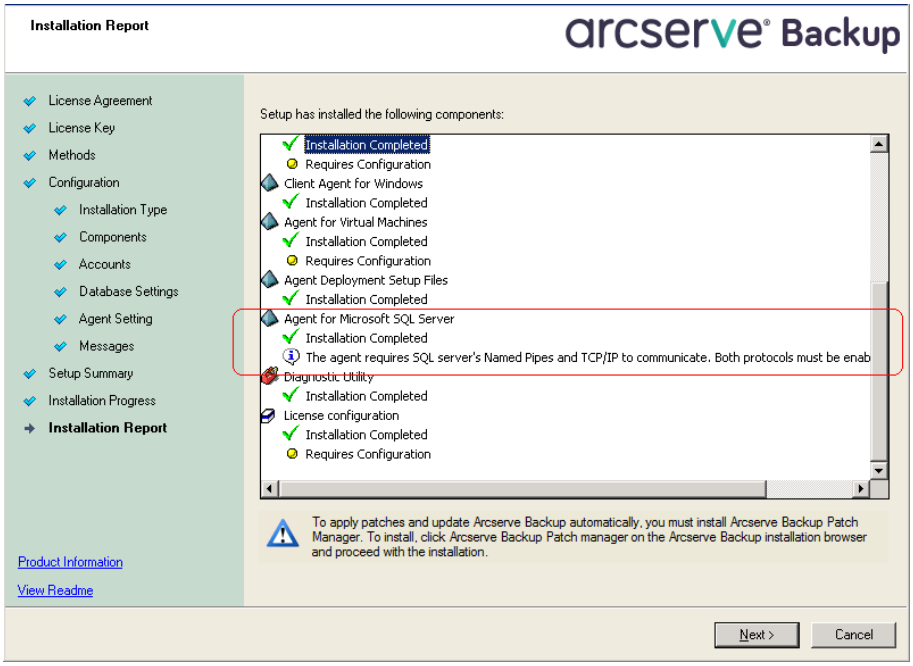
Setup Summary dialog

To modify the components that you want to install, click Back as often as necessary to return to the dialog containing the installation options that you want to change.

Installation Report dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

The diagram that follows illustrates the Installation Report dialog. The Agent for Microsoft SQL Server requires configuration.



Note: You may be required to restart the server after you install Arcserve Backup. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.

Installation Summary dialog

If any components you select require configuration, Setup displays the necessary configuration dialogs at the end of the installation. You can configure the component immediately or configure it later using Device Configuration or Enterprise Module Configuration. For example, if you are using a single-drive autoloader that requires configuration, Setup lets you start Device Configuration by double-clicking the message for it on the Install Summary dialog.

License Verification dialog

To enter license keys, locate the components, agents, and options that you are installing, select the Use License Key option, and enter the license key for the component.

Click Continue to close the License Verification dialog.

5. Click Finish on the Installation Summary dialog to complete the installation.
6. Install Arcserve Backup on the passive node.

   Note: Repeat Steps 1 to 5 to install Arcserve Backup on the passive node.
7. For each cluster node that Arcserve Backup will be deployed, you need to verify that the current node is set as the active node in the cluster so that it is capable of accessing the shared disk. If the current node is set as passive, you can change it to active by using the Move Group option from the Cluster Manager.

   After the cluster-aware installation is successfully finished, edit start.bat and stop.bat from details in the script resource for the applicable server:

   - For all member servers and non-SQL Server Express Edition primary servers, use the start.bat scripts contained in start.bat Script Changes for Member Servers and Non-SQL Express Primary Servers (see page 163).
   - For all member servers and non-SQL Server Express Edition primary servers, use the stop.bat scripts contained in stop.bat Script Changes for Member Servers and Non-SQL Express Primary Servers (see page 164).
   - For only SQL Server Express Edition primary servers, use the start.bat script contained in start.bat Script Changes for SQL Express Primary Servers (see page 165).
   - For only SQL Server Express Edition primary servers, use the stop.bat script contained in stop.bat Script Changes for SQL Express Primary Servers (see page 166).
8. Create registry synchronization resources for the failover group where the Arcserve Backup server is deployed:

   On x86 platforms, add the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe Backup\Base

   On x64 platforms, add the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\Base

start.bat Script Changes for Member Servers and Non-SQL Express Primary Servers

After installation, you need to modify the start.bat script by adding text in two locations: after NORMAL and after FAILOVER. The following script changes apply only to member servers and non-SQL Express primary servers.

Copy the following script and paste it in the start.bat file after NORMAL and after FAILOVER:

```
REM Set the following variable 'process' to 1 for normal
REM operation. During upgrade / migration, modify this
REM script to set the value to zero
SET process=1

REM Set this flag to 1 if it's a primary server and using
REM MS SQL Express 2008 database, otherwise set it to 0
SET PRIMARY_SQLE_FLAG=0

IF %process%==0 GOTO end

REM Do normal processing here

net stop CASDiscovery
net stop CASSvcControlSvr

if %PRIMARY_SQLE_FLAG%==0 GOTO CA_SERVICES
net start mssql$arcserve_db

:CA_SERVICES
net start CASDiscovery
net start CAsportmappe
armload CASSvcControlSvr /S /R 3 /FOV CASSvcControlSvr
armload CASunivDomainSvr /S /R 3 /FOV CASunivDomainSvr
armload CASDBEngine /S /R 3 /FOV CASDBEngine
armload CASMessageEngine /S /R 3 /FOV CASMessageEngine
armload CASTapeEngine /S /R 3 /FOV CASTapeEngine
armload CASJobEngine /S /R 3 /FOV CASJobEngine
armload CASMgmtSvc /S /R 3 /FOV CASMgmtSvc
net start "CA ARCserve Communication Foundation"
net start CA_ARCserve_RemotingServer
net start CADashboardSync
net start "CA ARCserve Communication Foundation (Global)"

:end
REM Exit out of the batch file
```

stop.bat Script Changes for Member Servers and Non-SQL Express Primary Servers

After installation, you need to modify the stop.bat script by adding text in two locations: after NORMAL and after FAILOVER. The following script changes apply only to member servers and non-SQL Express primary servers.

Copy the following script and paste it in the stop.bat file after NORMAL and after FAILOVER:

```
REM Set the following variable 'process' to 1 for normal
REM operation. During upgrade / migration, modify this
REM script to set the value to zero
SET process=1

REM Set this flag to 1 if it's a primary server and using
REM MS SQL Express 2008 database, otherwise set it to 0
SET PRIMARY_SQLE_FLAG=0

REM Set the ARCServe home directory here
SET ARCSERVE_HOME=s:\arcserve_home

IF %process%==0 GOTO end

REM Do normal processing here
armsleep 2
armkill  CASJobEngine
%ARCSERVE_HOME%\babha.exe -killjob
armkill CASMgmtSvc
armkill CASTapeEngine
armkill CASDBEngine
armkill CASMessageEngine
armkill CASunivDomainSvr
armkill CASSvcControlSvr
net stop "CA ARCserve Communication Foundation (Global)"
net stop CADashboardSync
net stop CA_ARCServe_RemotingServer
net stop "CA ARCserve Communication Foundation"
net stop CAsportmapper

if %PRIMARY_SQLE_FLAG%==0 GOTO end
net stop mssql$arcserve_db

:end
REM Exit out of the batch file
```

start.bat Script Changes for SQL Express Primary Servers

After installation, you need to modify the start.bat script by adding text in two locations: after NORMAL and after FAILOVER. The following script changes apply only to SQL Express primary servers.

Copy the following script and paste it in the start.bat file after NORMAL and after FAILOVER:

```
REM Set the following variable 'process' to 1 for normal
REM operation. During upgrade / migration, modify this
REM script to set the value to zero
SET process=1

REM Set this flag to 1 if it's a primary server and using
REM MS SQL Express 2008 database, otherwise set it to 0
SET PRIMARY_SQLE_FLAG=1

IF %process%==0 GOTO end

REM Do normal processing here

net stop CASDiscovery
net stop CASSvcControlSvr

if %PRIMARY_SQLE_FLAG%==0 GOTO CA_SERVICES
net start mssql$arcserve_db

:CA_SERVICES
net start CASDiscovery
net start CASportmappe
armload CASSvcControlSvr /S /R 3 /FOV CASSvcControlSvr
armload CASunivDomainSvr /S /R 3 /FOV CASunivDomainSvr
armload CASDBEngine /S /R 3 /FOV CASDBEngine
armload CASMessageEngine /S /R 3 /FOV CASMessageEngine
armload CASTapeEngine /S /R 3 /FOV CASTapeEngine
armload CASJobEngine /S /R 3 /FOV CASJobEngine
armload CASMgmtSvc /S /R 3 /FOV CASMgmtSvc
net start "CA ARCserve Communication Foundation"

:end
REM Exit out of the batch file
```

stop.bat Script Changes for SQL Express Primary Servers

After installation, you need to modify the stop.bat script by adding text in two locations: after NORMAL and after FAILOVER. The following script changes apply only to SQL Express primary servers.

Copy the following script and paste it in the stop.bat file after NORMAL and after FAILOVER:

```
REM Set the following variable 'process' to 1 for normal
REM operation. During upgrade / migration, modify this
REM script to set the value to zero
SET process=1

REM Set this flag to 1 if it's a primary server and using
REM MS SQL Express 2008 database, otherwise set it to 0
SET PRIMARY_SQLE_FLAG=1

REM Set the ARCServe home directory here
SET ARCSERVE_HOME=s:\arcserve_home

IF %process%==0 GOTO end

REM Do normal processing here
armsleep 2
armkill  CASJobEngine
%ARCSERVE_HOME%\babha.exe -killjob
armkill CASMgmtSvc
armkill CASTapeEngine
armkill CASDBEngine
armkill CASMessageEngine
armkill CASunivDomainSvr
armkill CASSvcControlSvr
net stop "CA ARCserve Communication Foundation"
net stop CAsportmapper

if %PRIMARY_SQLE_FLAG%==0 GOTO end
net stop mssql$arcserve_db

:end
REM Exit out of the batch file
```

Upgrade Arcserve Backup from r12.5, r15, and r16 to r16.5 in an NEC CLUSTERPRO Environment

This section describes the steps you must perform to upgrade r12.5, r15, and r16 including the latest service packs, in an MSCS cluster-aware environment, to this release.

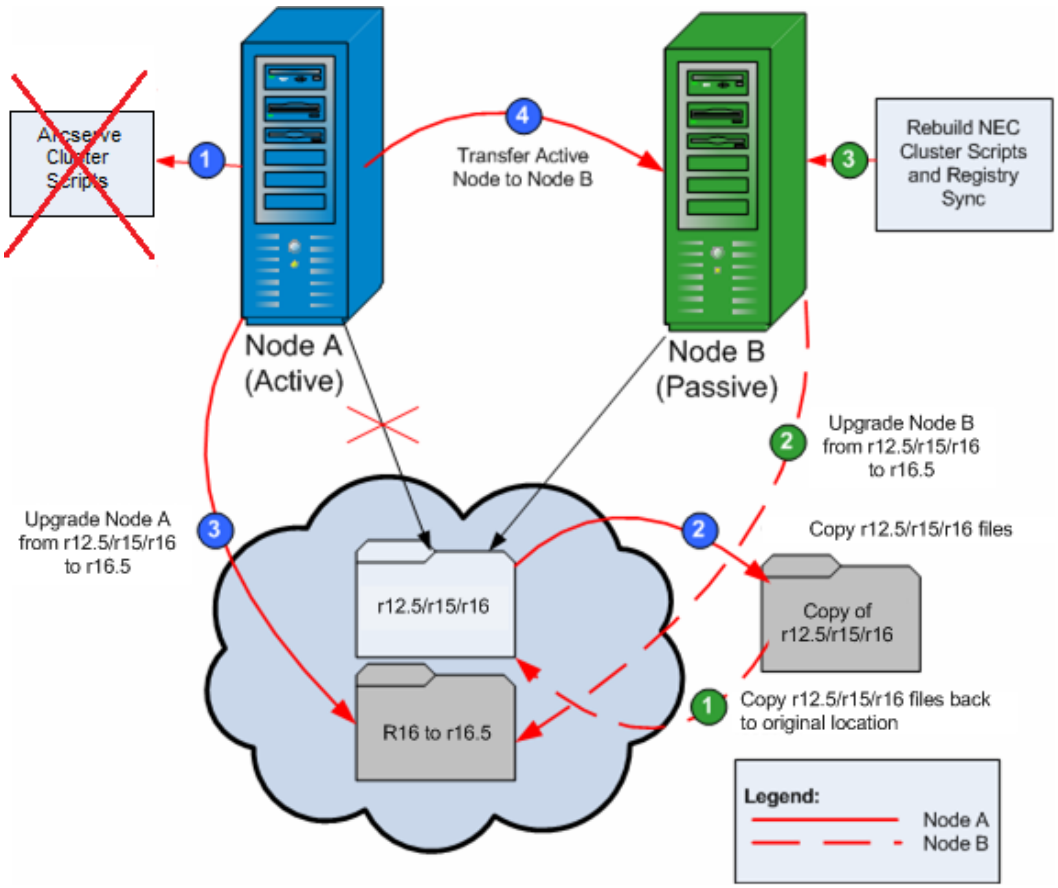
Before you begin, you should review the information in Upgrade Arcserve Backup from a Previous Release (see page 94).

When upgrading Arcserve Backup from r12.5/r15/r16 to r16.5 in an NEC CLUSTERPRO environment, the following procedure must be performed to safely protect your clustered backup data. If you are not already using Arcserve Backupr12.5/r15/r16 in a cluster environment, you do not need to perform this procedure. The procedure supports the following Arcserve Backup r12.5/r15/r16 upgrade scenarios in an NEC CLUSTERPRO environment:

- Primary server upgrade SQL Server to SQL Server
- Primary server upgrade SQL Server Express to SQL Server Express
- Member server upgrade to r16 Member server

This upgrade procedure is assuming you are operating in a two-node cluster environment, with Node A representing the initial Active Node and Node B representing the initial Passive Node.

In the diagram, the upgrade steps are illustrated.



To upgrade Arcserve Backup from r12.5/r15/r16 to r16.5 in an NEC CLUSTERPRO environment

On Node A:

1. Disable the NEC Cluster Scripts and delete the Registry Sync. For more information, see Disable Arcserve Backup in NEC Cluster Scripts (see page 175).
2. Copy the Arcserve Backup r12.5/r15/r16 installation directory files into a temporary location.

   A backup copy of the Arcserve Backup r12.5/r15/r16 files is located in a different location from the original files.

3. Perform Arcserve Backup r16.5 upgrade installation for Node A. For more information, see Upgrade Arcserve Backup from a Previous Release (see page 94).

   The installation path location for the Arcserve Backup r16.5 upgrade must be the same location where r12.5/r15/r16 is currently installed.

   Arcserve Backup for Node A is upgraded from r12.5/r15/r16 to r16.5. Do not set up new Arcserve cluster resources at this time.

4. Move the active node from Node A to Node B, as follows:

   a. Access the Cluster Manager. The Cluster Manager dialog opens.

      Note: Cluster Manager is a utility provided by NEC and is installed on servers that have NEC CLUSTERPRO installed. Cluster Manager is accessed from the NEC ExpressCluster Server group of the Start menu. From Cluster Manager, you can perform most of the configuration and management tasks associated with clusters.

   b. Select the NEC Group in which the Arcserve server is deployed and locate the corresponding Arcserve cluster resources. Right-click on each Arcserve cluster resource and select Move Group from the shortcut menu.

      - If there are only two nodes in the cluster, the active node status is automatically transferred from the initial active node (Node A) to the other node (Node B), making Node B active and Node A passive.
      - If there are more than two nodes in the cluster, a pop-up screen opens, allowing you to select the node to which you want to transfer the active status. When you select the node for transfer, the node you specified becomes active and the previously-selected node becomes passive. Repeat this procedure for each node in the cluster.

On Node B:

1. Copy the Arcserve Backup r12.5/r15/r16 installation directory files from the temporary location back into the original location.

   The Arcserve Backupr12.5/r15/r16 files are now located back in the original location.

2. Do one of the following:

   - Continue to the next step if you are upgrading a member server or a primary server that uses a remote deployment of Microsoft SQL Server to host the Arcserve Backup database.
   - For all other upgrades, do the following:

     a. Access the following directory on the shared disk in the cluster-aware environment:

     ARCserve_Home\SQLASDB\data

     Select all of the files in the above directory.

     Right-click the selected files and click Properties on the pop-up menu.

     The Properties dialog opens.

     b. Click the Security tab.

     Click Add and select the Network Service security group.

     Set the Network Service security group permissions to Allow Full Control.

     Click OK, and then click OK on the Properties dialog.

3. Perform Arcserve Backup r16.5 upgrade installation for Node B with the same settings selected for Node A (domain name, server type, install path, installed options, and so on). For more information, see Upgrade Arcserve Backup from a Previous Release.

4. Rebuild the NEC Cluster Scripts and Registry Sync. For more information, see Enable Arcserve Backup in NEC Cluster Scripts.

   The new NEC HA scripts are created and the registry is synchronized.

Note: Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

How to Verify a Cluster-aware Installation and Upgrade (see page 180)

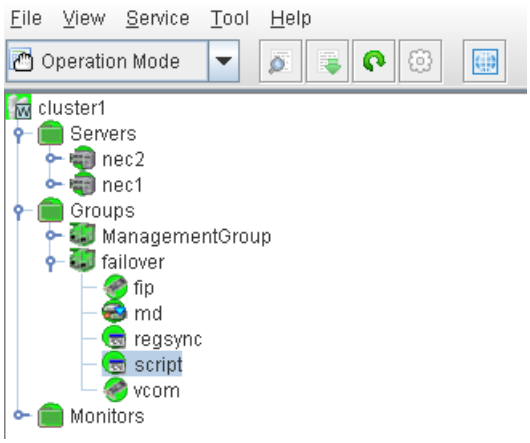
Manage and Configure NEC CLUSTERPRO/ExpressCluster X 3.1

In NEC CLUSTERPRO/ExpressCluster X 3.1 (Cluster 3.1), the Cluster Manager and the Cluster Builder are consolidated into one GUI called the Web Manager. For the Web manager, you can perform all tasks such as creating, configuring, and managing both the cluster and failover groups in Cluster 3.1.

To open the Web Manager enter the URL, such as http://10.0.0.3:29003/ from any server of the cluster in the address bar of a web browser and press Enter.

Follow these steps:

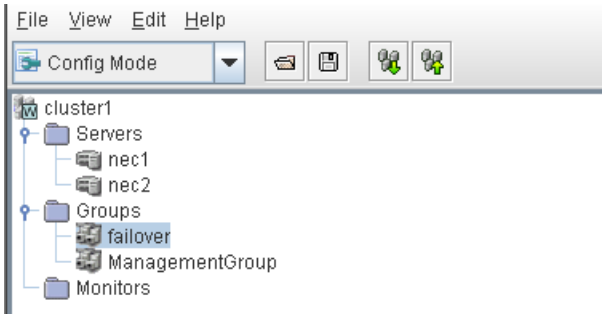
1. Manage NEC CLUSTERPRO/ExpressCluster X 3.1 by selecting the Operation Mode from the Web Manager.



In this mode, you can perform the following operational tasks for the cluster and the failover groups:

- Manage the cluster, such as to start, stop, suspend, resume, or restart the cluster.
- Manage the servers (nodes) in the cluster, such as to start or stop the cluster service on the nodes or to shutdown or reboot the nodes.
- Manage the failover groups in the cluster, such as start or stop the groups or move the groups among servers.
- Start or stop resources in the failover groups.

2. Configure NEC CLUSTERPRO/ExpressCluster X 3.1 by selecting the Config Mode from the Web Manager.



   In this mode, you can perform the following configuration tasks for the cluster and the failover groups:

   - Configure the cluster.
   - Add or remove servers to/from the cluster.
   - Configure the servers.
   - Add, remove, or configure failover groups.
   - Add, remove, or configure resources in the failover groups.

3. Once completed, select File > Apply the Configuration File, in order for the configuration tasks to take effect.
4. Select Tool > Reload from the Operation Mode menu to load the configuration to the cluster manager.

Uninstall Arcserve Backup from an NEC CLUSTERPRO/ExpressCluster

Uninstalling Arcserve Backup from a cluster can only be made on the active node and must also be made for all nodes within the cluster.

To uninstall Arcserve Backup from an NEC CLUSTERPRO/ExpressCluster

1. Stop the failover group that the Arcserve Backup server is deployed in and then suspend the cluster group.

   Note: For more information, see Stop NEC Cluster Groups (see page 174).

2. Remove the registry sync and edit the start.bat and stop.bat scripts to disable Arcserve Backup scripts added during installation. For more information, see Disable Arcserve Backup in NEC Cluster Scripts (see page 175).
3. Resume the cluster group and then start the failover group.

4. Access the Arcserve Backup home directory. Sort all files by type and then copy all the .dll files into a temporary location. (The recommended location for the copy is on the share disk so that you do not have to do a network copy later).

   Important! Verify that the current node for the .dll files being backed up is set as the active node.

   The dynamic-link library (.dll) files for Arcserve Backup are copied to a different location. This lets you uninstall Arcserve Backup from each node in the cluster.

5. (Optional) If Arcserve Backup Global Dashboard is installed, copy the directory named \GlobalDashboard and its contents to the temporary location.

6. From the Windows Control Panel, access the Add or Remove Programs utility, and remove Arcserve Backup from the current node.

   Arcserve Backup is removed from the current (active) node.

7. Copy the .dll files back into the original location in the Arcserve Backup home directory.

   The .dll files for Arcserve Backup are copied back into the Arcserve Backup home directory.

8. (Optional) If you copied the directory named \GlobalDashboard and its contents to the temporary location, copy the directory and its contents from the temporary location back to the original directory.

9. From the Cluster Manager, right-click on the group name and from the pop-up menu, select Move Group to change the active node.

   The status of the original node updates to offline (passive) and the status of the next node within the cluster updates to online (active).

10. Repeat Steps 6 through 9 for all remaining nodes in the cluster.

    Arcserve Backup is uninstalled from all nodes in the cluster.

Stop NEC Cluster Groups

If you need to edit the group properties (for example to edit the start.bat or stop.bat files, or remove or add registry sync) you must first stop the group. In addition, if you need to remove Arcserve Backup from NEC CLUSTERPRO/ExpressCluster, you must also stop the group.

Note: This section contains graphics that correspond with NEC CLUSTERPRO/ExpressCluster version 8.0. If you are running a more recent version of NEC CLUSTERPRO/ExpressCluster, see your NEC CLUSTERPRO/ExpressCluster documentation.

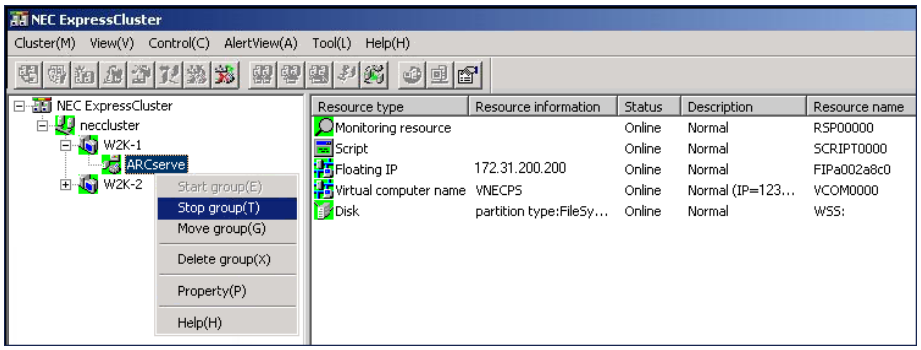
To stop the NEC cluster group

1. Access the Cluster Manager.

   The Cluster Manager window appears.

2. From the tree listing, right-click on the Arcserve group, and from the pop-up menu select Stop group.

   A confirmation pop-up screen appears.



3. Click OK.

   The selected group is stopped.

Disable Arcserve Backup in NEC Cluster Scripts

Cluster scripts and registry keys are inserted during the NEC post-setup process. When upgrading from a previous release, the cluster scripts need to be disabled and the registry key need to be deleted.

Note: This section contains graphics that correspond with NEC CLUSTERPRO/ExpressCluster version 8.0. If you are running a more recent version of NEC CLUSTERPRO/ExpressCluster, see your NEC CLUSTERPRO/ExpressCluster documentation.

To disable Arcserve Backup in NEC cluster scripts

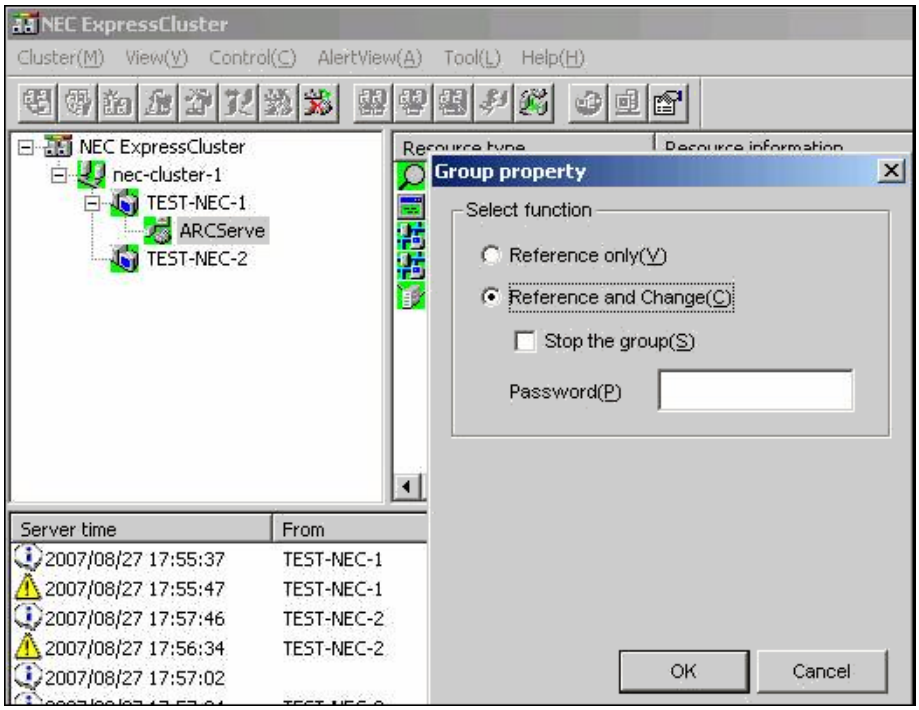
1. Access the Cluster Manager.

   The Cluster Manager window appears.

   Note: Cluster Manager is a utility provided by NEC and is installed on servers that have NEC CLUSTERPRO/ExpressCluster installed. From the Cluster Manager, you perform most of the configuration and management tasks associated with clusters.

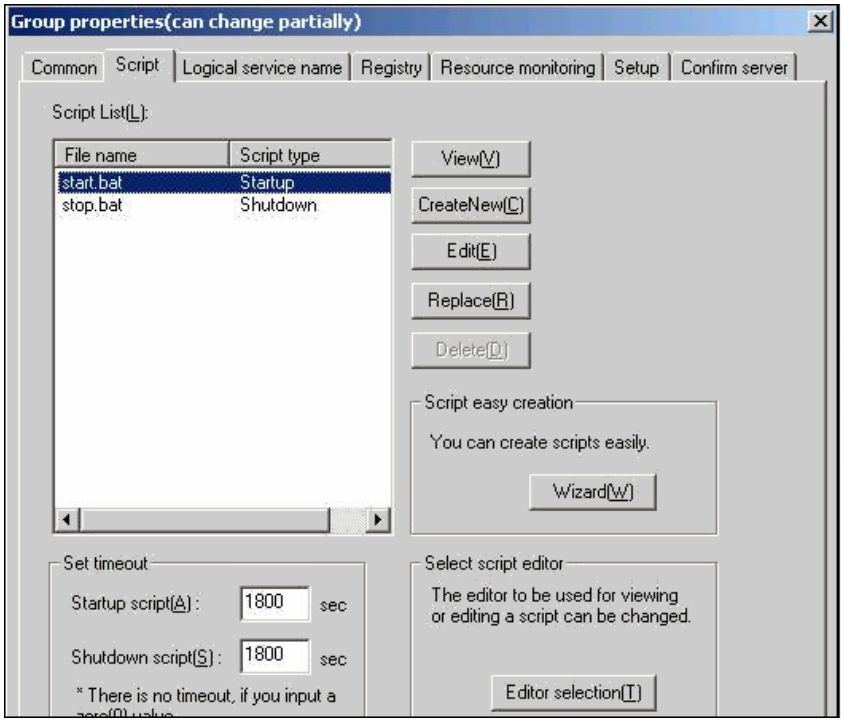
2. Select the NEC Group that the Arcserve server is deployed in, and locate the corresponding Arcserve cluster resources. Right-click on each Arcserve cluster resource and from the pop-up menu, select Property.

   The Group property dialog appears.



3. Select the Reference and Change option. When the Group properties dialog opens, select the Script tab.

   The Script tab dialog appears.



4. From the Script list, select start.bat and click Edit. When the start.bat script appears, locate the REM SET process script (two locations) and set the value to zero as follows:

   ```
   SET process=0
   ```

   Note: In the start.bat file, the REM SET process script is located after NORMAL and after FAILOVER.

   The start.bat script is modified.

5. From the Script list, select stop.bat and click Edit. When the stop.bat script appears, locate the REM SET process script (two places) and set the value to zero as follows:

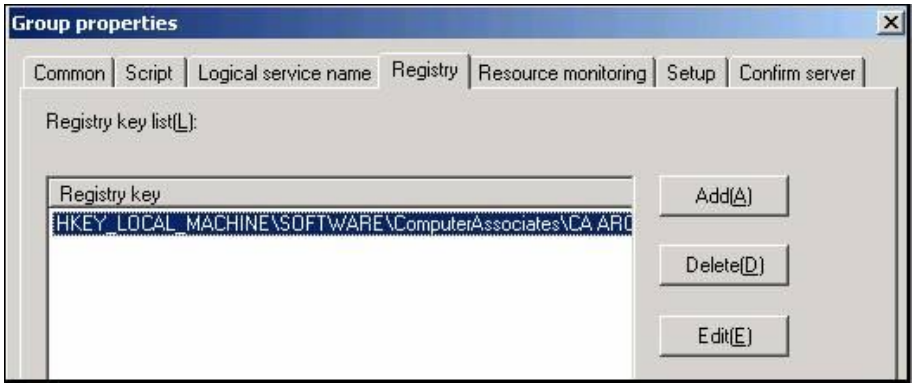
   ```
   SET process=0
   ```

   Note: In the stop.bat file, the REM SET process script is located after NORMAL and after FAILOVER.

   The stop.bat script is modified.

6. From the Group properties dialog, select the Registry tab.

   The Registry dialog appears.



7. From the Registry key list, select the existing registry key and click Delete.

   The Registry key is deleted.

Enable Arcserve Backup in NEC Cluster Scripts

Cluster scripts and registry keys are inserted during the NEC post-setup process. During the upgrade process, the cluster scripts are disabled and the registry key is deleted. When the upgrade is finished, these cluster scripts need to be enabled and registry keys need to be rebuilt.

Note: This section contains graphics that correspond with NEC CLUSTERPRO/ExpressCluster version 8.0. If you are running a more recent version of NEC CLUSTERPRO/ExpressCluster, see your NEC CLUSTERPRO/ExpressCluster documentation.

To enable Arcserve Backup in NEC cluster scripts

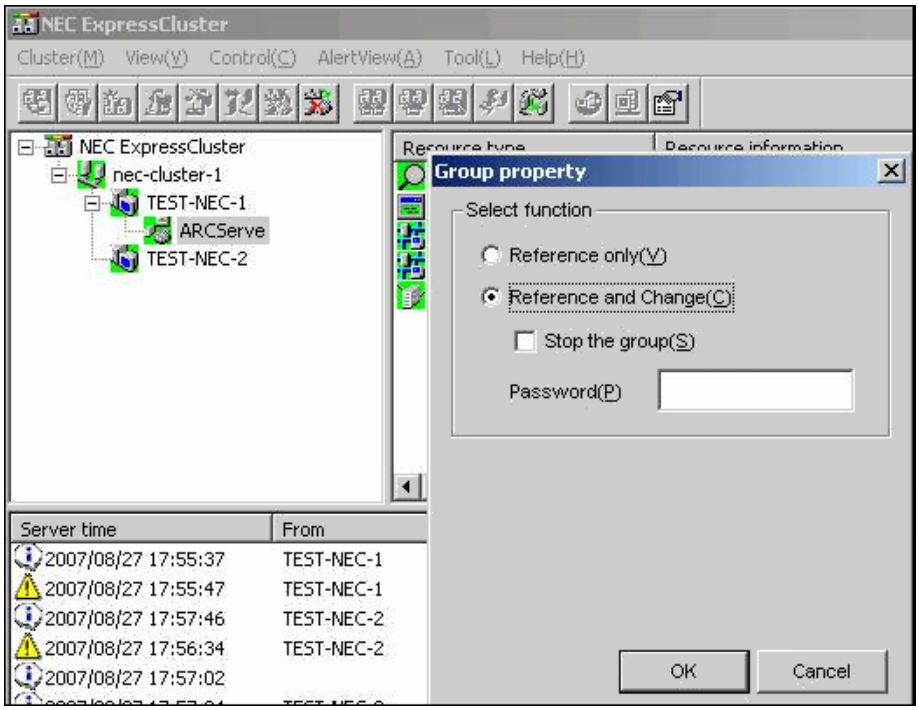
1. Access Cluster Manager.

   The Cluster Manager dialog appears.

   Note: Cluster Manager is a utility provided by NEC and is installed on servers that have NEC CLUSTERPRO/ExpressCluster installed. From the Cluster Manager, you perform most of the configuration and management tasks associated with clusters.

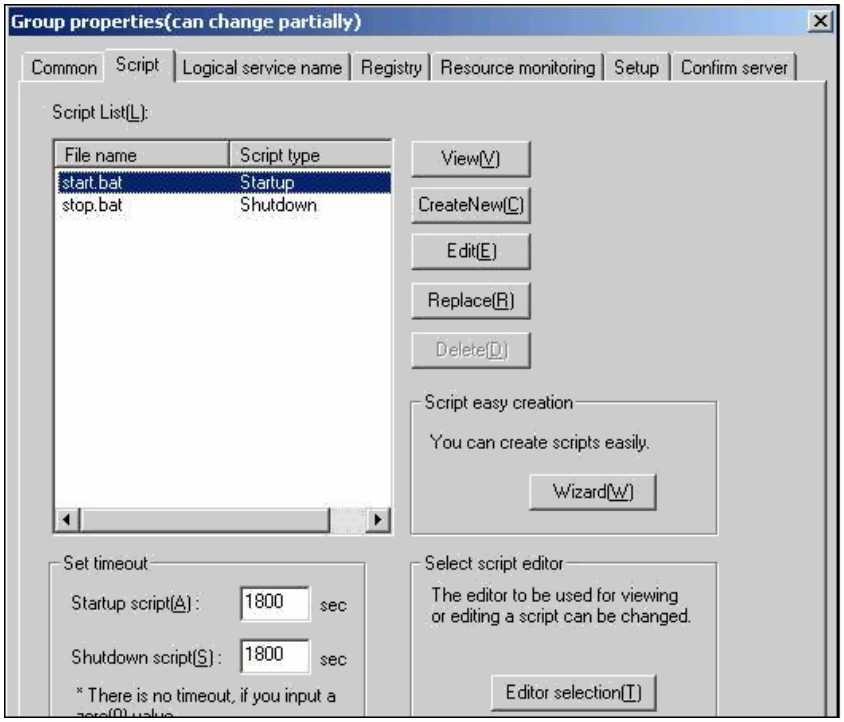
2. Select the NEC Group that the Arcserve server is deployed in, and locate the corresponding Arcserve cluster resources. Right-click on each Arcserve cluster resource and from the pop-up menu, select Property.

   The Group property dialog appears.



3. Select the Reference and Change option. When the Group properties dialog opens, select the Script tab.

   The Script tab dialog appears.



4. From the Script list, select start.bat and click Edit. When the start.bat script appears, locate the REM SET process script (two places) and set the value to 1 as follows:

   SET process=1

   Note: In the start.bat file, the REM SET process script is located after NORMAL and after FAILOVER.

   The start.bat script is modified.

5. From the Script list, select stop.bat and click Edit. When the stop.bat script appears, locate the REM SET process script (two places) and set the value to 1 as follows:

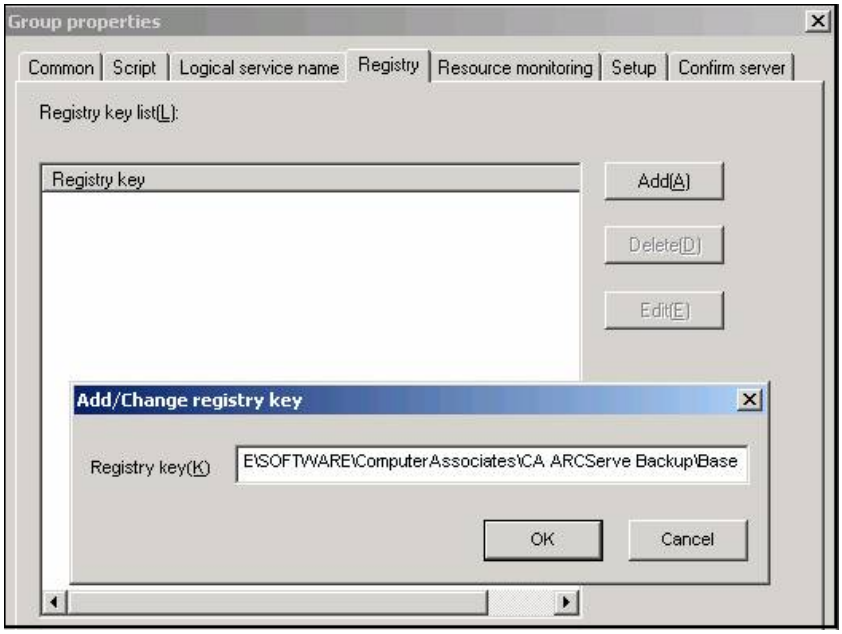
   SET process=1

   Note: In the stop.bat file, the REM SET process script is located after NORMAL and after FAILOVER.

   The stop.bat script is modified.

6. From the Group properties dialog, select the Registry tab. When the Registry dialog opens, click Add.

   The Add/Change registry key dialog appears.



7. Add the Registry key that corresponds with your computer's architecture:

   - **x86 Platforms:**

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCServe Backup\Base

   - **x64 Platforms:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\Base

   Click OK.

   The Registry key is added to the Registry key list on the Group Properties dialog.

How to Verify a Cluster-aware Installation and Upgrade

This section describes how to verify Arcserve Backup installations and upgrades in MSCS and NEC CLUSTERPRO cluster-aware environments.

To verify a cluster-aware installation and upgrade

1. Ensure that no errors occurred during the installation or upgrade process.

2. To ensure that Arcserve Backup services start properly, execute the cstop script to stop all Arcserve Backup services and then execute the cstart script to restart all Arcserve Backup services.

   Note: The cstop and cstart batch files are stored in the Arcserve Backup installation directory on the Arcserve Backup server. For more information about using cstop and cstart, see the *Administration Guide*.

3. Open the Arcserve Backup Manager Console on a stand-alone server.

   Note: Do not log in to the cluster node at this time.

4. From the Manager Console on the stand-alone system, log in to the newly installed or upgraded system using the virtual name.

5. If you can successfully log in to the new system, move the Arcserve cluster group to another node. Ensure that all Arcserve services started successfully.

6. After you move the Arcserve cluster group, ensure that you can navigate the Manager Console. For example, open the Backup Manager, the Restore Manager, and the Jab Status Manager.

   Note: The Manager Console may stop responding intermittently while the cluster group is moving.

7. Open the Server Admin. Ensure that the primary server detects all member servers.

8. Open the Device Manager. Ensure that Arcserve Backup detects your devices.

9. Open the Job Status Manager. Ensure that all data from the previous installation migrated to the new primary server. Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new primary server.

10. Submit a simple backup job on a member server.

Chapter 6: Integrating Arcserve Backup with Other Products

This section contains the following topics:

CA Antivirus Integration (see page 183)
Arcserve Replication Integration-IMPW (see page 183)
Arcserve Backup Patch Manager Integration (see page 184)
Arcserve D2D Integration (see page 184)

CA Antivirus Integration

CA Antivirus is bundled with Arcserve Backup. As a result, you can automatically scan for viruses during the job using the virus scanning options.

You can configure CA Antivirus to download updated virus signature files and program modules. These updates are then distributed to the participating applications. When this is complete, CA Antivirus broadcasts a message stating that the update has been completed. Under certain conditions, you must restart the computer to apply the anti-virus protection updates.

Note: Arcserve Backup provides only the scanning and curing components. It does not provide a full install of CA Antivirus.

For more information, see the *Administration Guide*.

Arcserve Replication Integration-IMPW

Arcserve Replication and Arcserve High Availability are data protection solutions that use asynchronous real-time replication to provide disaster recovery capabilities. This host-based software provides continuous data replication that transfers changes to application data as they occur to a standby replica server located locally or over the Wide Area Network (WAN). Continuous data replication ensures that the most recent data is always available for restoring purposes.

Arcserve Replication and Arcserve High Availability are separately-sold Arcserve products.

For information about integrating Arcserve Backup with Arcserve Replication, see the *Arcserve Replication Integration Guide*.

Arcserve Backup Patch Manager Integration

Arcserve Backup Patch Manager is packaged with Arcserve Backup for Windows on the Arcserve Backup for Windows installation media. You can install Arcserve Backup Patch Manager directly from the installation media using the Arcserve Backup for Windows Installation Browser.

For information about using Arcserve Backup Patch Manager, see the documentation provided with Arcserve Backup Patch Manager. You can open the Arcserve Backup Patch Manager Readme and the Arcserve Backup User Guide directly from the Arcserve Backup Patch Manager Installation Browser.

Arcserve D2D Integration

Arcserve Backup integrates with Arcserve D2D so that you can do the following:

- Manage Arcserve D2D servers from a central location.
  - Add computers running Arcserve D2D to the Arcserve D2D Servers object in the Backup Manager.
  - Add computers running Arcserve D2D to the Arcserve D2D Proxy Servers object in the Backup Manager.
  - Add Arcserve Host-Based VM Backup proxy servers running Arcserve D2D to the Arcserve D2D Proxy Servers object in the Backup Manager.
- Create Arcserve Backup sessions from Arcserve D2D backup data.
- Back up Arcserve D2D backup sessions stored locally on Arcserve D2D servers to Arcserve Backup media.
- Back up Arcserve D2D backup sessions stored remotely on proxy servers and remote shares (for example, NFS volumes on Linux servers) to Arcserve Backup media.

  Note: Arcserve Backup executes the backup from the server where the Arcserve D2D backup sessions reside; not from the Arcserve D2D server.
- Back up Arcserve D2D data using multistreaming.
- Store Arcserve Backup sessions on tape media (libraries), disk (file system devices), and network shares.
- Recover Arcserve D2D backup data at file and folder level granularity from Arcserve Backup media.
- Recover Microsoft SQL Server databases and Microsoft Exchange Server mailboxes at application level granularity from Arcserve Backup media.

Be aware of the following:

- The Arcserve Backup Client Agent for Windows must be installed on the Arcserve D2D servers to allow Arcserve Backup to communicate with and integrate with Arcserve D2D.

  Note: The Arcserve Backup Client Agent for Windows can be installed on the proxy server if the proxy server option is used to back up Arcserve D2D servers.

- The following sections describe how to integrate Arcserve D2D servers into your Arcserve Backup environment. For information about how to back up Arcserve D2D backup sessions and how to recover D2D data from Arcserve Backup backup sessions, see the *Administration Guide.*

Define How You Will Back Up Arcserve D2D Sessions

The method that you use to back up Arcserve D2D sessions is contingent upon your recovery time objective and the purpose of the Arcserve Backup backup sessions. You can use the following methods to back up Arcserve D2D sessions.

Arcserve D2D Backups

Consider the following aspects of Arcserve D2D backup operations:

- Use this method when you want to recover individual files and folders and recover data (Microsoft Exchange Server and Microsoft SQL Server) quickly at application level granularity.
- You install Arcserve D2D on the nodes that you want to protect.
- You add Arcserve D2D nodes to the Arcserve D2D Servers object in the Backup Manager Source tree.
- With this backup method, you let Arcserve Backup create backup sessions from the full and incremental Arcserve D2D backup sessions. This type of backup lets Arcserve Backup back up the Arcserve D2D catalog files.
- You can use multistreaming to back up the Arcserve D2D full and incremental backup sessions to decrease the overall backup window. Multistreaming lets you transmit multiple streams of backup data in one job. When using multistreaming with incremental backups, the backup window is fast.

Client Agent for Windows Backups

Consider the following aspects of Client Agent for Windows backup operations:

- Use this backup method when you want to use the backup data to perform full system recoveries, such as for disaster recovery and Bare Metal Recovery.
- You install Arcserve D2D and the Client Agent for Windows on the nodes that you want to protect.
- You add Arcserve D2D nodes to the Arcserve D2D Proxy Servers object in the Backup Manager Source tree.

  Note: Arcserve Host-Based VM Backup servers can function as backup proxy servers for Client Agent for Windows backups. Arcserve Host-Based VM Backup lets you back up Arcserve D2D nodes through a backup proxy system using fewer Arcserve D2D licenses. For more information about Arcserve Host-Based VM Backup, see the *Arcserve Host-Based VM Backup User Guide* on the Arcserve Central Applications Bookshelf on the Arcserve Support Online website.
- With this method, you let Arcserve Backup create full backup sessions from the Arcserve D2D backup sessions.
- You can use multistreaming to back up the Arcserve D2D sessions to decrease the overall backup window. Multistreaming lets you transmit multiple streams of backup data in one job. With multistreaming, the backup data for each node that is contained in a job is processed as one stream of backup data.

How You Manage Arcserve D2D Servers from the Backup Manager

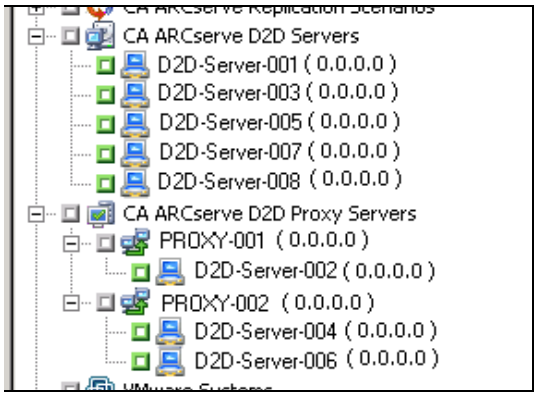
To configure backup policies and submit backups of Arcserve D2D servers, the Arcserve D2D servers must appear below the Arcserve D2D Servers object or the Arcserve D2D Proxy Servers object in the Backup Manager Source directory tree.

Note: To help ensure that backups complete successfully, verify that system time on the Arcserve Backup server, the Arcserve D2D nodes, and the Arcserve D2D proxy servers are the same. This approach helps ensure that backups complete successfully when you back up Arcserve D2D nodes and virtual machines protected by Arcserve D2D proxy servers.

Storage Resource Management Performance Key Indicators (SRM PKI) is a Arcserve Backup component that lets you monitor the performance of the agents running in your backup environment. When SRM PKI is running on the Arcserve Backup primary server, Arcserve Backup detects and populates the Backup Manager Source directory tree with the names or IP addresses of the Arcserve D2D servers that are running in your backup environment. For more information about SRM PKI, see the *Dashboard User Guide*.

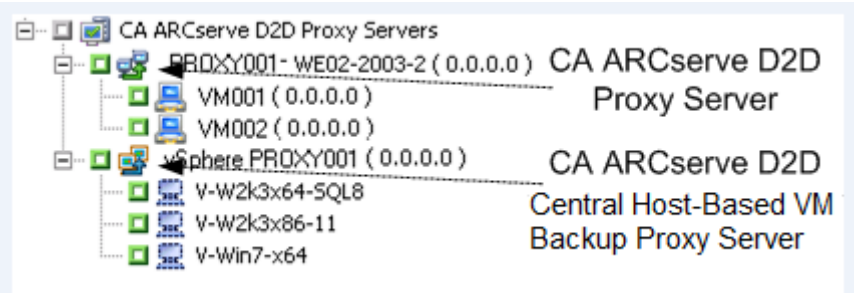
When SRM PKI is not running on the primary server, or the primary server did not detect Arcserve D2D servers, you can add the Arcserve D2D servers to the Source directory tree manually. For more information, see Assign Arcserve D2D Servers to the Arcserve D2D Servers Object (see page 188).

The following diagram illustrates the Arcserve D2D Servers and the Arcserve D2D Proxy Servers objects in the Backup Manager source tree. The objects list the host name or IP address of the Arcserve D2D servers and Arcserve D2D Proxy servers that reside in the Arcserve Backup environment.



Note: The Backup Manager does not support browsing the directories, files, and folders contained within the Arcserve D2D servers.

Arcserve Backup lets you manage virtual machines running Arcserve D2D based on the version of the VMware software that is running on your backup proxy systems. The following diagram illustrates the icons that differentiate Arcserve Host-Based VM Backup proxy systems from Arcserve D2D backup proxy systems:



From the Arcserve D2D Servers object and the Arcserve D2D Proxy Servers object, you can perform the following server management tasks:

- Assign Arcserve D2D Servers to the Arcserve D2D Servers Object (see page 188)
- Assign Arcserve D2D Servers to the Arcserve D2D Proxy Servers Object (see page 188)
- Delete Arcserve D2D Servers from the Backup Manager Source Tree (see page 190)

Assign Arcserve D2D Servers to the Arcserve D2D Servers Object

From the Backup Manager, you can add Arcserve D2D servers to the Arcserve D2D Servers object in the Backup Manager source tree.

You add D2D servers to the Arcserve D2D Servers object when you need to use the backup data to restore D2D data at file level, folder level, and application level granularity.

Follow these steps:

1. Open the Arcserve Backup Manager Console.

   From the Quick Start menu, click Backup to open the Backup Manager.

2. Click the Source tab.

   The Source tree appears.

3. Right-click the Arcserve D2D Servers object and click Add D2D Server on the pop-up menu.

   The Add D2D Server dialog opens.

4. Complete the following fields on the Add D2D Server dialog:

   - **Host name--**Specify the host name of the D2D server.
   - (Optional) **IP address--**Specify the IP address of the D2D server.

     Note: To specify the IP address, clear the checkmark next to the Use computer name resolution option.
   - **User name--**Specify the user name that is required to log in to the D2D server.
   - **Password--**Specify the password that is required to log in to the D2D server.

   Click OK.

The Arcserve D2D server is assigned to the Source tree below the Arcserve D2D Servers object.

Note: Arcserve Backup does not support browsing the drives and directories within Arcserve D2D servers after they are added to the Source tree.

Assign Arcserve D2D Servers to the Arcserve D2D Proxy Servers Object

From the Backup Manager, you assign Arcserve D2D servers to Arcserve D2D Proxy Servers object in the Backup Manager Source tree. When you assign D2D servers to the D2D Proxy Servers object, Arcserve Backup backs up all of the backup sessions for all D2D servers using one proxy server. In addition, when Arcserve Host-Based VM Backup is installed on the D2D proxy, Arcserve Backup backs up the backup sessions for all virtual machines running D2D that are assigned to the proxy server.

Arcserve Backup performs full backups of D2D backup sessions when D2D servers are assigned to the D2D Proxy Servers object. The Arcserve Backup backup sessions can then be used to perform full system recovery operations, such as bare metal recovery (BMR).

Note: To assign Arcserve D2D servers to Arcserve D2D proxy servers, Windows Remote Registry service must be running on the Arcserve D2D node.

Follow these steps:

1. Open the Arcserve Backup Manager Console.

   From the Quick Start menu, click Backup to open the Backup Manager.

2. Click the Source tab.

   The Source tree appears.

3. Do one of the following:

   - If you do not want to add Arcserve D2D proxy servers to the Arcserve D2D Proxy Servers object, go to Step 5.
   - To add Arcserve D2D proxy servers, right-click the Arcserve D2D Proxy Servers object and click Add D2D Proxy Server on the pop-up menu.

     The Add D2D Proxy Server dialog opens.

4. Complete the following fields on the Add D2D Proxy Server dialog:

   - **Host name--**Specify the host name of the D2D proxy server.
   - (Optional) **IP address--**Specify the IP address of the D2D proxy server.

     Note: To specify the IP address, clear the checkmark next to the Use computer name resolution option.

   - **User name--**Specify the user name that is required to log in to the D2D proxy server.
   - **Password--**Specify the password that is required to log in to the D2D proxy server.
   - (Optional) **This is a Central Host-Based VM Backup proxy--**Specify this option only when Arcserve Host-Based VM Backup is running on the backup proxy system and the servers that you want to protect are virtual machines.

   Click OK.

   The Add D2D Proxy Server dialog closes and the newly added Arcserve D2D proxy server appears in the Source tree. If you specified This is a Central Host-Based VM Backup proxy, Arcserve Backup adds the Central Host-Based VM Backup proxy server to the Arcserve D2D Proxy Servers object and populates the proxy server with the host names of the virtual machines that are running Central Host-Based VM Backup and are associated with the newly added proxy server.

5. To assign Arcserve D2D servers to Arcserve D2D proxy servers, right-click the proxy server and click Assign D2D Server on the pop-up menu.

   The Assign D2D Server to a Proxy Server dialog opens.

   Note: If the Arcserve D2D proxy server is a Arcserve Host-Based VM Backup proxy server, you cannot assign individual VMs directly to the proxy server.

6. Complete the following fields on the Assign D2D Server to a Proxy Server dialog:

   - **Host name--**Specify the host name of the D2D server.
   - (Optional) **IP address--**Specify the IP address of the D2D server.

     Note: To specify the IP address, clear the checkmark next to the Use computer name resolution option.
   - **User name--**Specify the user name that is required to log in to the D2D server.
   - **Password--**Specify the password that is required to log in to the D2D server.

   Click OK.

   The Assign D2D Server to a Proxy Server dialog closes.

The Arcserve D2D server is assigned to the Source tree below the Arcserve D2D proxy server.

Note: Arcserve Backup does not support browsing the drives and directories within Arcserve D2D servers after they are added to the Source tree.

Delete Arcserve D2D Servers from the Backup Manager Source Tree

From the Backup Manager, you can remove Arcserve D2D servers and Arcserve D2D proxy servers from the Backup Manager source tree.

To delete Arcserve D2D servers from the Backup Manager source tree

1. Open the Arcserve Backup Manager Console.

   From the Quick Start menu, click Backup to open the Backup Manager.

2. Click the Source tab

   The source tree appears.

3. Do one of the following:

   - **Arcserve D2D servers:** Expand the Arcserve D2D Servers object, right-click the server that you want to delete, and click Delete D2D Server on the pop-up menu.
   - **Arcserve D2D proxy servers:** Expand the Arcserve D2D Proxy Servers object, right-click the proxy server that you want to delete, and click Deleted D2D Proxy Server on the pop-up menu.

   The delete confirmation dialog opens.

4. Click Yes.

   The server is deleted from the Backup Manager source tree.

Note: If a Arcserve D2D server appears under the Arcserve D2D Servers object and the Arcserve D2D Proxy Servers object, the removal process deletes the Arcserve D2D server from both directory trees.

Open the Arcserve D2D Home Page from the Backup Manager

Arcserve Backup lets you open the Arcserve D2D Home Page from the Backup Manager.

Use these steps when you want to perform various Arcserve D2D tasks from the Arcserve D2D Home Page.

Follow these steps:

1. Open the Arcserve Backup Manager Console.

   From the Quick Start menu, click Backup to open the Backup Manager.

2. Click the Source tab.

   The source tree appears.

3. Do one of the following:

   - Expand the Arcserve D2D Servers object.

     Right-click the Arcserve D2D server that you want to configure and click Launch D2D on the pop-up menu.

   - Expand the Arcserve D2D Proxy Servers object.

     Expand the proxy server.

     Right-click the Arcserve D2D server that you want to configure and click Launch D2D on the pop-up menu.

   The Arcserve D2D Home Page opens.

   Note: For information about using Arcserve D2D, see the Arcserve D2D documentation.

How Arcserve Backup Processes Encrypted Arcserve D2D Backup Sessions

Arcserve D2D lets you protect sensitive data using data encryption. The data is protected using an encryption password that you specify when the backup is submitted. To recover the Arcserve D2D data, you specify the password when you submit the restore.

To back up Arcserve D2D sessions to Arcserve Backup media, you add the Arcserve D2D servers to the Backup Manager Source directory tree before you can submit backups. The process of adding the Arcserve D2D servers to the Source tree requires you to specify the Arcserve D2D computer name and credentials (user name and password). Arcserve Backup uses the Arcserve D2D credentials to retrieve the Arcserve D2D encryption password, to decrypt the data, and to back up the data to Arcserve Backup media. As a result, Arcserve Backup stores the Arcserve D2D backup sessions on Arcserve Backup media in decrypted format.

To recover Arcserve D2D data from Arcserve Backup media, a password is not required. If you want to encrypt the Arcserve D2D data on Arcserve Backup media, you can specify Arcserve Backup encryption options when you submit the job. For more information about encryption options, see Backup Manager Encryption/Compression Options in the *Administration Guide*.

Chapter 7: Configuring Arcserve Backup

This section describes how to configure the Arcserve Backup base product. For information about how to configure Arcserve Backup agents and options, see the corresponding agent or option guide.

This section contains the following topics:

Open the Manager or Manager Console (see page 193)
Arcserve Backup Home Page (see page 195)
First-Time Home Page and User Tutorial (see page 199)
Service State Icons (see page 200)
Log in to Arcserve Backup (see page 200)
Specify Arcserve Backup Manager Preferences (see page 202)
Code Pages (see page 204)
Arcserve Backup System Account (see page 206)
Start the Arcserve Backup Database Protection Job (see page 207)
Fine-Tune the Arcserve Backup SQL Server Database (see page 208)
Configure Devices Using the Device Wizard (see page 210)
Configure Enterprise Module Components (see page 211)
Configure Global Dashboard (see page 211)
Create File System Devices (see page 220)
How to Define Include and Skip Parameters for Arcserve Backup Database Agents (see page 222)
Configuring Firewalls to Optimize Communication (see page 223)

Open the Manager or Manager Console

The Manager Console is an interface that lets you administer backup and restore operations in your environment. With the Manager Console, you can log in to and administer local and remote Arcserve Backup servers and domains.

This release of Arcserve Backup provides you with a redesigned Manager Console. If you are running an older release of Arcserve Backup in your environment, you must log in to the system running the older release using the previous version of the Manager.

To open the Manager or Manager Console

1. Do one of the following:

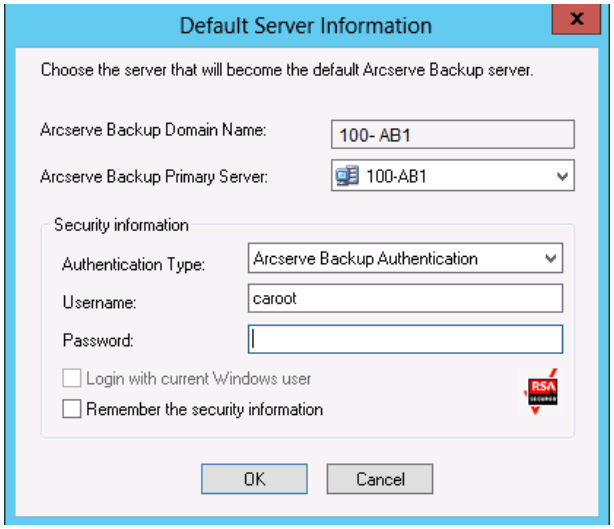
   - To access a server running this release of Arcserve Backup, click the Windows Start button, point to Programs, CA, ARCserve Backup, and click Manager.
   - To access an Arcserve server running a previous release, browse to the following file:

     C:\Programs Files\CA\ARCserve Backup\ARCserveMgr.exe

     Double-click ARCserveMgr.exe.
   - If you installed a previous Arcserve Backup release in the default installation directory, and used the installation process to upgrade Arcserve Backup, you can open the Manager by clicking the Windows Start button, select Programs, CA, ARCserve Backup, and click Manager.

   The Default Server Information page appears.

2. To change the default server or specify a different server, select a server from the Arcserve Backup Primary Server list. If the target server does not appear in the drop-down list, you can input the host name or IP address of the server in the Arcserve Backup Primary Server list.



3. To change the user, select either Arcserve Backup Authentication or Windows Authentication and specify a user name and password.

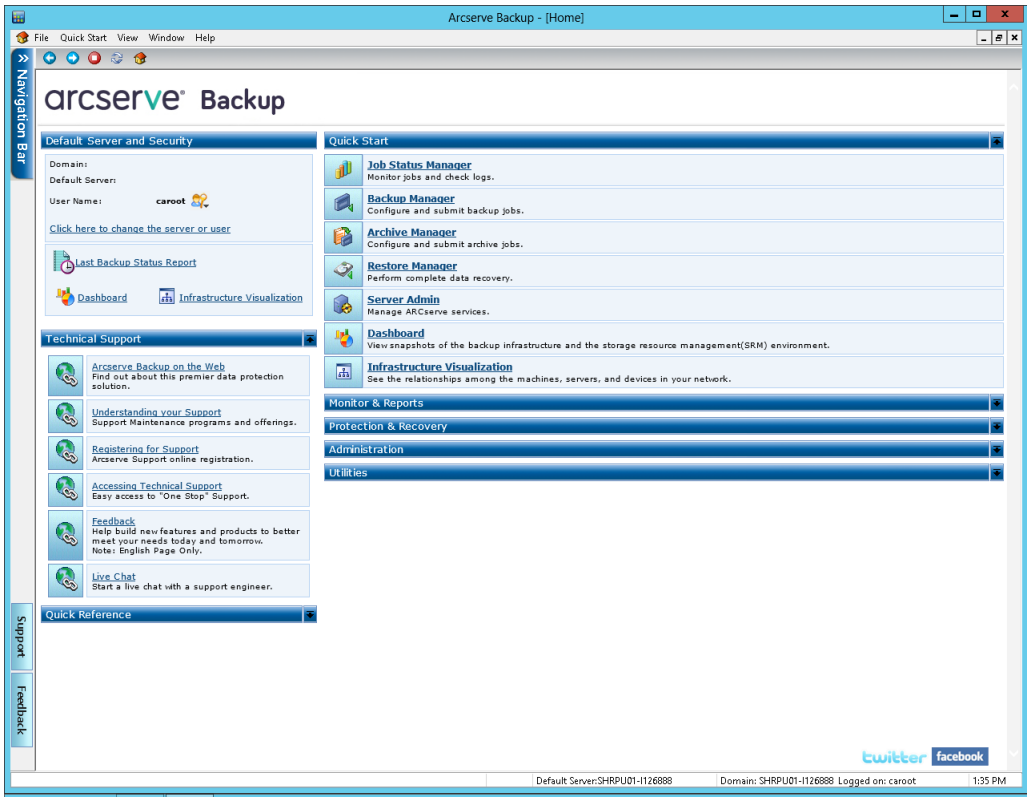
   By default, Arcserve Backup does not remember your security information. To save the user name and password information that you entered for this server, you must explicitly select Remember the security information. If you do not save this information, Arcserve Backup prompts you to provide Arcserve Backup security credentials the first time you open managers, wizards, and so on, and you must provide a Arcserve Backup user name and password.

4. Enter caroot in the User Name field, the appropriate password in the Password field, and click OK.

   The first time you log in to Arcserve Backup, a tutorial, called My First Backup, appears. This tutorial lets you become familiar with the basics of backing up and restoring data in a controlled and directed way. This tutorial appears automatically only the first time you log in. However, you can access My First Backup from the Help menu.

Arcserve Backup Home Page

The Home Page is the central location from which you can log in to other Arcserve Backup servers and access all of the Arcserve Backup managers, wizards, and utilities.



Note: When you open the Arcserve Backup Home Page, a message may appear that indicates access to http://www.google.com is blocked. The message displays in the RSS Feeds section on the home page. If necessary, you can stop the RSS Feeds communication process at any time. For more information, see "How to Access Arcserve Backup Managers, Wizards, and and Utilities" in the *Administration Guide*.

Default Server and Security

Displays the following information about the Arcserve Backup server:

- The Domain and Default Server that the current User name is logged in to.

  Note: For information about how to change the default server and login to a different Arcserve Backup primary or stand-alone server, see Log On to Arcserve Backup (see page 200).

- View a summary of the user and the user's roles when a Windows user is logged into Arcserve Backup. Click the Role Information icon next to the User Name field to see the User Role list which includes all the roles owned by the user.
- View the Daily Backup Status Report.
- Start Arcserve Backup Dashboard.
- View Infrastructure Visualization
- View details if the Enterprise Module is not installed or if the license is expired. Click the link on the Home Page GUI to see the limitations.

Quick Start

Lets you open the following Arcserve Backup Managers:

- **Job Status Manager--**Lets you monitor jobs and view logs.
- **Backup Manager--**Lets you configure and submit backup jobs.
- **Archive Manager--**Lets you configure and submit archive backup jobs.
- **Restore Manager--**Lets you perform complete data recovery.
- **Server Admin--**Lets you manage Arcserve Backup engines. For example, the Database Engine, the Job Engine, and the Tape Engine.
- **Dashboard**--Lets you access a snapshot overview of your backup infrastructure.
- **Infrastructure Visualization--**Lets you view the relationships between the computers, servers, and devices in your Arcserve Backup environment.

Monitor and Reports

Lets you open the following managers and utilities:

- **Job Status Manager--**Lets you monitor jobs and view logs.
- **Report Manager--**Lets you perform complete data recovery.
- **Report Writer--**Lets you create custom Arcserve Backup reports.
- **Dashboard**--Lets you access a snapshot overview of your backup infrastructure.
- **Infrastructure Visualization--**See the relationships among the machines, servers, and devices in your network.

Protection and Recovery

Lets you open the following managers and wizards:

- **Backup Manager**--Lets you configure and submit backup jobs.
- **Archive Manager**--Lets you configure and submit archive backup jobs.
- **Restore Manager**--Lets you perform complete data recovery.
- **Arcserve Replication**--Lets you start or install Arcserve Replication. Arcserve Replication is a data protection solution that uses asynchronous real-time replication to provide disaster recovery capabilities. This link is active when you install Arcserve Replication. For information, see the *Arcserve Replication Integration Guide*.
- **CA ARCserve D2D**--Lets you start or install CA ARCserve D2D. CA ARCserve D2D is a backup solution that lets you track changes to data at the block level, and back up only the changed blocks. CA ARCserve D2D lets you perform frequent incremental backups, which reduces the size of the backups and provides you with up-to-date backup data.

Administration

Lets you open the following managers, wizards, and utilities:

- **Server Admin**--Lets you manage Arcserve Backup engines. For example, the Database Engine, the Job engine, and the Tape engine.
- **Central Agent Admin**--Lets you manage Arcserve Backup agents.
- **Device Manager**--Lets you manage the storage devices in your environment.
- **Device Configuration**--Lets you configure your storage devices in your Arcserve Backup environment.
- **Device Wizard**--Lets you perform media operations.
- **Device Group Configuration**--Lets you configure the device groups in your Arcserve Backup environment and select the groups that you will use for the staging of data.
- **Media Pool**--Lets you create and maintain media pools in your Arcserve Backup environment.
- **Database Manager**--Lets you manage and maintain the Arcserve Backup database.
- **Alert Manager**--Lets you create alert notifications about events that occur during a backup.
- **User Profile**--Lets the Arcserve Backup administrator manage user profiles and provide access to Arcserve Backup.
- **Agent Deployment**--Launches the Agent Deployment tool, which lets you install and upgrade Arcserve Backup agents on remote hosts.
- **MM Admin**--Lets you manage off-site media resources.

Utilities

Lets you open the following wizards and utilities:

- **Job Scheduler Wizard--**Lets you control Arcserve Backup command line utilities.
- **Create Boot Kit--**Lets you create disaster recovery boot disk sets. This link is active when you install the Arcserve Backup Disaster Recovery Option.

  Note: For more information, see the *Disaster Recovery Option Guide.*
- **Diagnostic Wizard--**Lets you gather information from Arcserve Backup system logs. The information gathered can be used for troubleshooting and may help Arcserve Technical Support identify issues.
- **Merge--**Lets you merge session information from media into the Arcserve Backup database.
- **Media Assure & Scan--**Lets you gather information about the backup sessions on media.
- **Compare--**Lets you compare the contents of a media session to files on a computer.
- **Count--**Lets you count the files and directories on a computer.
- **Copy--**Lets you copy or move files from one hard disk to another.
- **Purge--**Lets you delete files and directories from a computer.

Technical Support

The Technical Support section provides quick access to the following support tools:

- **Arcserve Backup on the Web--**Links you to the Arcserve site that provides product information about Arcserve Backup.
- **Understanding your Support--**Provides maintenance and support information by product.
- **Registering for Support--**Provides an online form to register for Arcserve Support Online.
- **Accessing Technical Support--**Offers the latest Arcserve Backup news and information from Technical Support, including white papers, how-to documents, videos, forums and user groups, troubleshooting guides, patches, and more.
- **Feedback--**Links you to Get Satisfaction, where you can submit ideas and comments about the product, ask questions, exchange tips with other users, report problems, and provide praise.

  Note: The Feedback button on the Navigation Bar also links to the Arcserve Feedback dialog for Get Satisfaction.

Quick Reference

The Quick Reference section provides access to the following documentation:

- **Readme--**This document contains last minute updates and information that supplements the Arcserve Backup documentation.
- **Release Summary--**This document contains a summary of the new features added and enhancements made to Arcserve Backup.

Arcserve News

The Arcserve News section provides access to a list of news articles and press releases.

First-Time Home Page and User Tutorial

The first time you start Arcserve Backup, a tutorial called My First Backup introduces you to the product and its major functions. The tutorial guides you through the steps needed to set up a file system device and perform your first backup and restore operations.

Service State Icons

The toolbar at the top of each Arcserve Backup manager displays an icon for each of the back-end services--Job Engine, Tape Engine, and Database Engine, as shown by the following illustration:

Depending upon the color, the icons indicate one of the following states:

- **Green--**Indicates that the service is running.
- **Red--**Indicates that the service is not running.
- **Gray--**Indicates that the service cannot be connected to or is in an unknown state.
- **Blue--**Indicates that the service is paused.

Log in to Arcserve Backup

When you open the Arcserve Backup Manager Console, you must log in to Arcserve Backup. The first time you log in to Arcserve Backup, you can log in as caroot, which has administrator privileges, and provide the appropriate password in the password field. Optionally, you can log in to Arcserve Backup using the Windows account that was provided when you installed Arcserve Backup, or with any Windows administrative account associated with the computer that you are logging in to.

After you log in, you can change the password for the caroot user and add new users. You can also add new users using the command line utility, ca_auth.exe. For information about ca_auth.exe, see the *Command Line Reference Guide.*

Note: The caroot password can consist of any combination of alphanumeric and special characters, but may not exceed 15 bytes. A password totaling 15 bytes equates to approximately 7 to 15 characters.

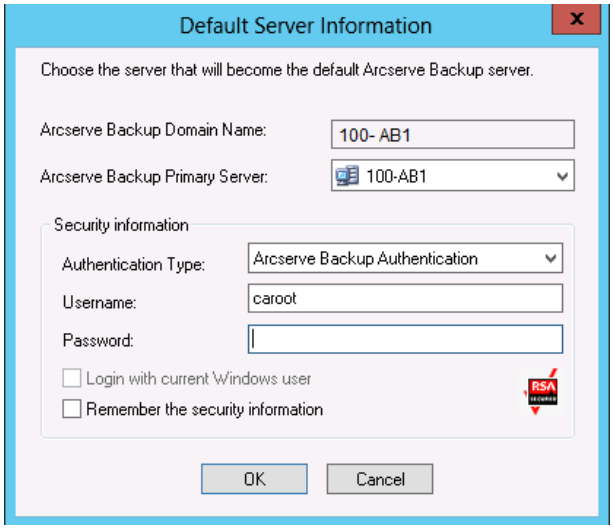
To log in to Arcserve Backup

1. Open the Arcserve Backup Manager Console.

   To open the Manager Console, click Start on the toolbar, select Programs, CA, ARCserve Backup, and click Manager.

   The Default Server Information page appears.

2. To change the default server or specify a different server, select a server from the Arcserve Backup Primary Server list. If the target server does not appear in the drop-down list, you can input the host name or IP address of the server in the Arcserve Backup Primary Server list.



3. To change the user, select either Arcserve Backup Authentication or Windows Authentication and specify a user name and password.

   By default, Arcserve Backup does not remember your security information. To save the user name and password information that you entered for this server, you must explicitly select Remember the security information. If you do not save this information, Arcserve Backup prompts you to provide Arcserve Backup security credentials the first time you open managers, wizards, and so on, and you must provide a Arcserve Backup user name and password.

4. Enter caroot in the User Name field, the appropriate password in the Password field, and click OK.

The first time you log in to Arcserve Backup, a tutorial, called My First Backup, appears. This tutorial lets you become familiar with the basics of backing up and restoring data in a controlled and directed way. This tutorial appears automatically only the first time you log in. However, you can access My First Backup from the Help menu.

Specify Arcserve Backup Manager Preferences

Arcserve Backup lets you configure how the Arcserve Backup Manager windows behave. From the Preferences dialog, you can specify global and library filter options.

To specify Arcserve Backup Manager preferences

1. From the Windows Start menu, open the Arcserve Backup Manager Console by clicking Start, Programs, CA, ARCserve Backup, and selecting Manager.

   The Arcserve Backup Manager Home Page opens.

2. From the Quick Start menu, click Backup.

   The Backup Manager window opens

   Note: You can complete this task from all Arcserve Backup Manager windows.

3. From the View menu, select Preferences.

   The Preferences dialog opens.

4. Select the Global Settings tab. Specify the following global preferences:

   Set Job Queue Refresh Rate to

   Lets you specify a time, in seconds, for periodic update of the Job Status Manager.

   Set Device Manager Refresh Rate to

   Lets you specify a time for periodic update of the Device Manager.

   Set Animated Speed to

   Lets you specify a speed at which the tape bitmap will rotate if animation is selected for the Device or Backup Manager.

   Show Registry

   Displays the registry file in order to select for a backup.

   Show Leaf Nodes

   Displays all leaf nodes within the tree view. This means that files will be displayed under directories and that media will be displayed beneath drives.

   Auto Start All Engines

   Indicates that the appropriate Arcserve Backup engines will start automatically when a manager is used.

   Note: The Auto Start All Engines preference is enabled by default.

Default Manager

Lets you go directly to a specific manager when you open the Manager Console.

Don't show the Server Selection dialog for Count/Copy/Purge job

Lets you hide the Server Selection dialog when you submit a Count job, a Copy job, or a Purge job.

When you submit one of these jobs, the Server Selection dialog opens to let you specify the server where you want to run the job. You can specify a primary server, stand-alone server, or member server for the job.

With this option enabled, Arcserve Backup remembers the server that you want to use for the job and the Server Selection dialog does not open when you submit the job.

Clear the check from the Don't show the Server Selection dialog for Count/Copy/Purge job option to allow the Select Server dialog to open when you submit a Count, Copy or Purge job.

5. Select the Library Filter tab. Specify the following library filter preferences:

Note: The following preferences apply to library devices, and only affect those Manager views in Arcserve Backup where a device or a group hierarchy displays (for example, in the Backup Manager under the Destination tab, or in the Device Manager view). By default, none of the options are selected, and there are no default values for any of the choices.

Show Write Protected Media in Format / Erase dialogs

Lets you view information about write-protected media in all Format and Erase dialogs.

Show device name as Vendor ID and Serial Number

Lets you view device names as the Vendor ID and the serial number.

Show Empty Slots

Lets you view the empty slots in the library.

Show Slots Between

Lets you specify the range of slots to be displayed in the current manager. To define the range, enter the minimum and maximum number of slots allowed.

Show Blank Media

Lets you view the blank media in the library.

Show Tapes Within Media Pool

Lets you view the tapes within a particular media pool. Wildcards (“*” and “?”) are accepted in the media pool.

Show Tapes Matching Serial #

Lets you view the tapes that match a certain serial number. Wildcards (“*” and “?”) are accepted in the serial number.

Important! Applying filters can significantly reduce the amount of data that you have to deal with at one time, and you should use them only with large libraries.

6. When you are finished specifying Arcserve Backup Manager preferences, click Apply.

   Note: To discard your changes, click Cancel.

7. To close the Preferences dialog, click OK.

Code Pages

The following sections describe how Arcserve Backup supports the use of multiple code pages.

This section contains the following topics:

How Arcserve Backup Supports Multiple Code Pages (see page 204)
Specify Code Pages in the Backup Manager Window (see page 205)
Specify Code Pages in the Restore Manager Window (see page 206)

How Arcserve Backup Supports Multiple Code Pages

A code page is a map of characters as they relate to a particular language. If the Arcserve Backup server resides in an environment where different languages and their character sets are running on other computers, the Backup Manager and the Restore Manager may not be able to interpret and display recognizable text in the source tree.

When you encounter this situation, you can specify any code page supported in your environment. The code page lets Arcserve Backup interpret the information and display the text in a format that is recognizable to you.

When you specify a code page at the node or volume level, Arcserve Backup applies the characteristics of the code page to all child volumes, directories, and so on. Although code pages do not affect Arcserve Backup functionality, Arcserve Backup cannot present a code page for more than one language at any time.

Specify Code Pages in the Backup Manager Window

You can change the code page on all nodes displayed in the source tree.

Note: You may be prompted to insert the Windows installation media into your computer to complete this task.

To specify a code page in the Backup Manager window

1. On the Arcserve Backup primary, stand-alone, or member server, open the Windows Control Panel.

   Open Regional and Language Options and select the Advanced tab.

   In the Code pages conversion tables field, click the check box next to the languages that you require to view the node, directory, and volume names on the remote and agent systems that are running in your Arcserve environment.

   (Optional) Click Apply all settings to the current user account and to the default user profile.

   Click Apply and click OK.

   Windows applies the Regional and Language Options.

2. Open the Manager Console and open the Backup Manager.

   From the Source tab, right-click the node, volume, or directory where you want to specify a code page.

   From the Display Encoding right-click menu, select the required code page.

   Arcserve Backup applies the new code page settings immediately.

Specify Code Pages in the Restore Manager Window

You can change the code page on all nodes displayed in the source tree.

Note: You may be prompted to insert the Windows installation media into your computer to complete this task.

To specify a code page in the Restore Manager window

1. On the Arcserve Backup primary, stand-alone, or member server, open the Windows Control Panel.

   Open Regional and Language Options and select the Advanced tab.

   In the Code pages conversion tables field, click the check box next to the languages that you require to view the node, directory, and volume names on the remote and agent systems that are running in your Arcserve environment.

   (Optional) Click Apply all settings to the current user account and to the default user profile.

   Click Apply and click OK.

   Windows applies the Regional and Language Options.

2. Open the Manager Console and open the Restore Manager.

   From the Source tab, right-click the node, volume, or directory where you want to specify a code page.

   From the Display Encoding right-click menu, select the required code page.

   Arcserve Backup applies the new code page settings immediately.

Arcserve Backup System Account

The Arcserve Backup System Account is the account Arcserve Backup uses to perform various storage-related functions on the local server. Local backup or restore jobs use the Arcserve Backup System Account as the security to run the job.

The Arcserve Backup System Account is entered into the System Account dialog when Arcserve Backup is installed, and must be previously established at the operating system level. It is not necessary to grant this account special rights because Arcserve Backup does this automatically.

The account that you enter into the System Account dialog at installation is added automatically to the Administrators and Backup Operators Windows security groups.

How Arcserve Backup Manages Authentication

Arcserve Backup uses Windows and third-party security to establish secure connections when performing various storage-related functions. For instance, if a job backs up a remote server, the security entered for that job must meet the Windows security criteria to access the remote server.

The security context under which the jobs are run varies depending on the resource being accessed. The security required to back up the local Arcserve Backup server may be different from the security required when backing up a domain resource.

Arcserve Backup also interacts with third-party security such as Microsoft SQL, Oracle, and Lotus Notes. For more information, see the various option and agent guides on the Arcserve Backup installation disk or you can download the guides from the Arcserve support website.

How to Use the System Account for Job Security

Typically, when you implement Arcserve Backup you give the Arcserve Backup System Account the following rights and use it as the main backup account:

- Group Rights: Administrators, Backup Operators, Domain Admins
- Advanced Rights: Act as part of operating system, Log on locally, Log on as a service

These security rights are only a reference and are not necessarily applicable to all scenarios.

Important! You should not use the Arcserve Backup System Account for job security for all of your backup and restore operations. However, you can enable this capability by granting rights to the Arcserve Backup System Account that exceed the local administrator and backup operator.

Start the Arcserve Backup Database Protection Job

The Arcserve Backup database maintains job, media, and device information on your system. After you install Arcserve Backup, the Database Protection Job maintains a status of Hold. To use the Database Protection Job to protect the Arcserve Backup, you must change the status of the Database Protection Job from Hold to Ready.

To start the Arcserve Backup Database Protection Job

1. Open the Arcserve Backup Manager Console.

   From the Quick Start menu on the Arcserve Backup Home Page, select Job Status.

   The Job Status Manager window opens.

2. Select the Job Queue tab and find the Database Protection Job.

   Note: If the Database Protection Job was deleted, you can recreate the job using the steps in Recreate the Arcserve Backup Database Protection Job.

   Right-click the Database Protection Job and select Ready from the pop-up menu.

   The status of the Database Protection Job changes from Hold to Ready. A full backup of the database will be performed at the next Execution Time.

3. (Optional) To start the Database Protection Job now, right-click the Database Protection Job and select Run Now from the pop-up menu.

   The Database Protection Job starts now.

   Important! After you start the Database Protection Job, the Tape Engine will connect to a blank media in the first group that Tape Engine detects, and assign the media pool labeled ASDBPROTJOB. If the Tape Engine cannot connect to a blank media in the first group within five minutes, the Tape Engine will try to connect with blank media in the other groups sequentially. If the Tape Engine cannot connect to blank media, in any group, the job will fail.

Note: For information about configuring devices and modifying the database protection job, see the *Administration Guide.*

Fine-Tune the Arcserve Backup SQL Server Database

The following sections describe how you can fine-tune your SQL Server installation to optimize performance.

This section contains the following topics:

How to Calculate the Number of Required SQL Connections (see page 209)
Database Consistency Checks (see page 209)
Specify ODBC Communication for Remote Database Configurations (see page 209)

How to Calculate the Number of Required SQL Connections

For each job that you run, you need two SQL connections. Be sure that you have set enough connections (or licenses) in your SQL server. To determine your default SQL connections, select Server and SQL server from the SQL Arcserve Manager. When you browse from the Configuration tab, you can see the user connections. Set these values to the appropriate user setting. If an error message appears, for example, “Cannot Update Record” or “Failed to Login,” you may have run out of connections. You should increase the open object to 2000.

Database Consistency Checks

When your database activity is low, we recommend that you run a database consistency check if you have a large database. Although it takes some time, it is important to determine that your SQL database is functioning well. For more information, see your Microsoft SQL guide.

Important! Be sure to monitor the log size periodically. If a log is full, the database cannot function. Although the default setting is “truncate log on checkpoint,” you should increase the log size to 50% of the database if you expect to keep a large number of records.

Specify ODBC Communication for Remote Database Configurations

If you have another Arcserve Backup server running that uses Microsoft SQL as its database, you can redirect the local database to the remote machine. Arcserve Backup can use ODBC to connect to the Microsoft SQL server. You can direct the ODBC data source to another server if the server has SQL installed and the Arcserve Backup SQL database is properly set up. You also need to make sure the local server user is authenticated in the remote server.

To specify ODBC communication for remote database configurations

1. Open the Windows Control Panel, select Administrative Tools, Data Sources (ODBC), and System DSN.
2. Add a System Data Source labeled as follows:

   Name: ASNT
   Server: MachineName\InstanceName
3. Follow the on-screen instructions to test and complete the configuration.

Configure Devices Using the Device Wizard

You can start the Device Wizard from the Wizards menu. The Device Wizard helps you see all of the devices connected to your machine.

To configure devices using the Device Wizard

1. From the Administration menu in the Navigation Bar on the Home Page, click Device Wizard.

   The Device Wizard Welcome screen appears.

2. Click Next.

   The Login dialog appears.

3. Enter or select the server you want the device command to operate on, enter your user name and password, and click Next.

4. Select the device you want to target. Click More Information to view more information about the device.

5. Click OK, and click Next.

6. Select a device operation, and click Next.

   Example: Select Format.

7. Enter a new media name and expiration date for the media Arcserve Backup is about to format, and click Next.

8. The schedule screen that appears lets you choose to run the device command immediately or schedule it for a later date and time. Select Run Now, and click Next to run the job immediately.

   To schedule your job for a later time, select the Schedule option, and enter a date and time for the job to run.

9. Click Finish to execute the job.

10. You are prompted to confirm the action you are about to take. Click OK to start the device operation and display its status.

11. A message appears to notify you that Arcserve Backup has completed the device operation. Click Next to work with another device, or click Exit to close the Device Wizard.

Configure Enterprise Module Components

Enterprise Option Configuration is a wizard-like application that lets you configure devices and applications associated with the Arcserve Backup Enterprise Module. With Enterprise Option Configuration you can configure the following devices and applications:

- StorageTek ACSLS libraries
- IBM 3494 libraries
- The Arcserve Backup Image Option

Enterprise Module Configuration opens when you are running Setup and you click Next on the Install Summary dialog.

Use the following steps to run Enterprise Module Configuration after you complete Setup or you want to add or modify Enterprise Module components after you installed Arcserve Backup.

To configure Enterprise Module components

1. From the Windows Start menu, select Programs (or All Programs), CA, ARCserve Backup, and click Enterprise Module Configuration.

   Enterprise Module Configuration opens.

2. Click the Enterprise Module component that you want to configure.

   Follow the prompts on the subsequent dialogs and complete all required information.

Configure Global Dashboard

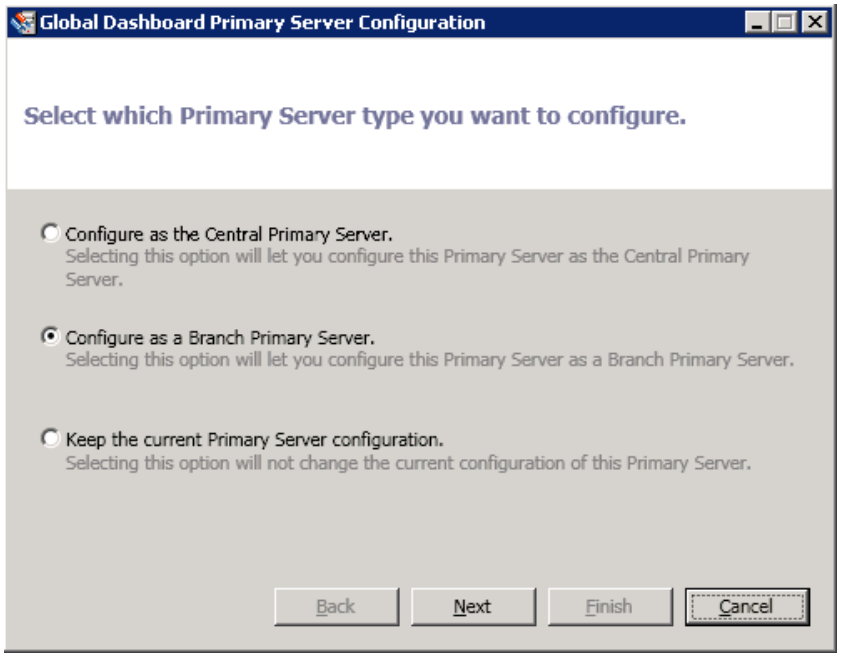
For Global Dashboard to work properly, it is important that the configuration process be performed at the central site and at each associated branch site to enable the necessary communication and synchronization of dashboard-related data from the branch site to the central site. You can configure the server immediately after installation or you can manually launch the configuration at a more convenient time from the Server Configuration Wizard.

Important! During the configuration process, the Arcserve Backup database engine will be shut down for a few minutes. Plan your configuration at a convenient and non-intrusive time when there are no Arcserve Backup jobs scheduled.

When you start the Global Dashboard configuration process, you must first select the type of primary server you want to configure. When making this selection, it is important to remember the following:

- Within your Arcserve Backup environment, there can only be one primary server configured as the Central Primary Server and a Branch Primary Server can only report to one Central Primary Server. When selecting the Central Primary Server, the main consideration should be database type and size. Make sure the selected Central Primary Server is Microsoft SQL Server 2005/2008/2008 R2/2012 and capable of storing dashboard data received from all registered Branch Primary Servers.
- Any primary server (or stand-alone server) within your Arcserve Backup environment can be configured to be a Branch Primary Server. A domain member server cannot be configured as a Branch Primary Server.
- All associated Branch Primary Servers must be registered with the Central Primary Server to enable synchronization.
- There are three roles for Global Dashboard: Central Primary Server, Branch Primary Server, and Global Dashboard Console.
  - The Global Dashboard Console role does not need configuration. After a Primary Server has selected the Global Dashboard option during installation, it automatically has Global Dashboard Console functionality.
  - A Primary Server with the Global Dashboard Console role can still be configured as the Central Primary Server or a Branch Primary Server.
  - After a Primary Server has been configured as the Central Primary Server or a Branch Primary Server, its role cannot be changed anymore.
  - The relationship of three roles is as follows:
    - A Branch Primary Server also has the functionality of a Global Dashboard Console.
    - The Central Primary Server also has the functionality of both a Branch Primary Server (there is a local branch) and a Global Dashboard Console.

- At the end of Arcserve Backup installation, setup will launch the Global Dashboard configuration utility. You can use this utility to configure your server as the Central Primary Server or a Branch Primary Server. If you only want to use the Global Dashboard Console functionality or you want to configure your server as the Central Primary Server or a Branch Primary Server at a later time, you can select the "Keep the current Primary Server configuration" option.



Configure the Central Site

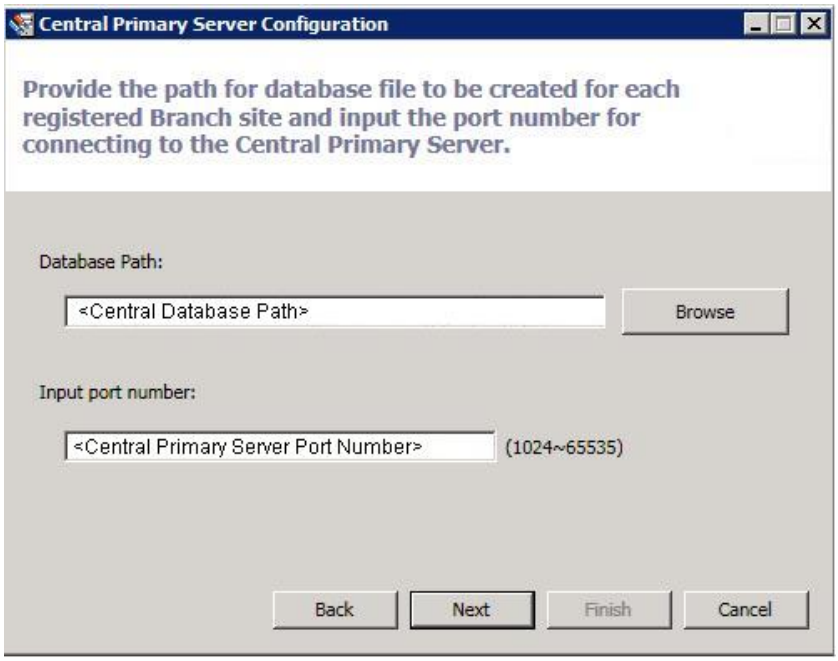
The parameters specified during the configuration of the central site must be used by each registered branch site to enable synchronization of dashboard-related data to the central site.

Note: The local Arcserve Backup database for the Central Primary Server will be treated the same as a normal branch site. However, you do not need to configure it manually because this was completed during setup of the Central Primary Server.

To configure the central site

1. Launch the Central Configuration wizard and click Next to start.

   The screen to provide the path and port information for the central site appears.



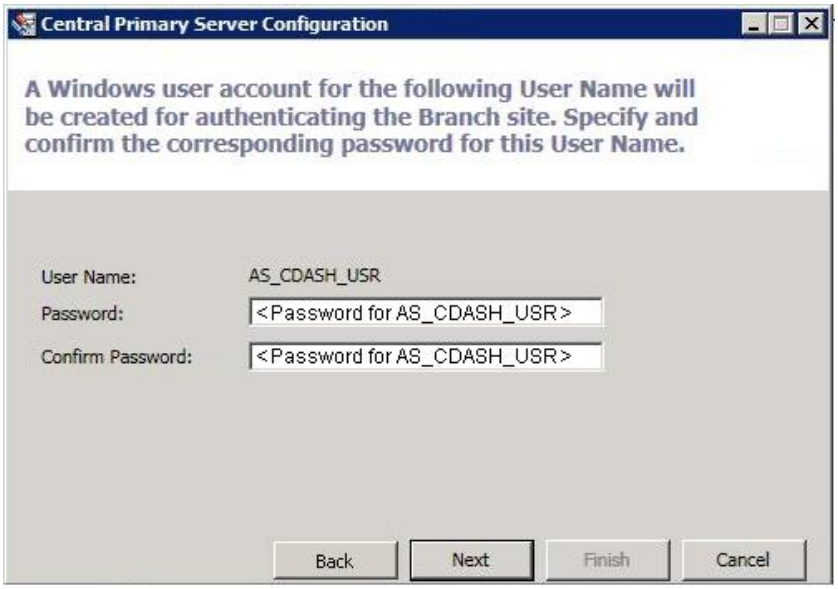
2. Specify the path for the central site database. (This will be the database location where the dashboard-related data from each branch site will be uploaded to and stored).

   Note: If a remote database is used as the ASDB of the Central Primary Server, the database path must be an existing path at the remote machine or else the configuration may fail.

3. Specify the input port number. This will be the port number for each Branch Primary Server to access the Central Primary Server. By default, the Port number is 18001, but can be changed from this screen.

4. Click Next.

   The screen to provide user authentication information appears.



5. Specify and confirm the password for the AS_CDASH_USR user name. A local Windows User with this account name and password will be created on the Central Primary Server. When a branch site connects to the central site, the connection will use this authentication information to allow access to the central site.

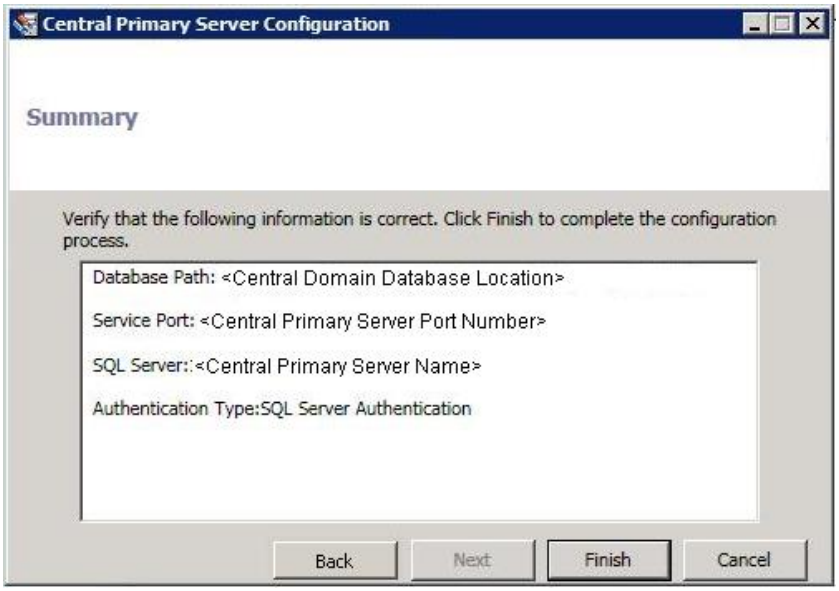
   This password is needed when each branch site wants to register to the Central Primary Server. If necessary, this password can be reset using the Windows User Management. However, if the password is changed, the new information must be manually reset at every branch site that is registered to this Central Primary Server.

   The "Set Password for AS_CDASH_USR" dialog for the Windows User Management is accessed from the Central Primary Server Start menu (Programs\Administrative Tools\Computer Management\Local Users and Groups\Users\AS_CDASH_USR\Set Password).

   Note: The pre-assigned user "AS_CDASH_USR" is for authentication purposes only. No other Arcserve Backup permissions are associated with this user name.

6. Click Next.

   The central site Summary screen appears.



7. The Summary screen displays all configuration-related information for the central Arcserve Backup database and the Central Primary Server. Verify that all displayed information is correct before continuing. If the information is correct, click Finish.

   An alert message appears reminding you that during the configuration process, the Arcserve Backup database engine will be shut down for a few minutes.

8. If it is a convenient and non-intrusive time when there are no Arcserve Backup jobs scheduled, click OK to continue.

   The configuration Progress screen appears displaying the status.

9. When the configuration process is finished, a confirmation screen appears. Click OK.

   The central site configuration process is completed.

Configure a Branch Site

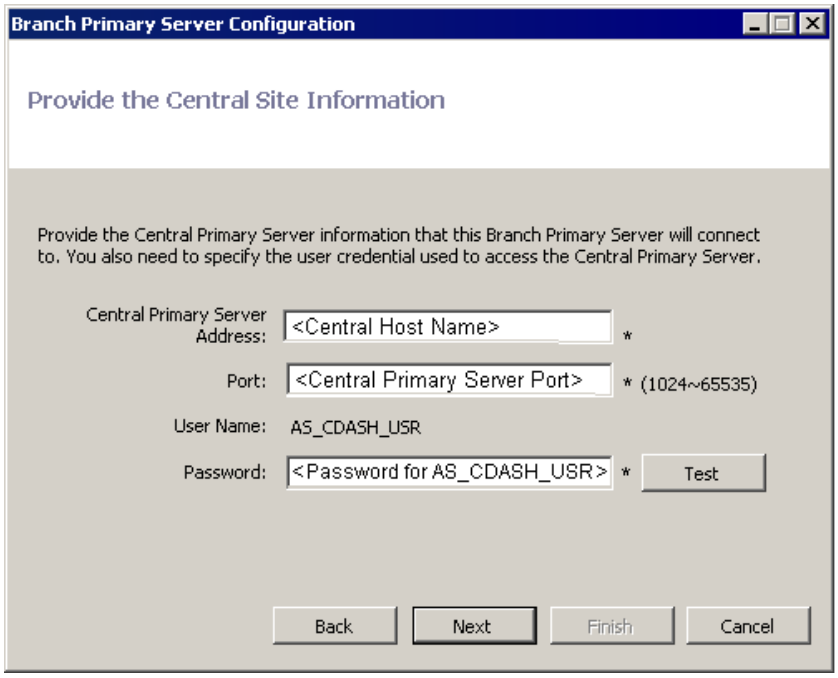
A branch site must be registered to the central site to enable synchronization of dashboard-related data to that central site. A branch site can only report to one Central Primary Server. To register your branch site, you must first configure it to communicate with the central site.

To configure a branch site

1. Launch the Branch Configuration wizard and click Next to start.

   The Provide Central Site Information screen appears.

   Important! For a branch site to properly communicate to the central site, you must provide three access and location parameters: the name (or IP address) of the Central Primary Server, the Port number to access the Central Primary Server, and the authentication Password for the AS_CDASH_USR user. You need to obtain this information before attempting to register your branch site.



2. Specify the name of the Central Primary Server, the Port number to the Central Primary Server, and the authentication Password.

   When the branch site connects to the central site, the connection will use this information to access the central site.

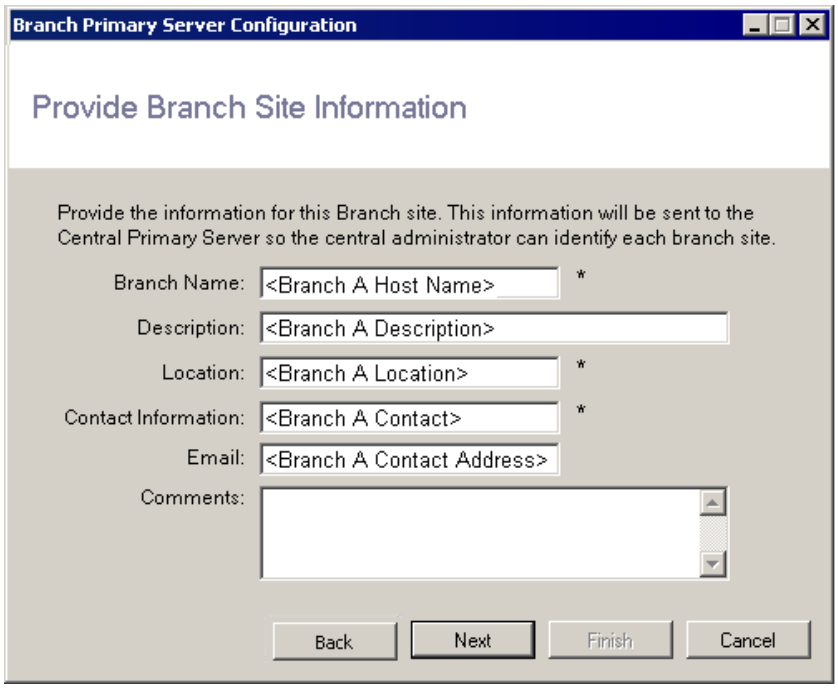
   By default, the Port number is 18001, but can be changed from the central site. For more information about changing the port number from the central site, see Configure the Central Site (see page 213).

3. Click Test to verify proper connection to the central site.

   A test connection status message appears.

4. If the test connection status is successful, click OK to continue. If the test connection status is not successful, verify you have the proper central site information specified before continuing.

   The Provide Branch Site Information screen appears.



5. You must specify the name of the Branch Primary Server, a location, and the name of the contact at that branch. In addition, you can also specify some additional branch-related information to further help the central site administrator to identify the branch site. Information such as the email address for the branch contact and any useful comments that you want the central site administrator to know can all be helpful in effectively maintaining your Global Dashboard environment.

   This information specified for the branch site user will be sent to the Central Primary Server and kept in the Central Primary Server database.

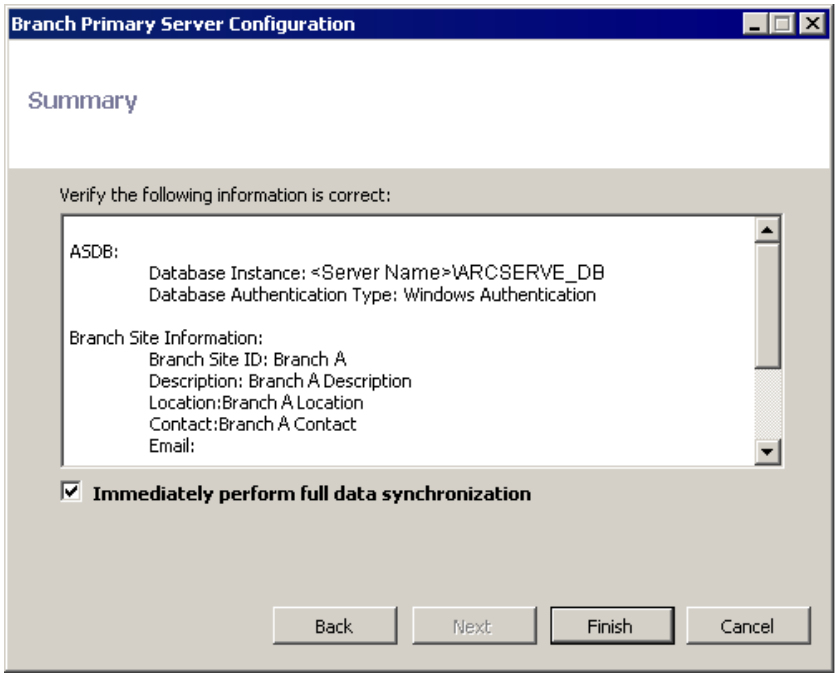
   Click Next to continue.

   a. If the name of the Branch Primary Server already exists, a message alert will appear informing you of this condition and requesting that you either specify a different branch name or have Arcserve Backup Global Dashboard automatically assign a new branch name (by appending a numerical suffix to your existing branch name).

      Click Yes to create an automatically appended branch name or click No to return to the Provide Branch Site Information screen and specify a different branch name.

b. If the name of the Branch Primary Server does not already exist, the branch configuration Summary screen appears.

The Summary screen displays all configuration-related information for the Central Arcserve Backup database, your branch site, and the Central Primary Server.



6. From the branch configuration Summary screen, you have the option to immediately perform a full data synchronization at this time.

Important! Data synchronization will temporarily interrupt and shut down the Arcserve Backup database engine and database for this branch site until the configuration and register process is complete. When the configuration and register process is finished, the Arcserve Backup database engine and all database functions will resume normally.

If you do not want to perform full data synchronization at this time, you can perform it after the configuration process is finished. For more information, see Manually Synchronize Data.

Note: The initial data synchronization will always be a full data synchronization. All subsequent data synchronizations will be incremental.

7. From the branch configuration Summary screen, verify that all displayed information is correct before continuing. If the information is correct, click Finish.

The Configuration Progress screen appears displaying the status.

8. When the configuration and register process is finished, a confirmation screen appears. Click OK.

   The branch configuration process is completed and the branch site is now registered to the central site.

Create File System Devices

Whether you want to back up files from your local machine or from a remote machine in your network, Device Configuration lets you take advantage of a large disk or disk array to use it as a backup resource.

To create file system devices

1. Open the Manager Console.

   From the Administration menu in the Navigation Bar on the Home Page, click Device Configuration.

   Device Configuration opens.

2. Select the File System Devices option and click Next.

   The Login Server dialog opens.

3. Complete the User Name and Password fields and click Next.

4. From the next Login Server dialog, select the server that you want to manage and click Next.

   The File System Devices Configuration dialog opens.

5. Click Add to create a new file system device.

   The new device appears in the File System Devices field.

6. Select the highlighted file system device under the File Device Name column, and specify a name for the device. Enter a description in the Description column, and enter a unique location in the Location column (for example, C:\FSD1, C:\FSD2, and so on). For remote file system devices, click Security and enter the user name, domain, and password for the remote computer. Click OK.

7. The status displayed in the Verify and Status column reads Pending while devices are being configured. Click the Verify button next to the status to check the accuracy of the information you provided. Arcserve Backup displays the Volume Size of the drive specified and a status of Pass if the information is valid.

If the status displayed is Failed:

- Make sure the paths you specified for the Location are unique for each device.
- Ensure the security credentials are accurate.
- Check that the volume is shared.

Note: From Device Configuration, you can add one or many devices. When you click Next, Arcserve Backup verifies the validity of information specified for all devices and alerts you if a particular device failed verification. Click the corresponding Verify button located in the Verify and Status column, or do so for each device as you configure it, to ensure successful verification before continuing. There are three possible outcomes displayed in this column:

- Pending--Displayed while a device is being configured.
- Pass-Displayed when verification of the information you specified succeeds.
- Failed--Displayed when Arcserve Backup finds problems with the information you specified. Click Failed in the Verify and Status column to obtain the cause of failure for each device that did not pass verification.

8. Click Exit to close Device Configuration.
9. Click Yes when the confirmation dialog appears.

You can choose the file system device you created as your backup media when you perform backups. Arcserve Backup lets you create multiple file system devices and treats them as additional media devices.

The user tutorial, My First Backup, provides information and a tutorial to guide you through the steps to configure your local disk as a backup device. My First Backup appears the first time you use Arcserve Backup and can also be accessed from the Help menu on the menu bar.

How to Define Include and Skip Parameters for Arcserve Backup Database Agents

Arcserve Backup contains registry keys that define the types of database related files that you can include or skip during backup jobs. Use of these keys is determined by the type of database agent you are running. Refer to the following list that defines the registry key, the affected database agents, and the types of files affected.

SkipDSAFiles

Note: This key was used in previous releases of Arcserve Backup.

For local server backups, the key is stored in the following registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve Backup\Base\Task\Backup

For agent backups, the key is stored in the following registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve Backup\ClientAgent\Parameters

Value Name: SkipDSAFiles

Type: DWORD

Value: 0 to back up and 1 to skip

- **Agent for Oracle**

  *.dbf
  Control*.*
  Red*.log
  Arc*.001

- **Agent for Lotus Domino**

  *.nsf
  *.ntf
  Mail.box

BackupDBFiles

For local server backups, the key is stored in the following registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve Backup\Base\Task\Backup

For agent backups, the key is stored in the following registry:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserveBackup\ClientAgent\Parameters

Value Name: BackupDBFiles

Type: DWORD

Value: 0 to skip and 1 to back up (0 is default)

- **Agent for Microsoft SQL Server**

  *.ldf
  *.mdf

  Except distmdl.ldf and distmdl.mdf, which cannot be skipped

- **Agent for Microsoft Exchange Server for database level backups and document level backups**

  *.chk
  *.log
  Res1.log
  Res2.log
  *.edb
  *.stm

  Note: This release of Arcserve Backup does not support brick level backups on Microsoft Exchange Server databases. In previous releases of Arcserve Backup, the SkipDSAFiles registry key was used to define the include and skip value for brick level backups.

Configuring Firewalls to Optimize Communication

In an environment where you are using multiple Arcserve Backup servers that reside across a firewall, or there is a firewall within a Storage Area Network (SAN) fibre loop, you must configure your servers to ensure the use of fixed ports and interfaces. The configuration on your Arcserve Backup servers must match your firewall configuration so that Arcserve Backup servers can communicate with each other.

A Arcserve Backup server communicates with other Arcserve Backup servers using a set of Remote Procedure Call (RPC) services. Each service can be identified by an interface (IP address) and a port. When you share data and tape libraries between Arcserve Backup servers, the services communicate with each other using the interface and port information provided by the RPC infrastructure. RPC infrastructure, however, does not ensure specific port assignment. Therefore, you must know your RPC infrastructure and port number assignments to configure your firewall properly. To achieve static binding, additional configuration is required.

You can customize your environmental port communication settings by modifying the ports configuration file (PortsConfig.cfg) located in the following directory:

CA\SharedComponents\ARCserve Backup

Note: You have the option to skip adding the firewall exceptions during the installation process by selecting the "Skip the Arcserve Services/Programs registration to Windows Firewall as Exceptions" option from the Firewall Registration screen. You can run the firewall exceptions at a later time by entering the following commands:

- For x64 - C:\Program Files (x86)\CA\SharedComponents\ARCserve Backup\Setup\r16\SetupFW.exe /INSTALL
- For x86 - C:\Program Files\CA\SharedComponents\ARCserve Backup\Setup\r16\SetupFW.exe /INSTALL

Ports Configuration File Guidelines

The following guidelines apply to modifying the ports configuration file:

- Changing port numbers requires the Arcserve Backup ServiceName.

  Note: For more information about service names, see Additional Resources - Firewall Ports Specifications (see page 245).

- Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Open Network Computing Remote Procedure Call (ONCRPC) services require only one port. If you do not provide a port number for these services, the default port is used.
- Microsoft Remote Procedure Call (MSRPC) services require only the Arcserve Backup service name (ServiceName). Arcserve Backup MSRPC-based services use system-assigned port numbers.
- You can use the key RPCServices for all Remote Procedure Call (RPC) services. This key lets Arcserve Backup use system-assigned ports for all Arcserve Backup RPC-based services.

- Changing the port configuration file on one Arcserve Backup server for MSRPC-based services does not ensure that Arcserve Backup applies the changes to all remote Arcserve Backup servers. You should modify the port configuration file on all remote Arcserve Backup servers.
- For TCP communication-based services, you can specify different port ranges for different host names with many IP addresses.
- You should specify an IP address only if a machine has more than one network interface card (NIC) and you want to use a specific NIC for TCP communication.

Note: For more information about specific Microsoft Windows system port requirements, see the Microsoft Support website.

Modify the Ports Configuration File

This section describes how to configure the protocols and ports that Arcserve Backup uses to communicate in your environment.

To modify the ports configuration file

1. Open PortsConfig.cfg using a text editor such as Notepad. You can access the file from the following directory:

   (installation_drive):\Program Files\CA\SharedComponents\ARCserve Backup

2. Add one or more lines of code using the following format:

   ServiceName(%s) PortRange_1;PortRange_2;...;PortRange_n [HostName(%s)] [IPAddress(%s)]

   - Use one of the following formats to specify a port or port range:

     SinglePort(number)
     PortBegin(number) - PortNumberEnd(number)

   - Use the following format to specify an IP address:

     %d.%d.%d.%d

   - The ServiceName is a string without spaces.
   - The HostName is a string that represents a valid computer name.

3. Close PortsConfig.cfg and save your changes.
4. After changing the Portsconfig.cfg file, restart all services affected by the changes. For all Arcserve Backup services, you can run cstop and cstart to stop and start the services.

To support backward compatibility, the keys corresponding to Arcserve Backup database agents are written to the PortsConfig.cfg file below the comment section. The database agents affected are the Tape Engine (tapeengine), the Job Engine (jobengine), and the Database Engine (databaseengine). These Arcserve Backup database agents send jobs to the Arcserve Backup queue using old ports. If you do not have old agents using old ports in your network, you can safely remove these lines from the PortsConfig.cfg file. However, you must restart each Arcserve Backup database agent service to enable communication using system ports.

Note: For more information about requirements for Microsoft Windows system services ports, see the Microsoft Support website.

Ports Used by Arcserve Backup Components

The following sections provide information about ports used by Arcserve Backup components, primarily for Windows configurations.

This section contains the following topics:

External Ports Used for Communication (see page 226)
Ports Used by the Arcserve Backup Base Product (see page 227)
Ports Used by Arcserve Backup Common Components (see page 236)
Ports Used by Arcserve Backup Agents and Options (see page 237)
How to Allow Agents and Database Agents to Communicate through a Firewall (see page 242)
Arcserve Backup Dashboard for Windows Firewall Communication Configuration (see page 244)
Additional Resources - Firewall Ports Specifications (see page 245)

External Ports Used for Communication

Arcserve Backup uses the following external ports for communication:

Port 135

This is owned by Microsoft endpoint-mapper (Locator) Service and is not configurable. All Arcserve Backup MSRPC services register their current ports with this service.

All Arcserve Backup clients (for example, the Manager) contact this service to enumerate the actual port used by the Arcserve Backup service and then contact the service directly.

Port 139/445

This is owned by Microsoft and is not a configurable port. Arcserve Backup services use MSRPC over the Named Pipes transport. Microsoft requires this port to be open for all communication using MSRPC over Named pipes. Be aware of the following:

- Port 139 is used only when the Arcserve Backup services are installed on Windows NT.
- Port 445 is used only when the Arcserve Backup services are installed on Windows XP, Windows Server 2003, and Windows Server 2008.

Port 53

This port allows Windows computers to reach each other using Domain Name Server (DNS) communication. Arcserve Backup uses port 53 to enable name resolution, which allows primary servers, stand-alone servers, member servers, and agent servers to communicate with each other.

You can find Microsoft Windows System port requirements at the following URL:

http://support.microsoft.com/kb/832017/en-us

Ports Used by the Arcserve Backup Base Product

For the Arcserve Backup base product, you can configure the following ports in the PortsConfig.cfg file:

CA Remote Procedure Call service

This is the ONCRPC portmapper service. Other ONCRPC services such as caserved, cadiscovd, caathd, lqserver, camediad, and idbserver use this service for registration. Clients that communicate using the other ONCRPC services first contact the ONCRPC portmapper service to enumerate the ports, and then contact the other ONCRPC service to communicate.

- Default Port: 111
- Protocol: TCP

Domain service (Cadiscovd.exe)

This service maintains a database of users, passwords, equivalences, and hosts for the Arcserve Backup domain concept. This service is required for GUI communication.

- Default Port: Dynamic Port
- Protocol: TCP

Service controller (Caserved.exe)

This service is used to manage other services remotely and is required for GUI communication.

- Default Port: Dynamic Port
- Protocol: TCP

Authentication service (Caauthd.exe)

This service validates the caroot user login and equivalence. It is required for GUI and backup server communication.

- Default Port: Dynamic Port
- Protocol: TCP

LDBServer.exe

This service is used for database communication and can only be configured using the command line. This service is not required for GUI and backup server communication.

- Default Port: Dynamic Port
- Protocol: TCP

LQServer.exe

This service is used for job queue communication and can only be configured using the command line. This service is not required for GUI and backup server communication

- Default Port: Dynamic Port
- Protocol: TCP

Mediasvr.exe

This service is used for tape engine communication and can only be configured using the command line. This service is not required for GUI and backup server communication.

- Default Port: Dynamic Port
- Protocol: TCP

Carunjob.exe

This service uses a port range for reconnection logic (on network communication failure) with the agents.

- Default Port: Dynamic Port
- Protocol: TCP

MS Endpoint Mapper Service

This is not a configurable port.

- Default Port: 135
- Protocol: TCP

CA Management Service (casmgmtsvc.exe)

CA Management Service is a configurable service that lets Arcserve Backup command line utilities (for example, ca_backup and ca_restore) communicate under the following scenarios:

- Remote services communication

  Note: To communicate using remote services, CA Management Service requires a callback service.

- Arcserve server and client server communication

  Note: To communicate with the Arcserve server and the client server, CA Management Service requires a callback service.

Location of Configuration Files

- CA Management Configuration File: To modify the ports used by CA Management Service, you must modify the configuration file labeled mgmt.properties located in the following directory:

  <$ARCserve_Home>\MgmtSvc\conf\mgmt.properties

- Callback Services Configuration File: CA Management Service requires a callback service labeled clntportrange. clntportrange is a value listed in the mgmt.properties configuration file located in the following directory:

  <drive letter>\Program Files\CA\Shared Components\ARCserve Backup\jcli\conf\mgmt.properties

Remote Services Communication

The default values are as follows:

- Protocol: SSL
- Port (sslport): 7099
- usessl: True

The optional values are as follows:

- Protocol: NON SSL
- Port (nonsslport): 2099

The Callback Service values are as follows:

- Default port range: [20000-20100]
- Optional port ranges: [10000|19999] or [20000-20100|10000|19999]

Arcserve Server and Client Server Communication

The default values are as follows:

- Protocol: SSL
- Port (sslport): 7099
- usessl: True

The optional values are as follows:

- Protocol: NON SSL
- Port (nonsslport): 2099

The Callback Service values are as follows:

- Default port range (clntportrange): 7199
- Optional port ranges: [20000-20100|20000|19999]

Manager Console Communication with the Base Product

The Manager Console component contacts the remote services on the base product whose port numbers need to be configured in the PortsConfig.cfg file on the machine where the Arcserve Backup Manager Console manager component is installed. Additionally, these services are installed on the Manager Console component.

CA Remote Procedure Call Service

This is the ONCRPC portmapper service. It is used for registration by other ONCRPC services. All clients to those services first contact this service to enumerate the ports and contact that service.

- Default Port: 111
- Protocol: TCP

Primary Server and Member Server Communication Ports

This section describes the ports and protocols used to allow communication between the primary server and member servers in a Arcserve Backup domain. You can configure the following ports in the PortsConfig.cfg file:

CA Remote Procedure Call service

This is the ONCRPC portmapper service. Other ONCRPC services such as caserved, cadiscovd, caathd, lqserver, camediad, and idbserver use this service for registration. Clients that communicate using the other ONCRPC services first contact the ONCRPC portmapper service to enumerate the ports, and then contact the other ONCRPC service to communicate.

- Default Port: 111
- Protocol: TCP
- Appears in PortsConfig.cfg as: catirpc

Domain service (Cadiscovd.exe)

This service maintains a database of users, passwords, equivalences, and hosts for the Arcserve Backup domain concept. This service is required for GUI communication.

- Default Port: Dynamic Port
- Protocol: TCP
- Appears in PortsConfig.cfg as: cadiscovd

Service controller (Caservd.exe)

This service is used to manage other services remotely and is required for GUI communication.

- Default Port: Dynamic Port
- Protocol: TCP
- Appears in PortsConfig.cfg as: caservd

Authentication service (Caauthd.exe)

This service validates the caroot user login and equivalence. It is required for GUI and backup server communication.

- Default Port: Dynamic Port
- Protocol: TCP
- Appears in PortsConfig.cfg as: caauthd

LDBServer.exe

This service is used for proxy for database communication and can only be configured using the command line. This service is not required for GUI and backup server communication.

- Default Port: Dynamic Port
- Protocol: TCP
- Appears in PortsConfig.cfg as: cadbd

LQServer.exe

Used for proxy for job queue communication and can only be configured using the command line. This service is not required for GUI and backup server communication

- Default Port: Dynamic Port
- Protocol: TCP
- Appears in PortsConfig.cfg as: caqd

Mediasvr.exe

Used for proxy for tape engine communication and can only be configured using the command line. This service is not required for GUI and backup server communication.

- Default Port: Dynamic Port
- Protocol: TCP
- Appears in PortsConfig.cfg as:

Carunjob.exe

Uses a port range for reconnection logic (on network communication failure) with the agents.

- Default Port: Dynamic Port
- Protocol: TCP
- Appears in PortsConfig.cfg as: reconnection

CA Management Service (casmgmtsvc.exe)

CA Management Service is a configurable service that lets Arcserve Backup command line utilities (for example, ca_backup and ca_restore) communicate under the following scenarios:

- Remote services communication

  Note: To communicate using remote services, CA Management Service requires a callback service.

- Arcserve server and client server communication

  Note: To communicate with the Arcserve server and the client server, CA Management Service requires a callback service.

Location of Configuration Files

- CA Management Configuration File: To modify the ports used by CA Management Service, you must modify the configuration file labeled mgmt.properties located in the following directory:

  <$ARCserve_Home>\MgmtSvc\conf\mgmt.properties

- Callback Services Configuration File: CA Management Service requires a callback service labeled clntportrange. clntportrange is a value listed in the mgmt.properties configuration file located in the following directory:

  <drive letter>\Program Files\CA\Shared Components\ARCserve Backup\jcli\conf\mgmt.properties

Remote Services Communication

The default values are as follows:

- Protocol: SSL
- Port (sslport): 7099
- usessl: True

The optional values are as follows:

- Protocol: NON SSL
- Port (nonsslport): 2099

The Callback Service values are as follows:

- Default port range: [20000-20100]
- Optional port ranges: [10000|1999] or [20000-20100|10000|19999]

Arcserve Server and Client Server Communication

The default values are as follows:

- Protocol: SSL
- Port (sslport): 7099
- usessl: True

The optional values are as follows:

- Protocol: NON SSL
- Port (nonsslport): 2099

The Callback Service values are as follows:

- Default port range (clntportrange): 7199
- Optional port ranges: [20000-20100|20000\19999]

Universal Agent service (univagent.exe)

Provides a central service for Arcserve Backup Client Agent for Windows and other backup agents.

- Default Port: 6050
- Protocol: TCP or UDP
- Appears in PortsConfig.cfg as: fsbackupservice (TCP) or fsbackupserviceudp (UDP)

Job Engine (jobeng.exe)

Maintains and executes jobs from the Arcserve Backup Job Queue.

- Default Port: 6503
- Protocol: TCP
- Appears in PortsConfig.cfg as: jobengine

DB Engine (dbeng.exe)

Provides database services for Arcserve Backup products.

- Default Port: 6504
- Protocol: TCP
- Appears in PortsConfig.cfg as: databaseengine

Tape Engine (tapeeng.exe)

Manages the configuration and operation of backup devices for Arcserve Backup products.

- Default Port: 6502
- Protocol: TCP
- Appears in PortsConfig.cfg as: tapeengine

Discovery Service (casdscsvc.exe)

Lets the Arcserve Backup server discover Arcserve Backup products that are running on the network using TCP/IP, MailSlots, and Broadcasts.

- Default Port: 41523 (TCP) or 41524 (UDP)
- Protocol: TCP and UDP
- Appears in PortsConfig.cfg as: casdscsvctcp (TCP) or casdscsvcudp (UDP)

Global Dashboard Server Communication

Within the Global Dashboard environment, a Branch Primary Server synchronizes dashboard-related information to the designated Central Primary Server. Data is always transmitted one way, from the Branch Primary Server to the associated Central Primary Server where it is processed and stored in the Central ASDB. For a Branch Primary Server to properly communicate to the Central Primary Server, you must provide the proper Port number to access the Central Primary Server.

- Central Primary Server Default Port: 18001
- Protocol: TCP

Base Product Communication with Arcserve Backup Agents and Options

The Arcserve Backup server contacts the remote services on the agents whose port numbers need to be configured in the PortsConfig.cfg file on the machine where the Base product is installed.

Note: For more information, see Ports Used by Arcserve Backup Agents and Options (see page 237).

Ports Used by Arcserve Backup Common Components

The following sections provide information about the ports used by Arcserve Backup common components.

Discovery Service Communication Ports

The Discovery Service discovers Arcserve Backup products, agents, and options on Windows platforms. You can configure the following ports in the PortsConfig.cfg file:

Discovery broadcast and response packets

Lets Arcserve Backup receive data and send responses about Arcserve Backup products running in your environment.

- Default Port: 41524
- Protocol: UDP

Discovery response

Lets Arcserve Backup receive data about Arcserve Backup products running in your environment.

- Default Port: 41523
- Protocol: TCP

Discovery broadcast

Lets Arcserve Backup broadcast its own Arcserve Backup product information to the network.

- Default Port: dynamic
- Protocol: UDP

Common Agent for UNIX and Linux Communication Ports

This information applies to all UNIX and Linux based agents, including client agents, database agents, and application agents. You can configure the following ports in the agent.cfg file:

Receiving and responding to discovery broadcast packets

- Default Port: 41524
- Protocol: UDP

Browsing, backup operations, and restore operations

- Default Port: 6051
- Protocol: TCP

Ports Used by Arcserve Backup Agents and Options

The following sections provide information about the ports used by Arcserve Backup agents and options.

Agent for Microsoft SharePoint Server Communication Ports

For the SharePoint Database Router Agent and the SharePoint External Data Agent, you can configure the following ports in the PortsConfig.cfg file:

Universal Agent service

This service is used for browsing operations.

- Default Port: 6050
- Protocol: UDP

Universal Agent service

This service is used for browsing/backup/restore operations.

- Default Port: 6050
- Protocol: TCP

Note: For information about the communication ports used by the SharePoint Database Agent, see Agent for Microsoft SQL Server and Agent for Microsoft SharePoint Server Database Communication Ports (see page 240).

Client Agent for Windows Communication Ports

For the Client Agent for Windows, you can configure the following ports in the PortsConfig.cfg file:

Universal Agent service

This service is used for browsing operations.

- Default Port: 6050
- Protocol: UDP

Universal Agent service

This service is used for browsing, backup, and restore operations.

- Default Port: 6050
- Protocol: TCP

Agent for Microsoft Exchange Server Communication Ports

For backups using the Agent for Microsoft Exchange Server, you can configure the following communication ports in the PortsConfig.cfg file:

Universal Agent service

This service is used for browsing operations.

- Default Port: 6050
- Protocol: UDP

Universal Agent service

This service is used for browsing, backup, and restore operations.

- Default Port: 6050
- Protocol: TCP

To restore brick level backups from previous versions of the Agent for Microsoft Exchange Server, the following ports are used:

Backup Agent RPC service

This service is required for browsing the Arcserve Backup Manager and all brick level backup and restore operations.

- Default Port: 6071
- Protocol: TCP

MS Endpoint Mapper service

This is not a configurable port.

- Default Port: 135
- Protocol: TCP

MS port (only Windows NT)

This service is used for only MSRPC communication using Named Pipes. You cannot configure this port.

- Default Port: 139
- Protocol: TCP

MS port (only Windows XP and Windows Server 2003)

This service is used for only MSRPC communication using Named Pipes. You cannot configure this port.

- Default Port: 445
- Protocol: TCP

Agent for Microsoft SQL Server Communication Ports

For the Agent for Microsoft SQL Server, you can configure the following communication ports in the PortsConfig.cfg file:

Universal Agent service

This service is used for browsing operations.

- Default Port: 6050
- Protocol: UDP

This service is used for browsing, backup, and restore operations.

- Default Port: 6050
- Protocol: TCP

Agent for Microsoft SharePoint Server Database Communication Ports

For the Agent for Microsoft SharePoint Server, you can configure the following ports for database communication in the PortsConfig.cfg file:

Backup Agent Remote Service

This service is used only for TCP/IP backups and restores.

- Default Port: 6070
- Protocol: TCP

Backup Agent RPC Server

This service is required for GUI Browsing and for Named Pipes backup and restore operations.

- Default Port: 6071
- Protocol: TCP

MS Endpoint Mapper Service

This is not a configurable port.

- Default Port: 135
- Protocol: TCP

MS port (only Windows NT)

This service is used only for MSRPC using Named Pipes. This is not a configurable port.

- Default Port: 139
- Protocol: TCP

MS port (only Windows XP and Windows Server 2003)

This service is used only for MSRPC using Named Pipes. This is not a configurable port.

- Default Port: 445
- Protocol: TCP

NDMP NAS Option Communication Ports

For the NDMP NAS Option, you can configure the following communication ports in the PortsConfig.cfg file:

NAS filer service

This service is used for communication with the NAS filer service. It is not required for GUI, backup, and restore communications.

- Default Port: 10000
- Protocol: TCP

Arcserve Backup Database Agents Communication Ports

For Arcserve Backup database agents, the PortsConfig.cfg file specifies the following ports:

Note: The following settings apply to the Agent for Informix, the Agent for SAP R/3, the Agent for Oracle, the Agent for Lotus Notes, and the Agent for Sybase.

Backup Agent RPC Server

This service is required for GUI browsing and for backup and restore operations. You can configure this port.

Note: The following values do not apply to the Agent for Oracle.

- Default Port: 6071
- Protocol: TCP

Backup Agent RPC Server - Agent for Oracle

This service is required for GUI browsing and for backup and restore operations using the Agent for Oracle. You can configure this port.

- Default Port (Agent for Oracle on Windows platforms): 6050
- Default Port (Agent for Oracle on Linux and UNIX platforms): 6050
- Protocol (all Agent for Oracle platforms): TCP

MS Endpoint Mapper Service

Note: You cannot configure this port.

- Default Port: 135
- Protocol: TCP

MS port (only Windows NT)

This service is used for MSRPC using Named Pipes. You cannot configure this port.

- Default Port: 139
- Protocol: TCP

MS port (only Windows XP and Windows Server 2003)

This service is used for MSRPC using Named Pipes. You cannot configure this port.

- Default Port: 445
- Protocol: TCP

GUI Communication to Arcserve Backup Agents

The Arcserve Backup manager contacts the remote services on the agents whose port numbers need to be configured in the PortsConfig.cfg file on the machine where the manager component is installed.

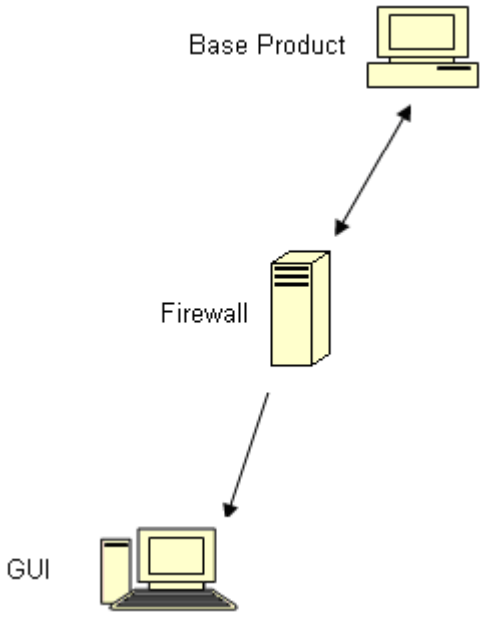
Note: For more information, see Ports Used by Arcserve Backup Agents and Options (see page 237).

How to Allow Agents and Database Agents to Communicate through a Firewall

The following sections provide examples about allowing Arcserve Backup agents and database agents to communicate through a firewall.

GUI Managing the Base Product

In the following scenario, a firewall separates the GUI and the machine where the base product is running.



On the machine where the base product is running, modify the Portsconfig.cfg file to contain the following entries:

```
ENABLE_CONFIGURABLE_PORTS=1
CASportmap          111
jobengine           6503
databaseengine      6504
tapeengine          6502
rtcports            6505
cadiscovd           9000
caservd             9001
caauthd             9003
caqd                9004
camediad            9005
cadbd               9006
reconnection        9010-9050
casdscsvctcp        41523
casdscsvcudp        41524
```

On the firewall, open these ports. These ports should allow incoming connections to the machine where the base product is running.

On the GUI machine, modify the Portsconfig.cfg file to contain the following entries:

```
ENABLE_CONFIGURABLE_PORTS=1
CASportmap          111    BaseproductMachinename
jobengine           6503    BaseproductMachinename
databaseengine      6504    BaseproductMachinename
tapeengine          6502    BaseproductMachinename
rtcports            6505    BaseproductMachinename
cadiscovd           9000    BaseproductMachinename
caservd             9001    BaseproductMachinename
caauthd             9003    BaseproductMachinename
casdscsvctcp        41523
casdscsvcudp        41524
```

Arcserve Backup Dashboard for Windows Firewall Communication Configuration

The installation wizard configures the firewall communication ports between Arcserve Backup server and the client system when you install Arcserve Backup and Arcserve Backup Dashboard for Windows.

The sections that follow describe the file names, locations, and required syntax for the configuration files, and the communication ports used on the client system and the Arcserve Backup server system.

Client System

The client system configuration file, labeled ClientConfig.xml, is installed in the directory that follows on the client system:

[ARCSERVE_HOME]/ClientConfig.xml

Syntax

The client system configuration file requires the syntax that follows:

```
<?xml version="1.0" encoding="utf-8" ?>
    <service>
    <primaryserver>LocalHost</primaryserver>
    <username>caroot</username>
    <port>6052</port>
    </service>
```

Arcserve Backup Server System

The Arcserve Backup server configuration file, labeled CA.ARCserve.CommunicationFoundation.WindowsService.exe.config, is installed in the directory that follows:

C:\Program Files\CA\ARCserve Backup

Syntax

The Arcserve Backup server configuration file requires the syntax that follows:

```
<services>
    <service name="CA.ARCserve.CommunicationFoundation.Impl.DBServicePInvokeImpl"
    behaviorConfiguration="DBServiceBehavior">
    <host>
    <baseAddresses>
    <add baseAddress="net.tcp://localhost:6052/DBService"/>
    </baseAddresses>
    </host>
    <endpoint binding="netTcpBinding" bindingConfiguration="BindingConfiguration"
    contract="CA.ARCserve.CommunicationFoundation.Contract.IDBService" address=""></endpoint>
    </service>
    <service name ="CA.ARCserve.CommunicationFoundation.Impl.AuthServiceImpl"
    behaviorConfiguration="AuthServiceBehavior">
    <host>
    <baseAddresses>
    <add baseAddress="net.tcp://localhost:6052/AuthService"/>
    </baseAddresses>
    </host>
    <endpoint address="" binding="netTcpBinding" bindingConfiguration="BindingConfiguration"
    contract="CA.ARCserve.CommunicationFoundation.Contract.IAuthService" />
    </service>
</services>
```

Additional Resources - Firewall Ports Specifications

The following tables list the Arcserve Backup services that you can configure using the ports configuration file:

Arcserve Backup MSRPC Services

Service Display Name	Process Name	Key	Default Port	Service Type
Agent RPC Server	dbasvr.exe	dbagentsrpcserver	System port	MSRPC
Tape Engine	tapeeng.exe	tapeengine	6502	MSRPC
Job Engine	jobeng.exe	jobengine	6503	MSRPC

Service Display Name	Process Name	Key	Default Port	Service Type
Database Engine	dbeng.exe	databaseengine	6504	MSRPC
Message Engine	msgeng.exe	rtcports	System port	MSRPC

Arcserve Backup TCP Services

Service Display Name	Process Name	Key	Default Port	Service Type
Universal Agent	univagent.exe	fsbackupservice	6050	TCP
Discovery service	casdscsvc.exe	casdscsvctcp	41523	TCP
NDMP NAS Option Agent	tapeeng.exe, UnivAgent.exe	nastcpservice	10000	TCP
Reconnection	carunjob.exe	reconnection	no port	TCP

Arcserve Backup ONCRPC Services

Service Display Name	Process Name	Key	Default Port	Service Type
Remote Procedure Call Server	Catirpc.exe	catirpc	111	ONCRPC
Service Controller	caserved.exe	caservd	System port	ONCRPC
Domain Server	cadiscovd.exe	cadiscovd	System port	ONCRPC
Domain Server	caauthd.exe	caauthd	System port	ONCRPC
caqd	lqserver.exe	caqd	System port	ONCRPC
cadbd	ldbserver.exe	cadbd	System port	ONCRPC
camediad	mediasvr.exe	camediad	System port	ONCRPC

Arcserve Backup UDP Services

Service Display Name	Process Name	Key	Default Port	Service Type
Universal Agent	univagent.exe	fsbackupservice	6050	UDP
Discovery service	casdscsvc.exe	casdscsvcudp	41524	UDP

Examples of How You Can Modify the Ports Configuration File

This section describes examples of modifying the PortsConfig.cfg file.

- Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Open Network Computing Remote Procedure Call (ONCRPC) services require only one port. If you do not provide a port number for these services, the default, hard-coded port is used. If you specify a port range, only the first available port from the range is used. The following examples show how to change a TCP service:

```
sqlagenttcpservice          8000    machine_name
fsbackupservice     7000    machine_name
```

- Machines A and D are Arcserve Backup servers, machines B and C are Client Agent machines, and you want to change the communication port between machine A and B to 7000. Also, on machine A, there is a client agent installed for the Arcserve Backup server on machine D, and you want to change the communication port from D to A to 8000.

  On machine B (Client Agent), modify the PortsConfig.cfg file to contain the following entries:

  ```
  ENABLE_CONFIGURABLE_PORTS = 1
  fsbackupservice          7000      MachineB
  fsbackupserviceudp                 7000      MachineB
  ```

  Be aware of the following:

  - You can perform this change using the Network Configuration application that is installed with the Backup Agent Admin.

    Note: For more information, see the *Client Agents Guide*.

  - You must restart the Universal Agent service.

  To allow machine A to browse and back up files on machine B, modify the Portsconfig.cfg file on machine A to contain the following entries:

  ```
  ENABLE_CONFIGURABLE_PORTS = 1
  fsbackupservice          7000   MachineB
  fsbackupserviceudp                 7000   MachineB
  ```

  Note: To apply this configuration, you must stop and restart all services on machine A using the cstop/cstart commands.

  To allow the client agent from machine A to communicate with Arcserve Backup machine D, modify the PortsConfig.cfg file on machine A and machine D to contain the following entries:

  ```
  ENABLE_CONFIGURABLE_PORTS = 1
  fsbackupservice          8000      MachineA
  fsbackupserviceudp                 8000      MachineA
  ```

  Be aware of the following:

  - You must restart the Universal Agent on machine A.
  - You must restart all Arcserve Backup services on machine D using the cstop and cstart commands.

  Note: You can apply this logic to the Arcserve Backup Agent for Microsoft SQL Server (sqlagenttcpservice) for TCP-based services (fsbackupservice, sqlagenttcpservice).

- For Arcserve Backup MSRPC services, the following occurs:

  MSRPC listens over ncacn_ip_tcp and ncacn_np protocols. The ncacn_ip_tcp uses system assigned ports by default rather than hard-coded ports. The hostname and IP address are not required for the RPC Services.

  For example, the following could be a change for an MSRPC service:

  dbagentsrpcserver 9000

  This setting means that the Arcserve Backup Agent RPC Server will try to use port 9000.

  dbagentsrpcserver 9000;9001

  This setting means that the Arcserve Backup Agent RPC Server will try to communicate using port 9000. If it does not succeed, it will try to use port 9001. If it does not succeed Arcserve Backup will write a message in the Windows Application Activity Log.

  dbagentsrpcserver 9000-9500

  This setting means that the Arcserve Backup Agent RPC Server tries to communicate using port 9000. If it does not succeed Arcserve Backup will try to communicate using port 9001, and continue to trying to communicate up to port 9500.

  If it cannot use any port in the range, will write a message in the Windows Application Activity Log.

Ports Configuration File Configuration Considerations

When modifying the PortsConfig.cfg file, consider the following scenarios:

- When you want to change the Network Attached Storage (NAS) port on the Arcserve Backup server after installing the Arcserve Backup NDMP NAS Option, you must change the port assignment on the NAS filer as well.
- Circumstances may arise when you want to specify a custom port or a range of ports for NAS filer to server backups. For example, there is a firewall between the backup server and the NAS filer. To specify custom ports, do the following:

  1. Log in to the backup server and open the following ports configuration files:

     Windows x64 operating systems

     C:\Program Files (x86)\CA\SharedComponents\ARCserve Backup\PortsConfig.cfg

     and

     C:\Program Files\CA\SharedComponents\ARCserve Backup\PortsConfig.cfg

     Windows x86 operating systems

     C:\Program Files\CA\SharedComponents\ARCserve Backup\PortsConfig.cfg

  2. Set ENABLE_CONFIGURABLE_PORTS=1

3. Add filertoserver 10000;10001-10005
4. Close and save the ports configuration files.
5. Restart all Arcserve Backup services on the backup server using the cstop.bat and cstart.bat batch files.
6. Repeat Steps 1 through 5 on all primary and member servers.

- The reconnection logic is implemented to avoid an existing network problem. This can occur when you perform client agent backups over the network. During the backup, the connection can be lost and the backup fails. If this occurs, you can specify the reconnection key and a port range that will be used during the backup. Use the reconnection key on the Arcserve Backup server side.
- If you are using CA eTrust Firewall software, you should perform the following steps:
  - From the command prompt, access the following:

    \Program Files\CA\eTrust\Firewall\Engine
  - Enter the following command:

    fwadmin -msrpc_chk_states_off
- For remote computer management, Arcserve Backup RPC services listen using the ncacn_ip_tcp and ncacn_np protocols. When using ncacn_ip_tcp, open the tcp ports (6502, 6503, and 6504) and open the system ports 137-139, 445 which are used by the Windows operating system when the ncacn_np protocol is used.

  Note: If eTrust Firewall blocks RPC communication, Arcserve Backup can respond slowly or stop responding completely.
- To change the port for the Universal Agent, you must change the communication port for all agents and options that use this service that are installed on the same machine (for example, the Arcserve Backup Client Agent, the Arcserve Backup Agent for Microsoft Exchange Server, and the Arcserve Backup NDMP NAS Option). If you add a machine with a Windows XP or Windows Server 2003 operating system, browsing functionality is performed through the Universal Agent.
- Changing the ports for the Arcserve Backup Agent for Microsoft Exchange Server and the Arcserve Backup Agent for Microsoft SQL Server is for TCP backups for these agents. The RPC server lets you browse all Arcserve Backup for Windows database agents.

- If you are upgrading from an older version of Arcserve Backup and your current installation uses a configuration file labeled CAPortConfig.cfg for Arcserve Backup Client Agents configurations, the installation process migrates CAPortConfig.cfg settings to the PortsConfig.cfg file.

  For previous Arcserve Backup installations, information in the CAPortConfig.cfg file is in the following format:

  ```
  MachineName  IPAddress tcpport  udpport
  ```

  The above-described CAPortConfig.cfg settings migrate to PortsConfig.cfg in the following format:

  ```
  fsbackupservice          tcpport  machinename  IPAddress
  fsbackupserviceudp       udpport  machinename  IPAddress
  fsbackupserviceunix      tcpport  machinename  IPAddress
  ```

Note: For more information about requirements for Microsoft Windows system services ports, see the Microsoft Support website.

Test Communication Through a Firewall

Windows platforms provide you with a command line utility called ping.exe that lets you test communication between computers.

To ensure that your systems can communicate through a firewall, ping.exe should be able to communicate with the other computers across the firewall (both directions) using the computer name.

To test communication though a firewall

1. Open the Windows Command Line.
2. From the prompt, specify the following syntax replacing MACHINE with the actual machine name:

   ```
   ping.exe MACHINE
   ```

Chapter 8: Uninstalling Arcserve Backup

This section contains the following topics:

Uninstall Arcserve Backup (see page 253)
Uninstall Arcserve Backup Components Using the Command Line (see page 255)
Uninstall Agent Deployment Setup Files (see page 258)

Uninstall Arcserve Backup

You can uninstall Arcserve Backup using the Add and Remove Programs application located in the Windows Control Panel.

To ensure that Arcserve Backup is completely uninstalled from your system, you should uninstall all Arcserve Backup components that appear in the Uninstall Components dialog. For example, you should uninstall Arcserve Backup Client Agent for Windows, Arcserve Backup Agent for Microsoft SQL Server, Arcserve Backup Diagnostic Utility, and so on.

You can uninstall the following Arcserve Backup components from Windows Add or Remove Programs:

- Arcserve Backup (base product)
- Arcserve Backup Agent for Informix
- Arcserve Backup Agent for Lotus Domino
- Arcserve Backup Agent for Microsoft Exchange Server
- Arcserve Backup Agent for Microsoft SharePoint Server
- Arcserve Backup Agent for Microsoft SQL Server
- Arcserve Backup Agent for Open Files for Windows
- Arcserve Backup Agent for Oracle
- Arcserve Backup Agent for Sybase
- Arcserve Backup Agent for Virtual Machines
- Arcserve Backup Client Agent for Windows
- Arcserve Backup Diagnostic Utility

- Arcserve Backup Disaster Recovery Option
- Arcserve Backup Enterprise Module
- Arcserve Backup Enterprise Option for SAP R/3 for Oracle
- Arcserve Backup Global Dashboard
- Arcserve Backup Image Option
- Arcserve Backup NDMP NAS Option

Use the Server Admin Manager to uninstall the following Arcserve Backup components:

- Arcserve Backup Central Management Option
- Arcserve Backup Tape Library Option
- Arcserve Backup Storage Area Network (SAN) Option

The uninstallation routine removes all Arcserve Backup components, directories, files, and so on from your computer, except for following directories and all of their contents:

- CA Licensing:
  - (x86 systems) C:\Program Files\CA\SharedComponents\CA_LIC
  - (x64 systems) C:\Program Files(X86)\CA\SharedComponents\CA_LIC

  Note: If there are no other applications on your computer using these files, you can safely delete them.
- C:\Program Files\CA\SharedComponents\Jre\JRE-1.7.0

  If you upgraded from a previous Arcserve Backup release, and the previous release was integrated with a previous version of Java Runtime Environment (JRE), the uninstallation routine does not remove the directory and files associated JRE 1.7.0 and any previous versions of JRE from your system.

  Note: If there are no other applications on your computer using these files, you can safely delete them.
- C:\Program Files\CA\ARCserve Backup

  The uninstallation routine does not remove files in this directory that were modified or created as a result of cluster installation.

  Note: You can safely delete this directory after Arcserve Backup is uninstalled from the last cluster node.
- C:\Program Files\CA\ARCserve Backup\ASDBBackups.txt

  The uninstallation routine does not remove Arcserve database log files that were created in a cluster installation. Arcserve database log files can be labeled ASDBBackups.txt and ASDBBackups.X.txt.

  Note: If you do not plan to reinstall Arcserve Backup in a cluster, you can safely delete this directory after Arcserve Backup is uninstalled from the last cluster node.

To uninstall Arcserve Backup

1. Close the Arcserve Backup Manager Console.
2. Open the Windows Control Panel.

   Double-click Add or Remove Programs.

   The Add or Remove Programs dialog opens.
3. Browse to and select Arcserve Backup.

   Click Remove.

   The Components dialog opens.
4. Select the Arcserve Backup components that you want to uninstall and click Remove.

   The Arcserve Backup components specified are uninstalled from your computer.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Uninstall Arcserve Backup Components Using the Command Line

Windows Server 2008 Server Core is a minimal installation option for servers running Windows Server 2008. Windows Server Core contains minimal user interface functionality. The primary method of interacting with Server Core is via the command line.

Due to the lack of a user interface, situations may arise that require you to uninstall Arcserve Backup components, agents, and options using the Windows command line. For example, you need to uninstall the Arcserve Backup Disaster Recovery Option from a Windows Server 2008 system that is running Server Core.

In this release, you can install the components that follow on a Windows Server 2008 System that is running Server Core.

- Arcserve Backup Member server and supported options
- Arcserve Backup Agent for Open Files
- Arcserve Backup Agent for Virtual Machines
- Arcserve Backup Client Agent for Windows
- Arcserve Backup for Windows Disaster Recovery Option

Important! The procedure that follows describes the steps to uninstall all Arcserve Backup components from all Windows operating systems using the command line.

To uninstall Arcserve Backup components using the command line

1. Log in to the computer where you want to uninstall Arcserve Backup components.

   Note: You must log in to the computer using an administrative account.

2. Open the Windows command line.

   Execute the syntax that corresponds with the architecture of the computer's operating system:

   - x**86 operating systems:**

     %ProgramFiles%\CA\SharedComponents\ARCserve Backup\Setup\r16\uninstall.exe /p <ProductCode>

   - **x64 operating systems:**

     %ProgramFiles%(x86)\CA\SharedComponents\ARCserve Backup\Setup\r16\uninstall.exe /p <ProductCode>

   <ProductCode>

   The table listed below defines the product code that you must specify for the Arcserve Backup component that you want to uninstall.

   Example:

   Use the following syntax to uninstall the Arcserve Backup base product from a Windows x86 operating system using the command line:

   %ProgramFiles%\CA\SharedComponents\ARCserve Backup\Setup\r16\uninstall.exe /p {CAABDF1F-E6BC-483F-B7E5-CEEF32EBE841}

Component	Platform	<Product Code>
BrightStorSAK	x86	{CAABD359-0497-414E-9423-711FDC90B38B}
Arcserve Backup (Base Product)	x86	{CAABD1E0-CC76-4057-BEC0-F55D76BB8D05}
Arcserve Backup Agent Deployment Packages	x86	{CAABD1C4-50E7-402E-80CB-AB0AAF8B6066}
Arcserve Backup Agent for Informix	x86	{CAABD568-F3FC-468E-92A4-2EDA409231D8}
Arcserve Backup Agent for Lotus Domino	x86	{CAABD126-715C-4484-B973-FFC0023F5F49}
Arcserve Backup Agent for Microsoft Exchange	x86	{CAABD938-ACC3-4F97-9E89-BC0DA98B02DB}
Arcserve Backup Agent for Microsoft Exchange 12	x64	{CAABD353-614B-4E13-B27A-CA538040E874}

Component	Platform	<Product Code>
BrightStorSAK	x86	{CAABD359-0497-414E-9423-711FDC90B38B}
Arcserve Backup Agent for Microsoft SharePoint 2007	x86	{CAABD3E6-9580-4D44-8C90-007963464B66}
Arcserve Backup Agent for Microsoft SharePoint 2007	x64	{CAABD7A3-77C0-4488-A852-7B40C197D3E6}
Arcserve Backup Agent for Microsoft SQL Server	x86	{CAABDC9E-4DDE-4036-A8EF-AFC00091DE45}
Arcserve Backup Agent for Microsoft SQL Server	x64	{CAABD7A7-60FC-48D7-9B12-36E332EF6477}
Arcserve Backup Agent for Open Files for Windows	x86	{CAABD8CF-8E01-49DE-BAB7-DCB33DDF676A}
Arcserve Backup Agent for Open Files for Windows	x64	{CAABDD41-1935-4C04-AE4B-803EF455E1A3}
Arcserve Backup Agent for Oracle	x86	{CAABD914-ED4B-44E9-BBCE-3312A25583F6}
Arcserve Backup Agent for Oracle	x64	{CAABD2F1-63E6-416F-A361-343CAF549883}
Arcserve Backup Agent for Sybase	x86	{CAABDDB2-A533-4C4E-AE7A-6F1300B085BB}
Arcserve Backup Agent for Virtual Machines	x86	{CAABD4D7-AF38-4BCE-89FA-1A8E76CCAEF9}
Arcserve Backup Agent for Virtual Machines	x64	{CAABD63D-2328-4353-B271-F08B4E21E0F5}
Arcserve Backup Client Agent for Windows	x86	{CAABD7A8-3190-4D8A-B0AC-4F43421F4A1D}
Arcserve Backup Client Agent for Windows	x64	{CAABD00D-1FA6-48CD-AD28-75BABE0522AE}
Arcserve Backup Diagnostic Utility	x86	{CAABD34D-F821-41CE-B4D2-5E06B86878F7}
Arcserve Backup Disaster Recovery Option	x86	{CAABD400-8ABB-40E9-A3B0-C72069ED796C}
Arcserve Backup Enterprise Module	x86	{CAABDA6A-9EED-4C96-9AB2-BCA270A9C22F}
Arcserve Backup Enterprise Option for SAP R3 for Oracle	x86	{CAABDAEE-B05D-4E60-8858-BFD874D833D5}
Arcserve Backup Enterprise Option for SAP R3 for Oracle	x64	{CAABD200-0E1D-4640-9483-376C21B3975A}
Arcserve Backup Image Option	x86	{CAABDAA9-1DFA-4811-BE57-1B22D9823E82}
Arcserve Backup Microsoft Windows EBS Option	x86	{CAABDC3B-9375-4AF8-AB1B-8555A6281E6A}
Arcserve Backup NDMP NAS Option	x86	{CAABD971-BF83-4817-965E-DACA6732E854}

Component	Platform	<Product Code>
BrightStorSAK	x86	{CAABD359-0497-414E-9423-711FDC90B38B}
Arcserve Backup Serverless Backup Option	x86	{CAABDCC6-9EB1-45BD-9113-E5087032A7DB}
Arcserve Backup Setup Support Files	x86	{CAABD0BC-0C3F-4E38-AF09-2300389691FF}
CA ARCserve Discovery Service	x86	{CAABDC77-9350-47CF-ADC1-682C60F70E2E}
CA ARCserve Universal Agent for Windows	X86	{CAABDEFE-0449-4AA1-8A7C-085EA5A52ECB}
CA ARCserve Universal Agent for Windows	X64	{CAABD4AD-A551-4AA4-82ED-87247EB7DD72}
Central Dashboard	x86	{CAABD3A2-C0CD-4F3C-A8B2-D55353C1225E}

After the command executes, the component is uninstalled.

Uninstall Agent Deployment Setup Files

Arcserve Backup does not contain a routine that lets you uninstall Agent Deployment Setup Files. If you need to free disk space on the Arcserve Backup server, you can safely delete Agent Deployment Setup Files from the Arcserve Backup server without adversely affecting your Arcserve Backup installation.

The best practice for uninstalling Agent Setup Files from your primary, member, or stand-alone server is to use steps described in this section.

To uninstall Agent Deployment Setup Files

1. Log in to the Arcserve Backup server.

   Note: The Arcserve Backup Manager Console can be open, however, Agent Deployment must be closed.

2. Open a command line window and execute the command that follows:

   - **x86 Platforms:**

     C:\Program Files\CA\SharedComponents\ARCserve Backup\Setup\r16\Uninstall.exe" /q /p {CAABD375-B0AA-4511-A384-439D5CBC6D94}

   - **x64 Platforms:**

     C:\Program Files (x86)\CA\SharedComponents\ARCserve Backup\Setup\r16\Uninstall.exe" /q /p {CAABD375-B0AA-4511-A384-439D5CBC6D94}

   Agent Deployment Setup Files are deleted from the Arcserve Backup server.

Note: To run Agent Deployment after the setup files are deleted from the Arcserve Backup server, do one of the following:

- Re-install Agent Deployment Setup Files using the Arcserve Backup installation media.
- Execute Agent Deployment and provide the Arcserve Backup installation media when prompted.

Appendix A: Troubleshooting Arcserve Backup Installations

This section contains the following topics:

Setup Cannot Communicate with Remote Microsoft SQL Server Databases (see page 261)
Unable to Log In to Arcserve Backup After Installing This Release (see page 263)
Arcserve Backup Services Fail to Initialize (see page 264)
The Tape Engine Does Not Start on Member Server Upgrades (see page 265)
Unable to Log in to Arcserve Backup After Upgrading to This Release (see page 265)
Unable to Determine What Devices Are Supported by Arcserve Backup (see page 266)
Cluster HA Resources Not Created (see page 268)

Setup Cannot Communicate with Remote Microsoft SQL Server Databases

Valid on Windows platforms.

Symptom

Setup cannot communicate with Microsoft SQL Server database instances installed on remote computers. As a result, the installation process fails.

Solution

ODBC communicates with the SQL Server browser service using UDP port 1434 to detect the TCP port that SQL Server is using to communicate. ODBC then uses the detected port to communicate with SQL Server. If UDP port 1434 is blocked, Setup cannot communicate with remote Microsoft SQL Server instances, which causes the installation process to fail.

To help ensure that Setup can communicate with remote Microsoft SQL Server databases, verify whether UDP port 1434 is blocked or not blocked. Then do one of the following:

- **UDP port 1434 is blocked**--If UDP port 1434 is blocked, configure the ODBC data source to specify port 1433 as the TCP/IP port number of the System DSN. To set the port number, do the following:

  1. Open Odbcad32.exe located in the following directory:

     - **x86 systems:**

       %systemdrive%\Windows\system32

     - **x64 systems:**

       %systemdrive%\Windows\SysWoW64

     The ODBC Data Source Administrator dialog opens.

  2. Click the System DNS tab and then click Add.

     The Create New Data Source dialog opens.

  3. Specify SQL Server as the data source and click Finish to continue.

     The Create a New Data Source to SQL Server dialog opens.

  4. Complete the following fields on the Create a New Data Source to SQL Server dialog:

     - **Name**--The name of the data source. For example, testmachine1.
     - **Server**--The name of the SQL Server system. For example, testmachine1\mysqlserver.

     Click Next.

  5. On the next dialog, click Client Configuration.

     The Add Network Library Configuration dialog opens.

  6. On the Add Network Library Configuration dialog, clear the checkmark next to Dynamically determine port number.

     In the Port field, specify 1433.

     Click Finish.

     UDP port 1433 is applied.

- **UDP Port 1434 is not blocked**--If UDP port 1434 is not blocked, verify that the SQL Server browser service is enabled.

  Note: The SQL Server browser service is disabled when you install Microsoft SQL Server.

Unable to Log In to Arcserve Backup After Installing This Release

Valid on Windows platforms.

Symptom

After you perform a new installation of Arcserve Backup, you cannot log in to Arcserve Backup.

Solution

The services responsible for authenticating users may not be running. From the Control Panel, open the Service Panel and verify that the following services are running:

- Arcserve Backup Domain Server
- Arcserve Backup Service Controller
- CA Remote Procedure Call Server

You can also check this by opening the Task Manager and looking for the application caauthd. If you do not find an instance of this application in the Task Manager, go to the Services Panel, stop and start the Arcserve Backup Domain Server, and try to log in to the Arcserve Backup Manager Console again. If you still cannot log in, open the command window, change the directory to the Arcserve Backup home directory, and run the following commands:

```
ca_auth –user getall
```

The output on the screen should be similar to the following:

```
User names:
caroot
```

If you do not see at least one user, caroot, or if you receive some other error when running the command, run the following debugging authentication commands so that you can send the logs to Arcserve Backup support for investigation:

- ping the machine by name. For example:

  ```
  ping.exe BAB_MACHINE
  ```

  In this example, BAB_MACHINE is your machine. If this does not work, resolve the name to an IP address by changing the etc/hosts file or on the DNS.

  Enter the following command

  ```
  ipconfig /all > ipconfig.log
  ```

- Enter the following command to tell Technical Support if the portmapper is running on your machine:

  ```
  netstat -na >netstat.log
  ```

- Enter the following command to let Technical Support know which Arcserve Backup services have registered with the rpc server running on the client machine:

  rpcinfo.exe -p BAB_MACHINE >rpcinfo.log

  In this syntax, BAB_MACHINE is your machine.

- Enter the following command:

  rpcinfo.exe -t BAB_MACHINE 395648 1 > caauthd.txt

  In this syntax, BAB_MACHINE is your machine.

  Note: Using '>' to a file does not show the results on the screen.

- Create the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\Base\LogBrightStor\[DWORD]DebugLogs ==1

  This creates the rpc.log file in the Arcserve Backup home directory under \log.

Arcserve Backup Services Fail to Initialize

Valid on Windows platforms.

Symptom:

Why are my Arcserve Backup services failing to initialize?

Solution:

Arcserve Backup requires a portmapper for its RPC engines. The Windows service, CA Remote Procedure Call Server, provides the portmapper functionality and uses the standard portmap, port 111.

If Arcserve Backup detects port 111 conflicts, indicating that it is using the same port number for the CA Remote Procedure call server service as a previously installed portmapper, Arcserve Backup automatically switches to another port number.

If you want other computers to be able to communicate with your computer, we recommend that you configure a specific port. To do so, use the file labeled portsconfig.cfg file located in the directory that follows:

C:\Program Files\CA\SharedComponents\ARCserve Backup

Arcserve Backup can work with external portmappers (Microsoft Services for UNIX (SFU), Noblenet Portmapper, StorageTek LibAttach, and so on). However, during the machine boot up sequence, Arcserve Backup services may try to initialize before the external portmapper has fully initialized. Under these circumstances, Arcserve Backup services then fail to initialize. To avoid this problem, perform the following steps:

1. Create the following registry key:

   HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA ARCserve Backup\Base\Portmap

2. Create the DWORD DelayedRegistration under this key.
3. Assign a decimal value for this key, indicating the number of minutes Arcserve Backup services wait before initializing portmapper registration. For example, DelayedRegistration=1 causes all Arcserve Backup services to start but not register with the portmapper for one minute after startup.

The Tape Engine Does Not Start on Member Server Upgrades

Valid on Windows platforms.

Symptom:

After you upgrade a stand-alone server or a primary server from a previous release to a member server, the Tape Engine on the member server does not start.

Solution:

After you complete the process of upgrading a primary server or a stand-alone server to a member server, the Tape Engine on the member server should start automatically. If the Tape Engine on the member server does not start automatically, check the status of the Tape Engine on the primary server. In all probability, the Tape Engine on the primary server was not running when the upgrade process on the member server completed.

To remedy this problem, ensure that the Tape Engine is running on the primary server. If necessary, you can start the Tape Engine on the primary server using the Server Admin Manager. Then, after you are sure that the Tape Engine is running on the primary server, start the Tape Engine on the member server.

Note: For more information about starting and stopping Arcserve Backup engines, see the *Administration Guide*.

Unable to Log in to Arcserve Backup After Upgrading to This Release

Valid on Windows platforms.

Symptom

User profiles do not migrate when you upgrade to this release of Arcserve Backup. As a result, the users cannot log in to the Arcserve Backup managers and domain.

Solution

This problem only affects upgrades from previous releases of Arcserve Backup, such as Arcserve Backup r12.5. The problem occurs under one or both of the following conditions:

- The IP address of the backup server was changed before you started the upgrade process.
- The backup server was rebooted after the upgrade was complete and then the IP address was changed.

As a result of the above conditions, the user accounts that you added in the previous release do not migrate as you upgrade to this release of Arcserve Backup. To remedy this problem, you must re-create equivalence on the backup server using the ca_auth command (based on the new IP address), and then update the user accounts.

To complete this task, do the following:

1. From the Arcserve Backup server, open a Command Line window.
2. Execute ca_auth using the following syntax:

   ca_auth -equiv add <domainnameA\NT user(administrator)> <hostnameA> caroot caroot <passwordofcaroot>

   Equivalence is created.
3. Execute the following commands for each user account:

   caauthd.exe -setupuser
   cadiscovd.exe -m

   The user account information is updated.

Note: The command line utilities are stored in root of the Arcserve Backup installation directory. For example:

C:\Program Files\CA\ARCserve Backup\caauthd.exe

Unable to Determine What Devices Are Supported by Arcserve Backup

Valid on Windows platforms.

Symptom:

What devices does Arcserve Backup support?

Solution:

Refer to the Arcserve web site for a certified device list to confirm the firmware and model of the supported device. To access this information, open the Arcserve Backup Home Page and click the Accessing Technical Support link under Technical Support, as shown in the following illustration:

More information:

Arcserve Backup Home Page (see page 195)

Cluster HA Resources Not Created

Valid on Windows platforms running Microsoft Cluster Server (MSCS).

Symptom

Arcserve Backup cannot create cluster HA resources.

Solution

This problem presents itself after you install Arcserve Backup, and then attempt to create the cluster HA resources using the babha -postsetup command. When you execute this command, a message box appears indicating that the cluster resource could not be created. In addition, the following message appears in the Cluster.log file:

open or create fileshare , return error: [87]

To remedy this problem, do the following:

1. Under the Arcserve Backup cluster group, create an object named "Arcserve Share" with a resource type of file share.
2. Add the resource's dependence with shared disk and the Arcserve Backup virtual name.
3. Specify the following:
   - **Share name:** ARCSERVE$
   - **Path:** The Arcserve Backup home directory.
4. Execute the babha –postsetup command.

Appendix B: Using Best Practices to Install and Upgrade Arcserve Backup

This section contains the following topics:

Best Practices for Installing Arcserve Backup (see page 269)
Best Practices for Upgrading Arcserve Backup from a Previous Release (see page 299)
General Best Practices (see page 343)

Best Practices for Installing Arcserve Backup

Consider the following best practices when you are installing Arcserve Backup.

This section contains the following topics:

How to Complete Prerequisite Tasks for Installing Arcserve Backup (see page 270)
Installing Arcserve Backup into a Single-server Environment (see page 271)
Installing a Primary Server with Member Servers (see page 274)
Installing a Primary Server with Member Servers and Devices (see page 278)
Installing a Primary Server with Member Servers and Shared Devices in a SAN (see page 284)
Installing Multiple Primary Servers with Member Servers in a SAN (see page 289)
Installing Arcserve Backup into a Cluster-aware Environment (see page 295)

How to Complete Prerequisite Tasks for Installing Arcserve Backup

Before you install Arcserve Backup, complete the following prerequisite tasks:

Licensing

Ensure that you have the licenses that you require to install Arcserve Backup.

System requirements

Review the readme file for a description of the system requirements for the computers where you will install Arcserve Backup.

Arcserve Backup database

Determine the application that you will use for the Arcserve Backup database. Consider the following architectural criteria:

- The recommended database application is Microsoft SQL Server 2008 Express Edition.
- Microsoft SQL Server 2008 Express Edition does not support remote communication. If your current topology consists of a remote database configuration, or you plan to access a database application that is installed on a different system (remote system), you must specify Microsoft SQL Server as the Arcserve Backup database.

Note: For more information, see Database Requirements (see page 46).

Arcserve Backup server type

Determine the type of Arcserve Backup server that you require. The installation wizard detects and analyzes your current configuration. The installation wizard then determines the type of Arcserve Backup server that you should install and the agents and options that you need to install. If your topology consists of a single Arcserve server, you should install a stand-alone server.

If you plan to add Arcserve Backup servers to your environment in the future, you can specify either of the following Arcserve server installations:

- **Stand-alone server--**With a stand-alone server installation, you must deploy independent stand-alone servers in the future.
- **Primary server--**With a primary server installation you can centrally manage multiple Arcserve Backup servers.

  To enable central management capabilities, you must specify the Arcserve Primary Server option and install the Central Management Option.

Note: For more information about the different types of Arcserve server installations, see Types of Arcserve Backup Server Installations.

Attached devices

Ensure that all devices, such as libraries, are attached to the Arcserve servers before you start the installation process. After the installation is complete, the first time the Tape Engine starts, Arcserve Backup automatically detects and configures attached devices; manual configuration is not required.

Installing Arcserve Backup into a Single-server Environment

The following sections describe best practices that you can use to install Arcserve Backup into a single-server environment.

This section contains the following topics:

Recommended Configuration - Stand-alone Server (see page 271)
Components You Must Install (see page 272)
How to Install a Stand-alone Server or Primary Server (see page 272)
How to Verify a Stand-alone Server Installation (see page 272)

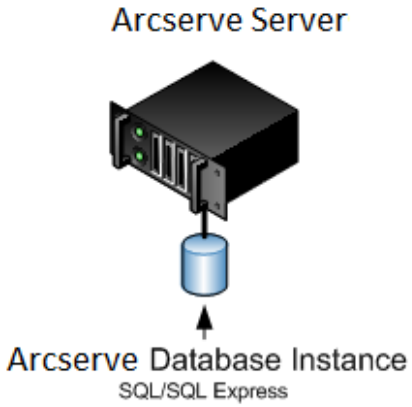
Recommended Configuration - Stand-alone Server

When you require a single backup server to protect your environment, the best practice is to install Arcserve Backup using the Stand-alone Server installation.

With a Stand-alone Server installation, you can run, manage, and monitor jobs running locally to and from the backup server.

If you determine at some point that you require additional backup servers to protect your environment, you can install the Primary Server option and then add member servers to your Arcserve Backup domain. You must install the Central Management Option when you install the Primary Server option.

The following diagram illustrates the architecture of a Arcserve Backup Stand-alone Server or a Arcserve Backup Primary Server.



Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Stand-alone Server

Lets you install Arcserve Backup on a stand-alone backup server.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

How to Install a Stand-alone Server or Primary Server

Complete the following tasks to install Arcserve Backup into a single-server environment:

1. Install the Arcserve Backup Stand-alone Server installation option on the target system.
2. Verify the installation.

How to Verify a Stand-alone Server Installation

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

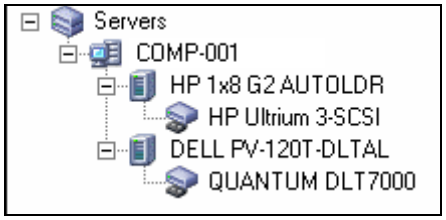
1. Open the Arcserve Backup Manager Console.
2. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

3. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the server.

   The following diagram illustrates the Device Manager window with a stand-alone server with attached libraries. The libraries are not shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   Note: For information about configuring devices, see the *Administration Guide*.

4. (Optional) Using Device Configuration, perform required configurations. For example, configure a file system device.

5. Submit a simple backup job.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contained warning messages, error messages, or both, double-click the message view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple restore job.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contained warning messages, error messages, or both, double-click the message view a description of the problem and the steps that you can take to correct the problem.

   After you correct the problem, resubmit the job.

7. Open the Job Status Manager.

   Ensure the Job Queue tab and Activity Log display information about the jobs.

Installing a Primary Server with Member Servers

The following sections describe best practices that you can use to install Arcserve Backup with a primary server and one or more member servers.

This section contains the following topics:

Recommended Configuration (see page 274)
Components You Must Install (see page 275)
How to Install a Primary Server with Member Servers (see page 276)
How to Verify a Primary Server with Member Servers Installation (see page 276)

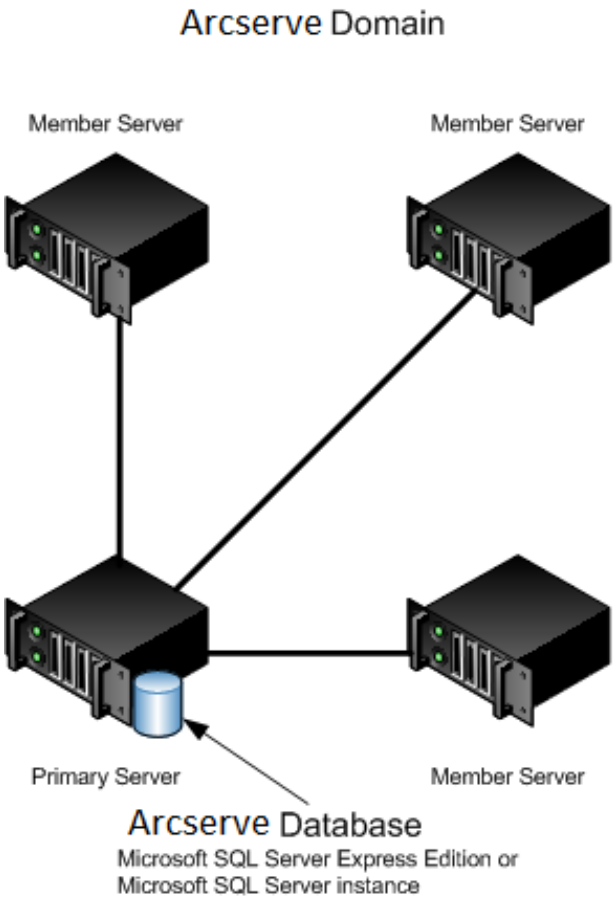
Recommended Configuration

When you require multiple backup servers that reside in the same domain to protect your environment, the best practice is to install Arcserve Backup using the Primary Server and Member Server installation options. With this configuration, you can create a centralized management environment.

A primary server controls itself and one or more member servers. A primary server lets you manage and monitor backup, restore, and other jobs that run on primary and member servers. Using primary and member servers, you can have a single point of management for multiple Arcserve Backup servers in your environment. You can then use the Manager Console to manage the primary server.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the topology of a centralized management environment. The environment consists of a primary server and one or more member servers. The Arcserve Backup database is hosted by Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.



Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Member Server

Lets servers in a Arcserve Backup domain receive instructions about jobs and devices from a primary server.

How to Install a Primary Server with Member Servers

Complete the following tasks to install a primary server with member servers:

1. Install the Arcserve Backup Primary Server on the system that will function as the Primary server.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

2. Install the Arcserve Backup Member Server on all servers that will function as members of the new Arcserve Backup domain.
3. Verify the installation.

How to Verify a Primary Server with Member Servers Installation

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.
2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.

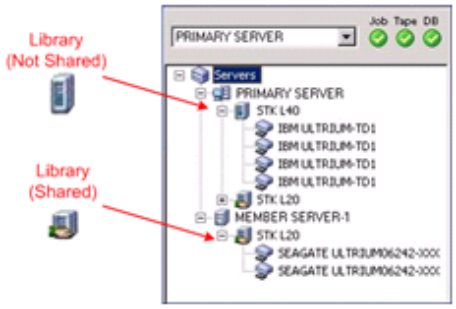
3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. (Optional) Open the Device Manager and configure a file system device.

6. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

9. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Installing a Primary Server with Member Servers and Devices

The following sections describe best practices that you can use to install Arcserve Backup with a primary server, one or more member servers, and devices that are attached to the primary server, member servers, or both.

This section contains the following topics:

Recommended Configuration (see page 279)
Components You Must Install (see page 280)
How to Install a Primary Server with Member Servers and Devices (see page 281)
How to Verify a Primary Server with Member Servers and Devices Installation (see page 282)

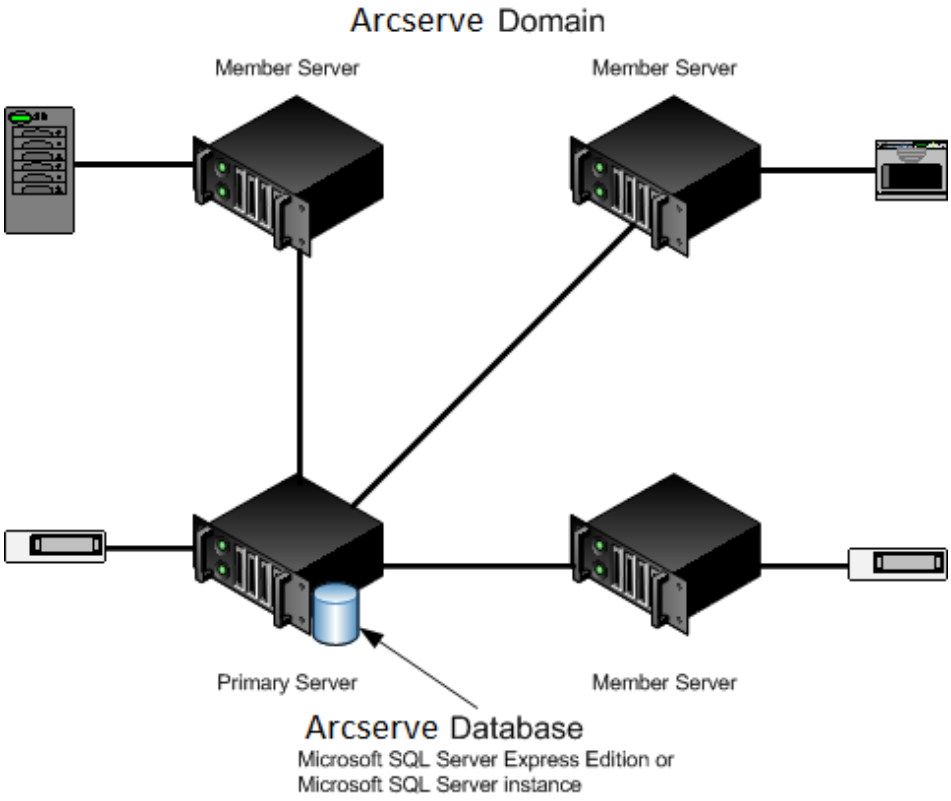
Recommended Configuration

When you require multiple backup servers that reside in the same domain and devices, such as libraries, to protect your environment, the best practice is to install Arcserve Backup using the Primary Server and Member Server installation options. With this configuration, you can create a centralized management environment.

A primary server controls itself and one or more member servers. A primary server lets you manage and monitor backup, restore, and other jobs that run on primary and member servers. Using primary and member servers, you can have a single point of management for multiple Arcserve Backup servers in your domain. You can then use the Manager Console to manage the primary server.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management environment with attached devices. The environment consists of a primary server and one or more member servers. The Arcserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.



Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Tape Library Option

Lets you perform backup, restore, and media management tasks using multiple-libraries and tape RAID libraries.

Arcserve Backup Member Server

Lets servers in a Arcserve Backup domain receive instructions about jobs and devices from a primary server.

How to Install a Primary Server with Member Servers and Devices

Complete the following tasks to install a primary server with member servers and devices:

1. Install the Arcserve Backup Primary Server on the system that will function as the Primary server.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

2. Install the options that you require to support the devices connected to the primary server. For example, the Tape Library Option or the NDMP NAS Option.
3. Install the Arcserve Backup Member Server on all servers that will function as members of the new Arcserve Backup domain.
4. Install the options that you require to support the devices connected to the member servers. For example, the Tape Library Option or the NDMP NAS Option.
5. Verify the installation.

How to Verify a Primary Server with Member Servers and Devices Installation

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

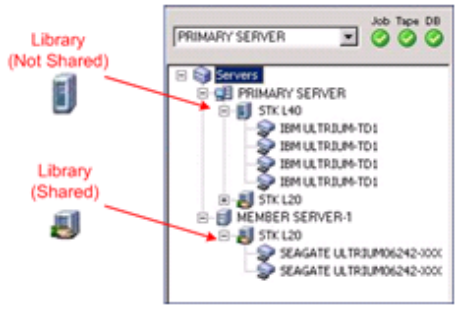
1. Open the Arcserve Backup Manager Console on the primary server.
2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.
3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.
4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Installing a Primary Server with Member Servers and Shared Devices in a SAN

The following sections describe best practices that you can use to install Arcserve Backup with a primary server, one or more member servers, and devices that are shared in your storage area network (SAN).

This section contains the following topics:

Recommended Configuration (see page 284)
Components You Must Install (see page 285)
How to Install a Primary Server with Member Servers and Shared Devices in a SAN (see page 287)
How to Verify a Primary Server with Member Servers and Shared Devices in a SAN Installation (see page 287)

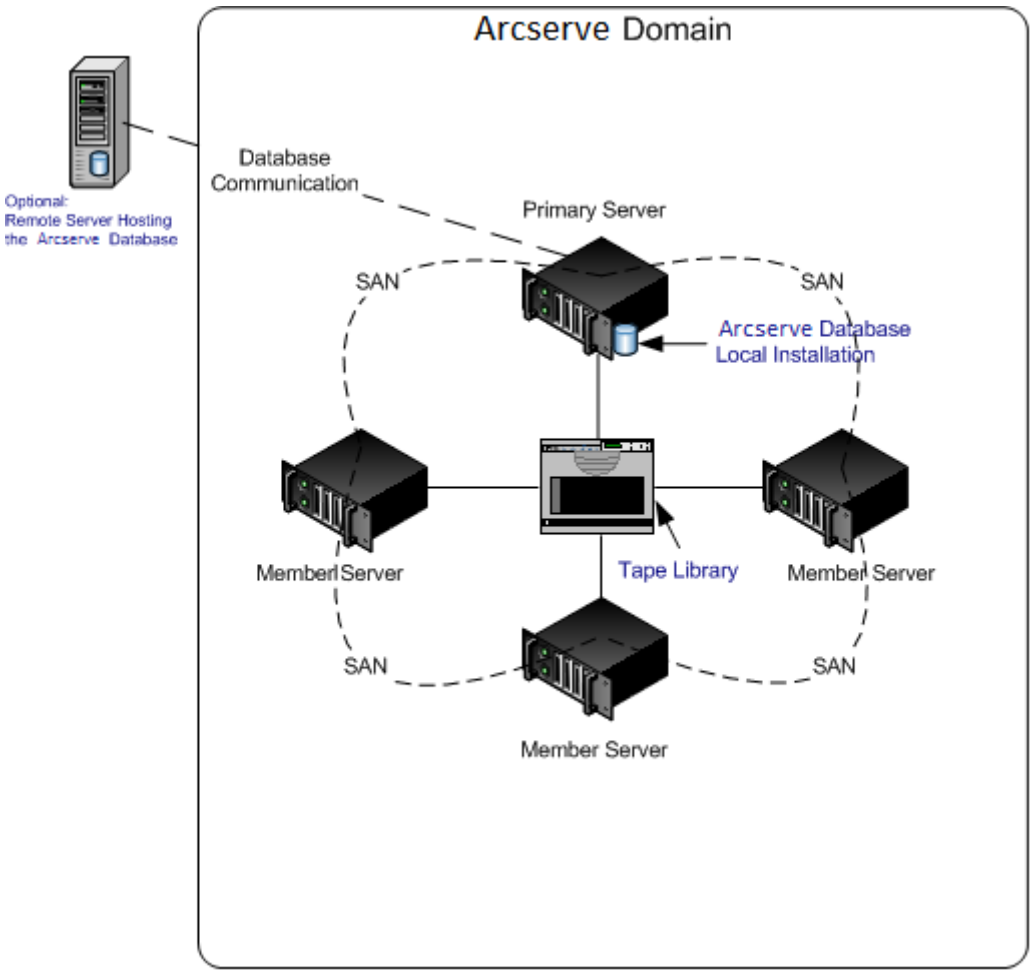
Recommended Configuration

When you require multiple backup servers that reside in the same domain and devices, such as libraries, that are shared in your SAN to protect your environment, the best practice is to install Arcserve Backup using the Primary Server and Member Server installation options. With this configuration, you can create a centralized management environment.

A primary server controls itself and one or more member servers. A primary server lets you manage and monitor backup, restore, and other jobs that run on primary and member servers. Using primary and member servers, you can have a single point of management for multiple Arcserve Backup servers in your domain. You can then use the Manager Console to manage the primary server.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management environment in a storage area network with shared devices. The environment consists of a primary server and one or more member servers. The Arcserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.



Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Tape Library Option

Lets you perform backup, restore, and media management tasks using multiple-libraries and tape RAID libraries.

Arcserve Backup Storage Area Network (SAN) Option

Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the Arcserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

Arcserve Backup Member Server

Lets servers in a Arcserve Backup domain receive instructions about jobs and devices from a primary server.

Note: To deploy this configuration, you must issue one Storage Area Network (SAN) Option and one Tape Library Option license for each server in your SAN.

How to Install a Primary Server with Member Servers and Shared Devices in a SAN

Complete the following tasks to install a primary server with member servers and shared devices in a SAN:

1. Install the Arcserve Backup Primary Server on the system that will function as the Primary server.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

2. Install the Tape Library Option and the Storage Area Network (SAN) Option on the primary server.

   Note: Ensure that you issue one Storage Area Network (SAN) Option license and one Tape Library Option license for each server in your SAN.

3. Install the options that you require to support the devices connected to the primary server. For example, the NDMP NAS Option.

4. Install the Arcserve Backup Member Server on all servers that will function as members of the new Arcserve Backup domain.

5. Install the options that you require to support the devices connected to the member servers. For example, the NDMP NAS Option.

6. Verify the installation.

How to Verify a Primary Server with Member Servers and Shared Devices in a SAN Installation

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.

2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.

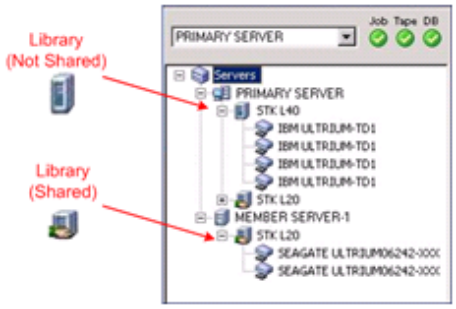
3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Installing Multiple Primary Servers with Member Servers in a SAN

The following sections describe best practices that you can use to install Arcserve Backup with a multiple primary servers, each primary server manages one or more member servers, and devices are shared in your storage area network (SAN).

This section contains the following topics:

Recommended Configuration (see page 290)
Components You Must Install (see page 291)
How to Install Multiple Primary Servers with Member Servers in a SAN (see page 293)
How to Verify a Multiple Primary Servers with Member Servers in a SAN Installation (see page 293)

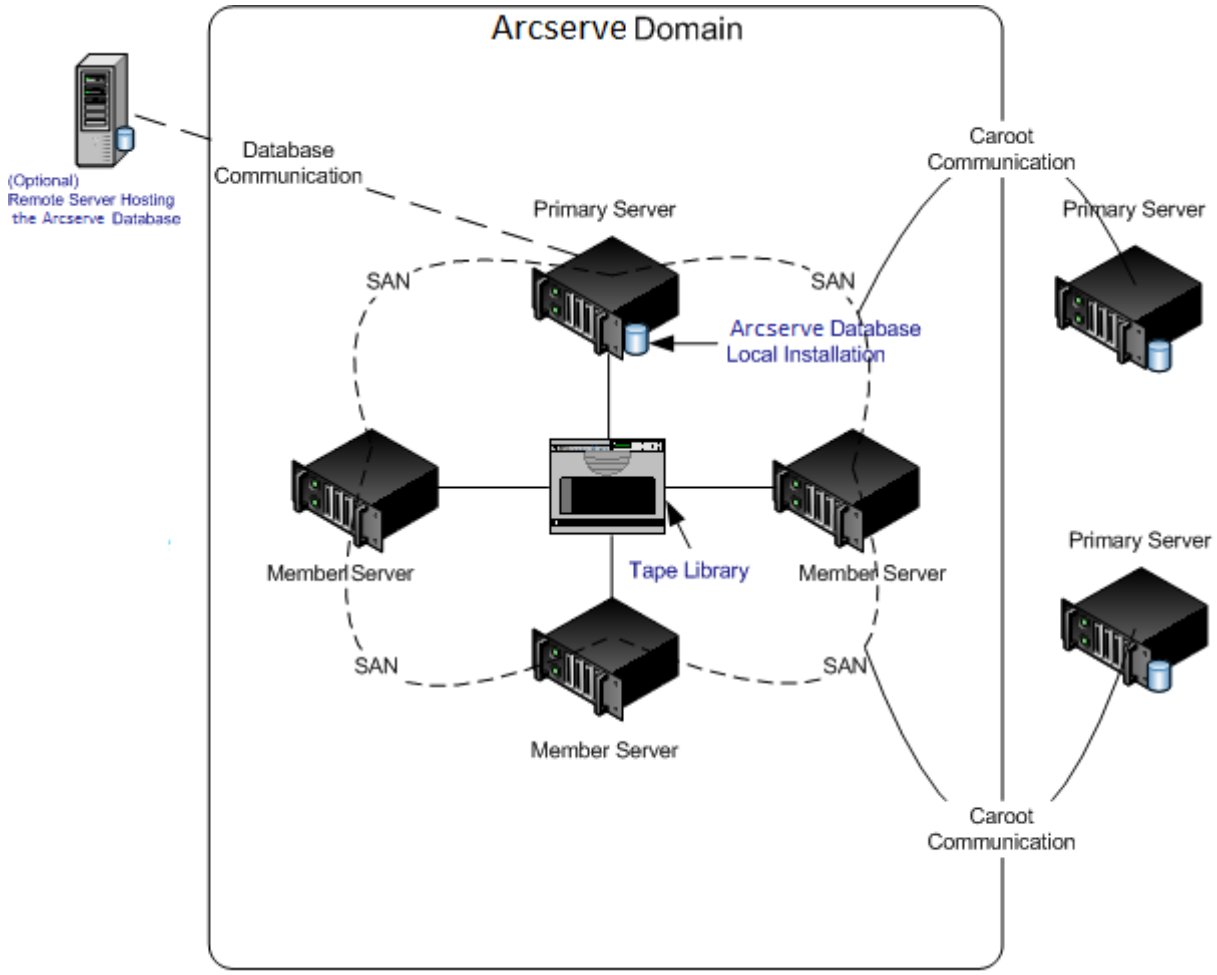
Recommended Configuration

When you require multiple backup servers that reside in the same domain and devices, such as libraries, that are shared in your SAN to protect your environment, the best practice is to install Arcserve Backup using the Primary Server and Member Server installation options. With this configuration, you can create a centralized management environment.

A primary server controls itself and one or more member servers. A primary server lets you manage and monitor backup, restore, and other jobs that run on primary and member servers. Using primary and member servers, you can have a single point of management for multiple servers in your Arcserve Backup domain. You can then use the Manager Console to manage the primary server.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management environment in a storage area network with shared devices. The environment consists of a primary server and one or more member servers. The Arcserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.



Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Tape Library Option

Lets you perform backup, restore, and media management tasks using multiple-libraries and tape RAID libraries.

Arcserve Backup Storage Area Network (SAN) Option

Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the Arcserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

Arcserve Backup Member Server

Lets servers in a Arcserve Backup domain receive instructions about jobs and devices from a primary server.

Note: To deploy this configuration, you must issue one Storage Area Network (SAN) Option and one Tape Library Option license for each server in your SAN.

How to Install Multiple Primary Servers with Member Servers in a SAN

Complete the following tasks to install multiple primary servers with member servers in a SAN:

1. Install the Arcserve Backup Primary Server on the system that will function as the Primary server.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

2. Install the Tape Library Option and the Storage Area Network (SAN) Option on the primary server.

   Note: Ensure that you issue one Storage Area Network (SAN) Option license and one Tape Library Option license for each server in your SAN.

3. Install the options that you require to support the devices connected to the primary server. For example, the Tape Library Option or the NDMP NAS Option.

4. Install the Arcserve Backup Member Server on all servers that will function as members of the new Arcserve domain.

5. Install the Arcserve Backup Primary Servers that will reside outside the SAN.

   Note: You must assign a domain name to primary servers that reside outside the SAN that is different from the domain name that is assigned to the primary server that resides inside the SAN.

6. Install the options that you require to support the devices connected to the member servers. For example, the NDMP NAS Option.

7. Verify the installation.

How to Verify a Multiple Primary Servers with Member Servers in a SAN Installation

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.

2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.

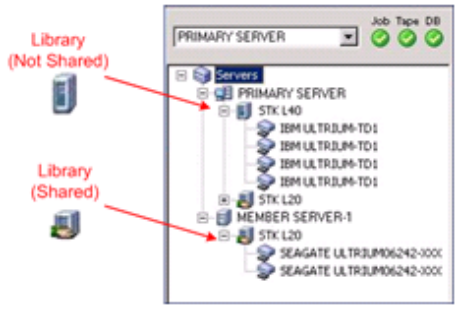
3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Installing Arcserve Backup into a Cluster-aware Environment

The following sections describe best practices that you can use to install Arcserve Backup into a cluster-aware environment.

This section contains the following topics:

Recommended Configuration (see page 296)
Components You Must Install (see page 297)
How to Install Arcserve Backup into a Cluster-aware Environment (see page 297)
How to Verify a Cluster-aware Installation (see page 298)

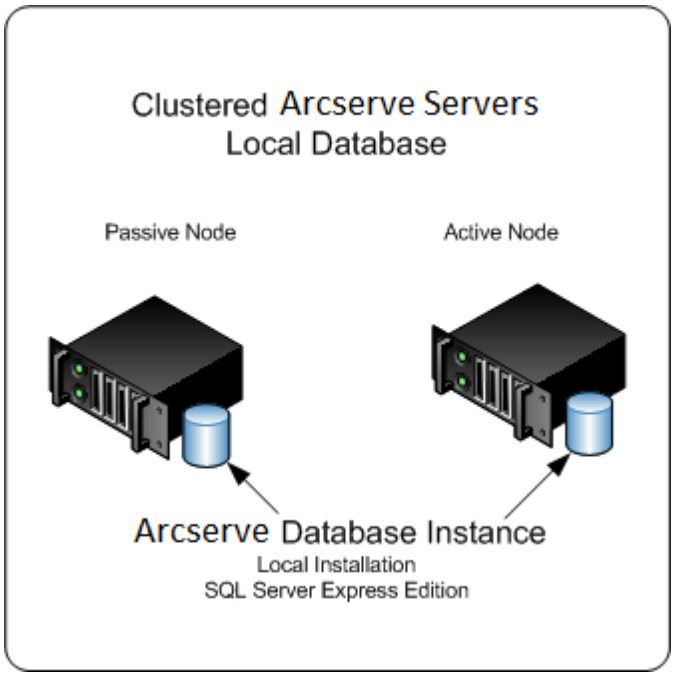
Recommended Configuration

When you require multiple backup servers that reside in the same domain to protect your environment, and the high-availability of a cluster-aware environment, the best practice is to install Arcserve Backup using the Primary Server and Member Server installation options into your cluster aware environment. This architecture lets you centrally manage your Arcserve Backup environment and maintain the high availability capabilities of a cluster-aware environment.

A primary server controls itself and one or more member servers. A primary server lets you manage and monitor backup, restore, and other jobs that run on primary and member servers. Using primary and member servers, you can have a single point of management for multiple servers in your Arcserve Backup domain. You can then use the Manager Console to manage the primary server.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management, cluster-aware environment. The environment consists of a primary server and one or more member servers. The Arcserve database is hosted by Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.



Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Member Server

Lets servers in a Arcserve Backup domain receive instructions about jobs and devices from a primary server.

How to Install Arcserve Backup into a Cluster-aware Environment

You can install Arcserve Backup to a cluster environment with job failover capability on the following cluster platforms:

- Microsoft Cluster Server (MSCS) in x86/AMD64 Windows Server
- NEC CLUSTERPRO/ExpressCluster X 2.1 for Windows
- NEC CLUSTERPRO/ExpressCluster X 3.0 for Windows
- NEC CLUSTERPRO/ExpressCluster X 3.1 for Windows

To install Arcserve Backup into a cluster aware environment

1. Refer to one of the following sections for information about how to install Arcserve Backup into a cluster-aware environment:
   - For MSCS, see Deploy Arcserve Backup Server on MSCS (see page 130).
   - For NEC CLUSTERPRO, see Deploy Arcserve Backup Server on NEC Cluster (see page 150).
2. Verify the installation.

How to Verify a Cluster-aware Installation

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.

   Ensure that you can view database information and Activity Log data in the Job Status Manager.

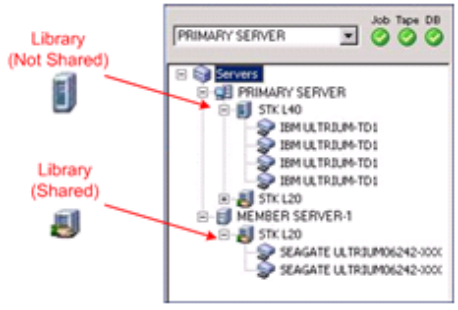
2. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

3. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



If the Device Manager does not detect all of your devices, complete the following tasks:

- Ensure that the device is properly attached to the server.
- Ensure that you have proper device drivers installed.
- Configure the devices using Device Configuration.

If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

Note: For information about configuring devices, see the *Administration Guide*.

4. Move the Arcserve cluster group to a different node.

   Ensure that all Arcserve services started successfully.

   Note: The Manager Console may stop responding intermittently while the cluster group is moving to a different node.

5. (Optional) Perform required configurations. For example, configure a file system device.

6. Submit a simple backup job.

   Ensure that the backup job completes successfully.

7. Submit a simple restore job.

   Ensure that restore job completes successfully.

8. Open the Job Status Manager.

   Ensure that information about the jobs display on the Job Queue tab and in the Activity Log.

Best Practices for Upgrading Arcserve Backup from a Previous Release

Consider the following best practices when upgrading Arcserve Backup from a previous release.

This section contains the following topics:

How to Complete Prerequisite Tasks for Upgrading Arcserve Backup (see page 300)
Upgrading a Stand-alone Server or Primary Server (see page 301)
Upgrading Multiple Stand-alone Servers in a Domain (see page 306)
Upgrading Multiple Stand-alone Servers Sharing a Remote Database (see page 312)
Upgrading Servers in a SAN Using a Local or Remote Database (see page 318)
Upgrading Multiple Servers in a SAN and Non-SAN Environment to this Release (see page 324)
Upgrading Multiple Servers Using a Central Database (see page 330)
Upgrading Multiple Servers in a Cluster-aware Environment (see page 336)

How to Complete Prerequisite Tasks for Upgrading Arcserve Backup

Before you upgrade Arcserve Backup, complete the following prerequisite tasks:

Licensing

Ensure that you have the licenses that you require to upgrade Arcserve Backup.

System requirements

Review the readme file for a description of the system requirements for the computers where you will upgrade Arcserve Backup.

Upgrade requirements

Determine if you can upgrade your current installation to this release. If your current installation does not support an upgrade, you must uninstall Arcserve and then install this release. For more information, see Supported Upgrades (see page 55) and Backward Compatibility (see page 56).

Note: For a description of supported platforms for all Arcserve Backup agents, see the readme file.

Arcserve Backup database

Determine which application that you will to host the Arcserve Backup database. Consider the following architectural criteria:

- If you are currently using RAIMA (VLDB) to host the Arcserve database, you can upgrade to either Microsoft SQL Server 2008 Express Edition or Microsoft SQL Server. The recommended database application is Microsoft SQL Server 2008 Express Edition.
- If you are currently using Microsoft SQL Server to host the Arcserve database, you must continue using Microsoft SQL Server.

  Arcserve Backup cannot migrate data from a Microsoft SQL Server database to a Microsoft SQL Server 2008 Express database. Therefore, if you are currently running Microsoft SQL Server as the Arcserve database, you must specify Microsoft SQL Server as the Arcserve Backup database.
- Microsoft SQL Server 2008 Express Edition does not support remote communication. If your current environment consists of a remote database configuration, or you plan to access a database application that is installed on a remote system, you must host the Arcserve database using Microsoft SQL Server.

Note: For more information about Arcserve database requirements, see Database Requirements (see page 46).

Arcserve Backup server type

Determine the type of Arcserve Backup server that you require. The installation wizard detects and analyzes your current configuration. Then, based on your current installation, the installation wizard then determines the type of Arcserve Backup server that you should upgrade to and the agents and options that you need to install.

If you plan to add Arcserve Backup servers to your environment in the future, consider the following server installation types:

- **Stand-alone server--**With a stand-alone server installation, you must install independent, stand-alone servers in the future.
- **Primary server--**With a primary server installation you can centrally manage multiple Arcserve Backup servers.

  To enable central management capabilities, you must install and license Arcserve Backup and the Central Management Option.

  Note: For more information about the different types of Arcserve server installations, see Types of Arcserve Backup Server Installations (see page 41).

Attached devices

Ensure that all devices, such as libraries, are attached to the Arcserve Backup servers before you start the upgrade process. The first time the Tape Engine starts after the upgrade is complete, Arcserve Backup automatically detects and configures the attached devices; manual configuration is not required.

In-progress jobs

Ensure that all jobs are stopped before you start the upgrade process. Arcserve Backup detects all jobs with a Ready Status and places them in a Hold status for you. If there are jobs in progress, Arcserve Backup displays a message and the upgrade process pauses until all jobs in progress are complete.

Upgrading a Stand-alone Server or Primary Server

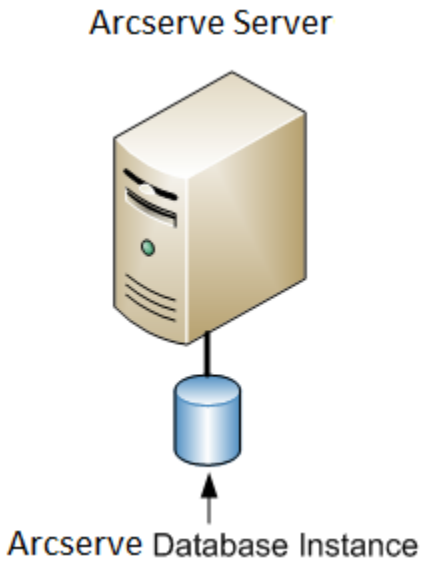
The following sections describe best practices that you can use to upgrade an Arcserve stand-alone server to this release.

This section contains the following topics:

Current Configuration - Arcserve Stand-alone Server-IMPW (see page 302)
Recommended Configuration - Arcserve Backup Stand-alone Server or Primary Server (see page 302)
New Components You Must Install (see page 303)
Components You Must Upgrade (see page 303)
How to Upgrade to an Arcserve Stand-alone Server-IMPW (see page 303)
How to Verify a Stand-alone Server or Primary Server Upgrade (see page 304)

Current Configuration - Arcserve Stand-alone Server-IMPW

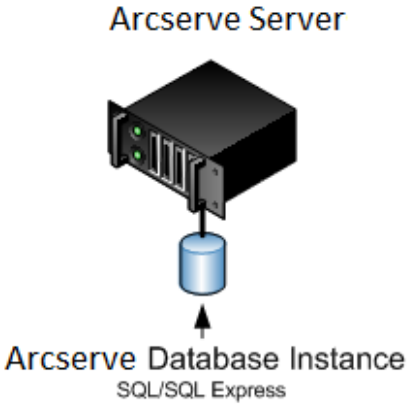
The following diagram illustrates the architecture of a Arcserve Backup stand-alone server configuration in previous releases:



Recommended Configuration - Arcserve Backup Stand-alone Server or Primary Server

If your current Arcserve installation consists of a single, stand-alone server, the best practice is to upgrade to a Arcserve Backup Stand-alone Server or a Arcserve Backup Primary Server.

The following diagram illustrates the architecture of a Arcserve Backup Primary Server or a Arcserve Backup Stand-alone Server.



New Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Stand-alone Server

Lets you install Arcserve Backup on a stand-alone backup server.

(Optional) Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following Arcserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade to an Arcserve Stand-alone Server-IMPW

Complete the following tasks to upgrade an Arcserve stand-alone server environment to a Arcserve Backup Stand-alone or Primary Server environment.

1. Install the Arcserve Backup Primary Server or the Arcserve Backup Stand-alone Server on the target system.

2. When you are prompted, migrate the data from the previous release to the new database.

   After you upgrade Arcserve Backup, Setup launches a migration wizard that lets you migrate data from your previous installation to the new Arcserve Backup server. You can migrate data relating to jobs, logs, and user security.

   To migrate the data, follow the prompts on the subsequent dialogs and complete all required information.

3. Verify the installation.

4. (Optional) Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

Upgrade Considerations (see page 54)
Upgrade Arcserve Backup from a Previous Release (see page 94)

How to Verify a Stand-alone Server or Primary Server Upgrade

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console.

2. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

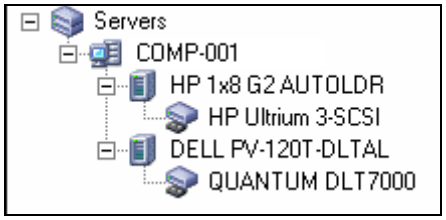
   Ensure that all previous backup data migrated successfully.

   Note: Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new installation.

3. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the server.

   The following diagram illustrates the Device Manager window with a stand-alone server with attached libraries. The libraries are not shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   Note: For information about configuring devices, see the *Administration Guide*.

4. (Optional) Using Device Configuration, perform required configurations. For example, configure a file system device.

5. Submit a simple backup job.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contained warning messages, error messages, or both, double-click the message view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple restore job.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contained warning messages, error messages, or both, double-click the message view a description of the problem and the steps that you can take to correct the problem.

   After you correct the problem, resubmit the job.

7. Open the Job Status Manager.

   Ensure the Job Queue tab and Activity Log display information about the jobs.

Upgrading Multiple Stand-alone Servers in a Domain

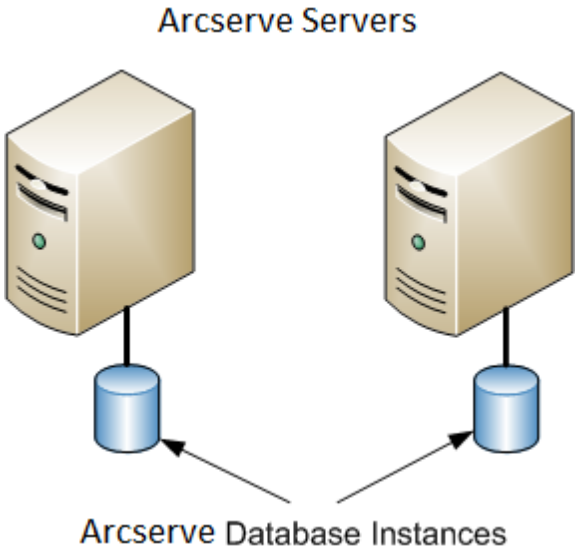
The following sections describe best practices that you can use to upgrade multiple Arcserve servers that do not share a database in a domain to a Arcserve Backup domain that consists of a primary server and multiple member servers.

This section contains the following topics:

Current Configuration - Multiple Arcserve Servers in a Domain-IMPW (see page 306)
Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers (see page 307)
New Components You Must Install (see page 308)
Components You Must Upgrade (see page 308)
How to Upgrade Multiple Arcserve Servers to a Centralized Management Environment-IMPW (see page 309)
How to Verify a Domain with a Primary Server and Member Servers Upgrade (see page 309)

Current Configuration - Multiple Arcserve Servers in a Domain-IMPW

The following diagram illustrates the architecture of multiple Arcserve Backup servers in a domain in previous releases:



Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers

If your current configuration consists of multiple Arcserve Backup servers in a domain, the best practice is to upgrade to a centralized management environment that consists of a primary server and one or more member servers.

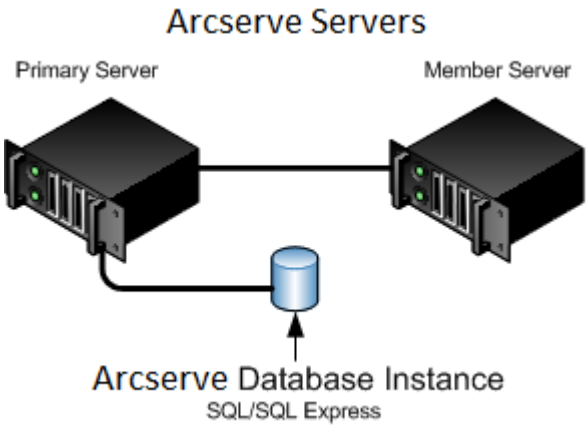
To upgrade to a centralized management environment, you must upgrade one of your existing Arcserve Backup servers to a Arcserve Backup Primary Server and then upgrade all other servers in the domain to Arcserve Backup Member Servers.

Note: The domain primary from your previous installation must assume the role of the Arcserve Backup Primary Server.

To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and primary server name in your network. You should therefore install Arcserve Backup on at least one primary server before you install member servers.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management environment:



Note: To enable Arcserve Backup to communicate with a remote database, you must use Microsoft SQL Server to host the Arcserve database.

New Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Member Server

Lets servers in an ARCserve domain receive instructions about jobs and devices from a primary server.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following Arcserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade Multiple Arcserve Servers to a Centralized Management Environment-IMPW

Complete the following tasks to upgrade multiple Arcserve servers to a centralized management environment that consist of a Arcserve Backup Primary Server and one or more Arcserve Backup Member Servers.

1. Install the Arcserve Backup Primary Server on the system that will function as the Primary server.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

   When you are prompted, migrate the data from the previous release to the new database.

2. Install the Arcserve Backup Member Server on all servers that will function as members of the new Arcserve domain.

   When you are prompted, migrate the data from the previous release to the new database.

3. Verify the installation.

4. (Optional) Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

Upgrade Considerations (see page 54)
Upgrade Arcserve Backup from a Previous Release (see page 94)

How to Verify a Domain with a Primary Server and Member Servers Upgrade

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.

2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.

3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

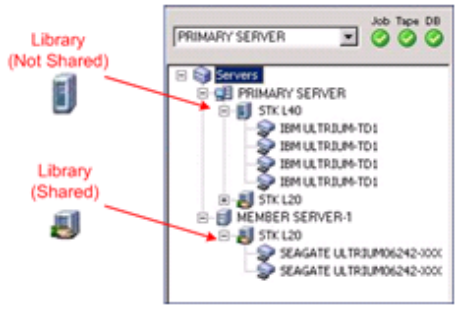
   Ensure that all previous backup data migrated successfully.

   Note: Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new primary server.

4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Upgrading Multiple Stand-alone Servers Sharing a Remote Database

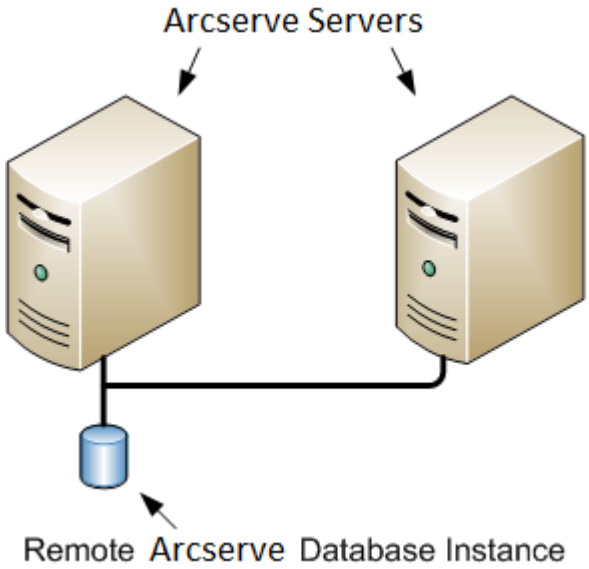
The following sections describe best practices that you can use to upgrade multiple Arcserve stand-alone servers, sharing a remote Arcserve database, to a Arcserve Backup Primary server and multiple Arcserve Backup Member servers.

This section contains the following topics:

Current Configuration - Multiple Arcserve Servers Sharing a Remote Database-IMPW (see page 312)
Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers (see page 313)
New Components You Must Install (see page 314)
Components You Must Upgrade (see page 314)
How to Upgrade Multiple Arcserve Servers Sharing a Database to a Centralized Management Environment-IMPW (see page 315)
How to Verify a Centralized Management Environment Upgrade (see page 315)

Current Configuration - Multiple Arcserve Servers Sharing a Remote Database-IMPW

The following diagram illustrates the architecture of multiple Arcserve Backup stand-alone servers in a domain, sharing a remote database, in previous releases:



Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers

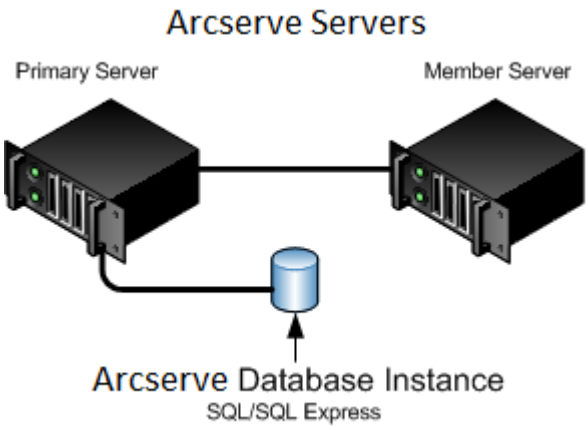
If your current configuration consists of multiple Arcserve Backup servers in a domain, the best practice is to upgrade to a centralized management environment that consists of a primary server and one or more member servers. A centralized management environment lets you share a local or remote database in a Arcserve Backup domain.

To upgrade to a centralized management environment, you must upgrade one of your existing Arcserve servers to a Arcserve Backup Primary Server and then upgrade all other servers in the domain to Arcserve Backup Member Servers.

Note: The system from your previous installation that is hosting the Arcserve database must assume the role of the Arcserve Backup Primary Server.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management environment:



Note: To enable Arcserve Backup to communicate with a remote database, you must use Microsoft SQL Server to host the Arcserve Backup database instance.

New Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Member Server

Lets servers in an ARCserve domain receive instructions about jobs and devices from a primary server.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following Arcserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade Multiple Arcserve Servers Sharing a Database to a Centralized Management Environment-IMPW

Complete the following tasks to upgrade multiple Arcserve servers sharing a database to a centrally managed Arcserve domain.

1. Install the Arcserve Backup Primary Server on the system that will function as the Primary server.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

   When you are prompted, migrate the data from the previous release to the new database.

2. Install the Arcserve Backup Member Server on all servers that will function as members of the new Arcserve domain.

   When you are prompted, migrate the data from the previous release to the new database.

3. Verify the installation.

4. (Optional) Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

Upgrade Considerations (see page 54)
Upgrade Arcserve Backup from a Previous Release (see page 94)

How to Verify a Centralized Management Environment Upgrade

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.

2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.

3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

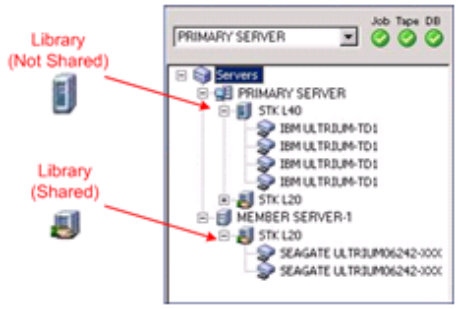
   Ensure that all previous backup data migrated successfully.

   Note: Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new primary server.

4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Upgrading Servers in a SAN Using a Local or Remote Database

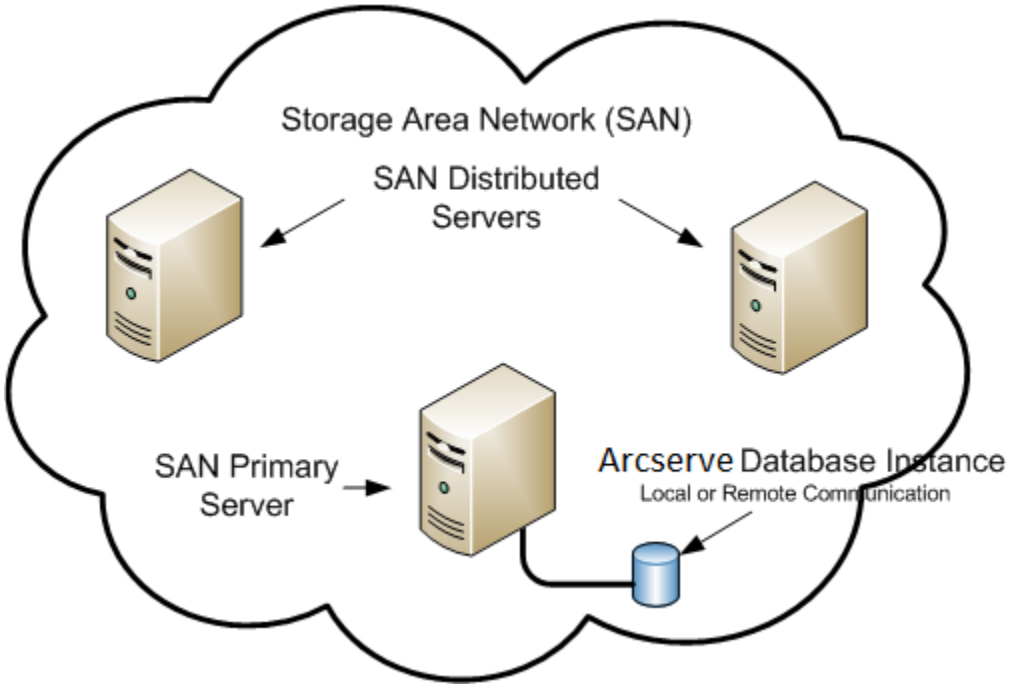
The following sections describe best practices that you can use to upgrade multiple Arcserve servers that reside on a SAN and share a local or remote Arcserve database.

This section contains the following topics:

Current Configuration - Multiple Arcserve Servers in a SAN Using a Local or Remote Database-IMPW (see page 318)
Recommended Configuration - Arcserve Backup Domain with a SAN Primary Server and SAN Distributed Servers (see page 319)
New Components You Must Install (see page 320)
Components You Must Upgrade (see page 321)
How to Upgrade Multiple Arcserve Servers in a SAN to This Release-IMPW (see page 321)
How to Verify a Centralized Management Environment Upgrade+ (see page 322)

Current Configuration - Multiple Arcserve Servers in a SAN Using a Local or Remote Database-IMPW

The following diagram illustrates the architecture of multiple Arcserve Backup servers in a SAN environment, using a local or remote database, in previous releases:



Recommended Configuration - Arcserve Backup Domain with a SAN Primary Server and SAN Distributed Servers

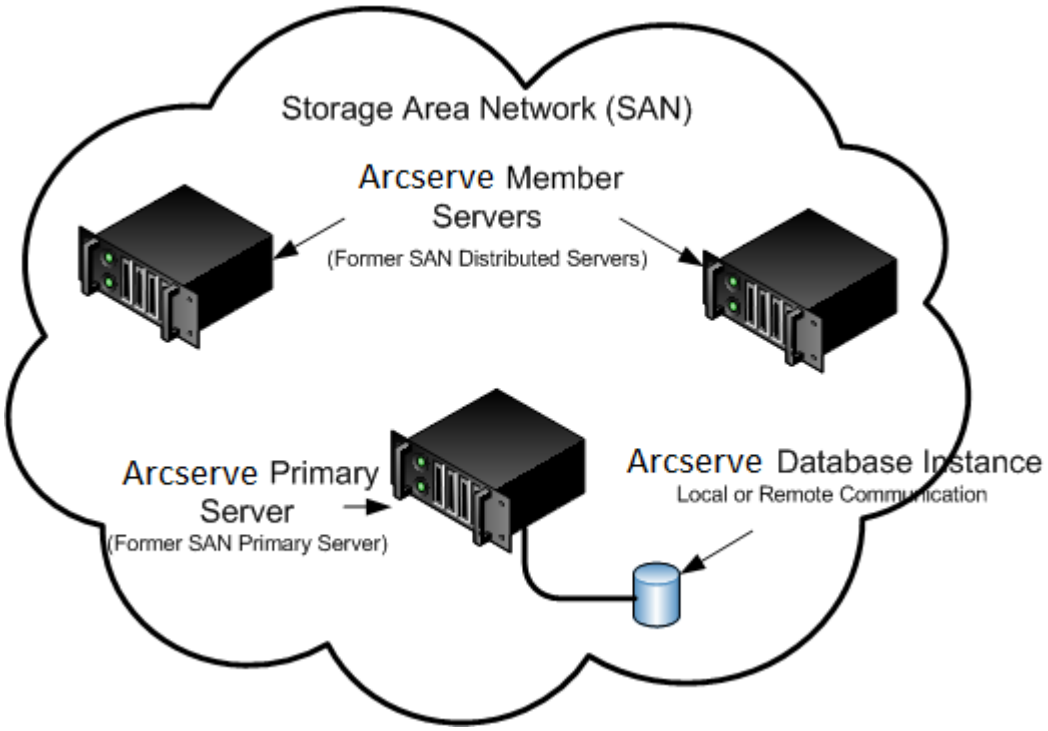
If your current configuration consists of multiple Arcserve Backup servers that reside on a SAN and share a local or remote Arcserve Backup database, the best practice is to upgrade to a centralized management environment. With a centralized management environment, you can share libraries and a local or remote database.

To upgrade your current SAN environment to a centralized management environment, you must upgrade your current SAN primary server to a Arcserve Backup Primary Server, and then upgrade your SAN distributed servers to Arcserve Backup Member Servers of that particular primary server.

To install member servers, the installation wizard must be able to detect the Arcserve Backup domain name and the primary server name in your environment. You should therefore install Arcserve Backup on at least one primary server before you install the member servers.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management environment integrated with a SAN and a local or remote Arcserve database.



New Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Tape Library Option

Lets you perform backup, restore, and media management tasks using multiple-libraries and tape RAID libraries.

Arcserve Backup Storage Area Network (SAN) Option

Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the Arcserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

Arcserve Backup Member Server

Lets servers in an ARCserve domain receive instructions about jobs and devices from a primary server.

Note: To deploy this configuration, you must issue one Storage Area Network (SAN) Option and one Tape Library Option license for each server in your SAN.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following Arcserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade Multiple Arcserve Servers in a SAN to This Release-IMPW

Complete the following tasks to upgrade a SAN environment to a SAN environment in this release.

1. Install the Arcserve Backup Primary Server on your current SAN primary system. This system will function as the primary server to the new Arcserve domain.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   Install the Storage Area Network (SAN) Option on your current SAN primary system

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

   When you are prompted, migrate the data from the previous release to the new database.

2. Install the Arcserve Backup Member Server on all of your current SAN distributed servers. These systems will function as member servers to the new Arcserve domain.

   When you are prompted, migrate the data from the previous release to the new database.

3. Verify the installation.

4. (Optional) Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

Upgrade Considerations (see page 54)
Upgrade Arcserve Backup from a Previous Release (see page 94)

How to Verify a Centralized Management Environment Upgrade+

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.
2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.
3. Open the Database Manager and the Job Status Manager.

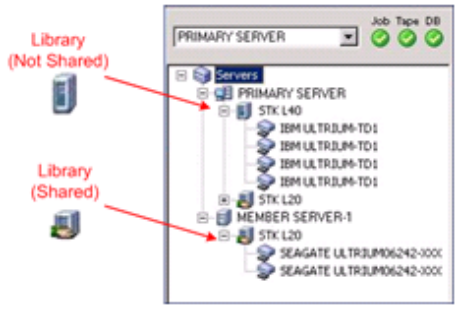
   Ensure that you can view database information and Activity Log data.

   Ensure that all previous backup data migrated successfully.

   Note: Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new primary server.
4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



If the Device Manager does not detect all of your devices, complete the following tasks:

- Ensure that the device is properly attached to the server.
- Ensure that you have proper device drivers installed.
- Configure the devices using Device Configuration.

If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Upgrading Multiple Servers in a SAN and Non-SAN Environment to this Release

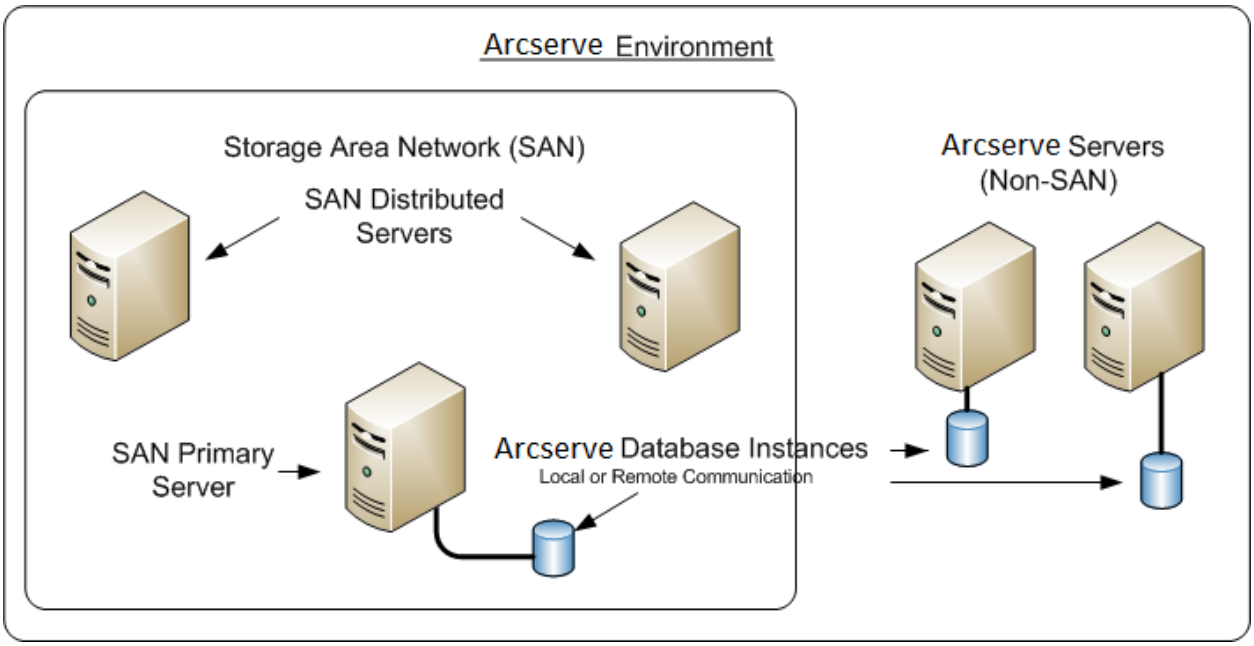
The following sections describe best practices that you can use to upgrade multiple Arcserve servers in a SAN and non-SAN environment to this release.

This section contains the following topics:

Current Configuration - Multiple Arcserve Servers in a SAN and Non-SAN Environment-IMPW (see page 325)
Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers (see page 325)
New Components You Must Install (see page 326)
Components You Must Upgrade (see page 327)
How to Upgrade Multiple Arcserve Servers in a SAN and a Non-SAN Environment to this Release-IMPW (see page 328)
How to Verify a Centralized Management Upgrade (see page 328)

Current Configuration - Multiple Arcserve Servers in a SAN and Non-SAN Environment-IMPW

The following diagram illustrates the architecture of multiple Arcserve Backup servers in a SAN environment and non-SAN environment, using a local or remote database, in previous releases:



Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers

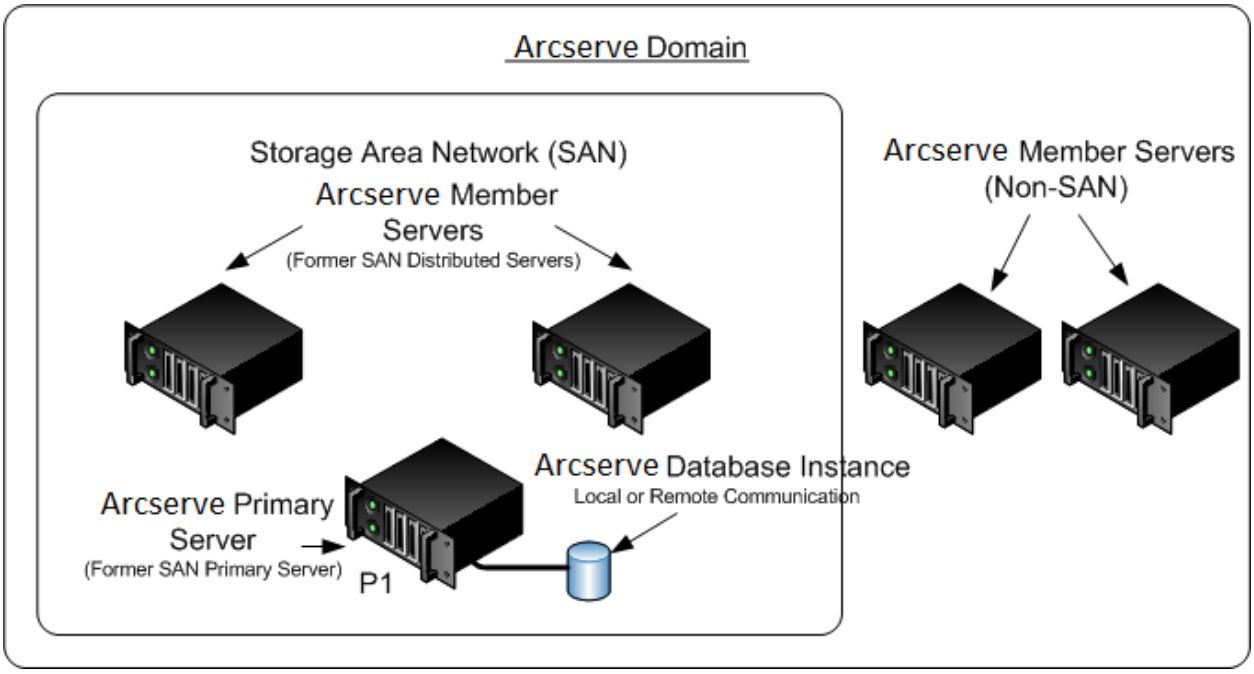
If your current configuration consists of a SAN environment where Arcserve Backup servers reside on the SAN and other Arcserve Backup servers do not reside on the SAN, the best practice is to install Arcserve Backup in a centrally managed environment.

To upgrade your current SAN environment to a centralized management environment, you must upgrade your current SAN primary server to a Arcserve Backup Primary Server, and then upgrade your SAN distributed servers to Arcserve Backup Member Servers.

To install member servers, the installation must be able to detect the Arcserve Backup domain name and the primary server name in your environment. You should therefore install Arcserve Backup on at least one primary server before you install the member servers.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of a centralized management environment consisting of a primary server and member servers that reside on a SAN, and member servers that do not reside on the SAN.



New Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Tape Library Option

Lets you perform backup, restore, and media management tasks using multiple-libraries and tape RAID libraries.

Arcserve Backup Storage Area Network (SAN) Option

Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the Arcserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

Arcserve Backup Member Server

Lets servers in an ARCserve domain receive instructions about jobs and devices from a primary server.

Note: To deploy this configuration, you must issue one Storage Area Network (SAN) Option and one Tape Library Option license for each server in your SAN.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following Arcserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade Multiple Arcserve Servers in a SAN and a Non-SAN Environment to this Release-IMPW

Complete the following tasks to upgrade Arcserve servers in a SAN and non-SAN environment to this release.

1. Install the Arcserve Backup Primary Server on your current SAN primary system. This system will function as the primary server to the new Arcserve domain.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   Install the Storage Area Network (SAN) Option on your current SAN primary system

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

   When you are promoted, migrate the data from the previous release to the new database.

2. Install the Arcserve Backup Member Server on all of your current SAN distributed servers and non-SAN servers. These systems will function as member servers to the new Arcserve domain.

   When you are prompted, migrate the data from the previous release to the new database.

3. Verify the installation.

4. (Optional) Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

Upgrade Considerations (see page 54)
Upgrade Arcserve Backup from a Previous Release (see page 94)

How to Verify a Centralized Management Upgrade

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.

2. Open the Server Admin.

   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.

3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

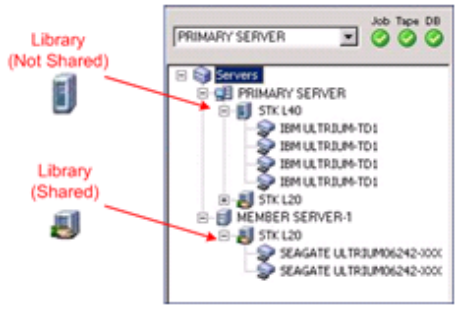
   Ensure that all previous backup data migrated successfully.

   Note: Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new primary server.

4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Upgrading Multiple Servers Using a Central Database

The following sections describe best practices that you can use to upgrade multiple Arcserve servers that share a centralized database to this release.

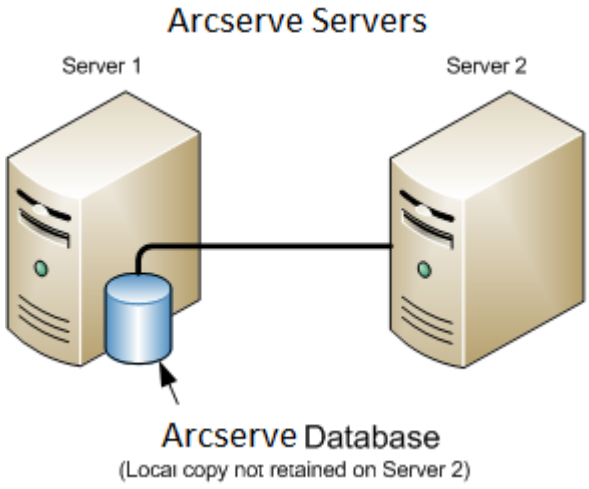
This section contains the following topics:

Current Configuration - Multiple Arcserve Servers Using a Central Database-IMPW (see page 330)
Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers (see page 331)
New Components You Must Install (see page 332)
Components You Must Upgrade (see page 333)
How to Upgrade Multiple Arcserve Servers Using a Remote Database to a Centralized Management Environment-IMPW (see page 333)
How to Verify a Centralized Management Upgrade (see page 334)

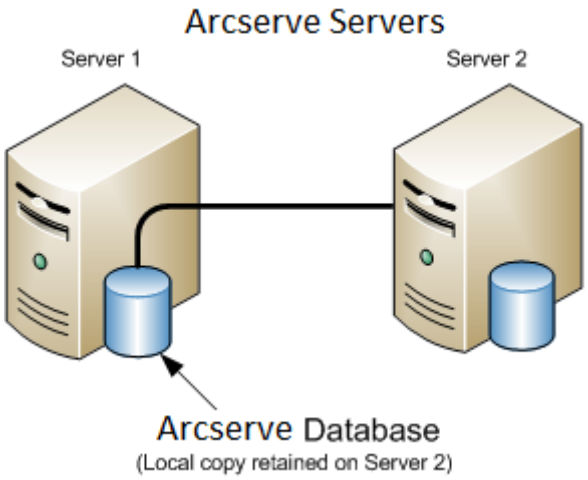
Current Configuration - Multiple Arcserve Servers Using a Central Database-IMPW

The following diagram illustrates the architecture of multiple Arcserve Backup servers using a centralized database in previous releases.

In the following diagram, multiple Arcserve Backup servers are sharing a centralized database. A copy of the Arcserve Backup database is not retained on one of the servers sharing the database.



In the following diagram, multiple Arcserve Backup servers are sharing a centralized database. A copy of the Arcserve Backup database is retained on one of the servers sharing the database.



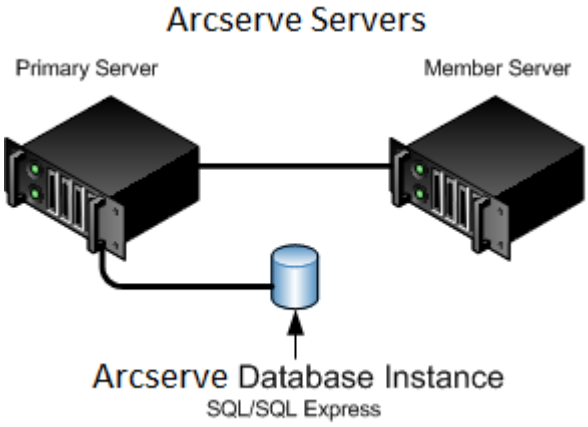
Recommended Configuration - Arcserve Backup Domain with a Primary Server and Member Servers

If your current configuration consists of multiple Arcserve Backup servers sharing a centralized database, the best practice is to upgrade to a centralized management environment containing a primary server and one or more member servers. A centralized management environment lets you host the Arcserve Backup database on the primary server or a remote system. You do not need to install Arcserve Backup on the system that hosts the Arcserve Backup database instance.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

To upgrade to a centralized management environment, you must upgrade one of your current systems to a Arcserve Backup Primary Server and then upgrade all other systems to Arcserve Backup Member Servers.

The following diagram illustrates the architecture of a centralized management environment with a remote system hosting the Arcserve Backup database.



New Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following Arcserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade Multiple Arcserve Servers Using a Remote Database to a Centralized Management Environment-IMPW

Complete the following tasks to upgrade multiple Arcserve servers using a centralized database to this release.

1. Install the Arcserve Backup Primary Server on the system that will function as the Primary server.

   Note: Setup installs the Central Management Option when you install the Arcserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the Arcserve Backup database.

   When you are promoted, migrate the data from the previous release to the new database.

2. Install the Arcserve Backup Member Server on all servers that will function as members of the new Arcserve domain.

   When you are prompted, migrate the data from the previous release to the new database.

3. Verify the installation.

4. (Optional) Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

More information:

Upgrade Considerations (see page 54)
Upgrade Arcserve Backup from a Previous Release (see page 94)

How to Verify a Centralized Management Upgrade

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on the primary server.
2. Open the Server Admin.

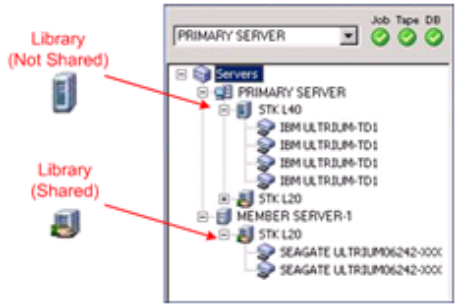
   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.
3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

   Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new primary server.
4. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

5. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

6. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

7. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple restore job on a member server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

Upgrading Multiple Servers in a Cluster-aware Environment

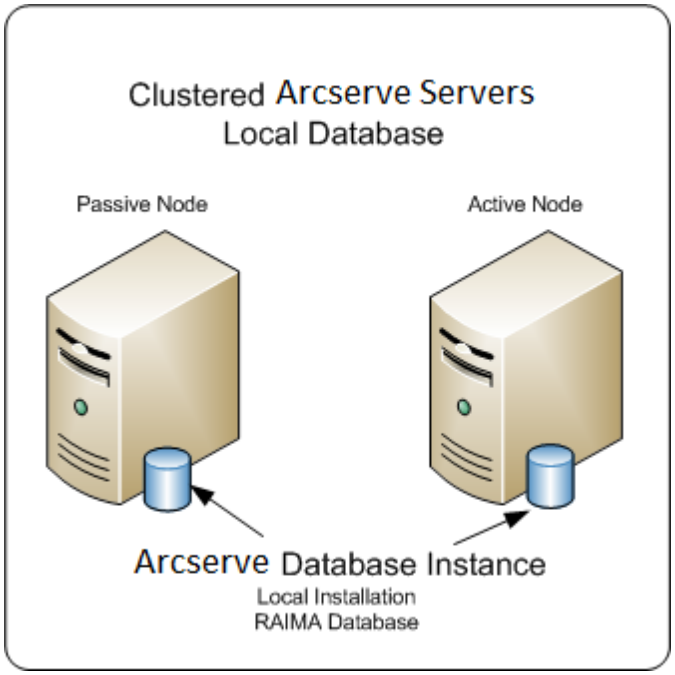
The following sections describe best practices that you can use to upgrade multiple Arcserve servers that reside in a Microsoft Cluster Server (MSCS), cluster-aware environment to this release.

This section contains the following topics:

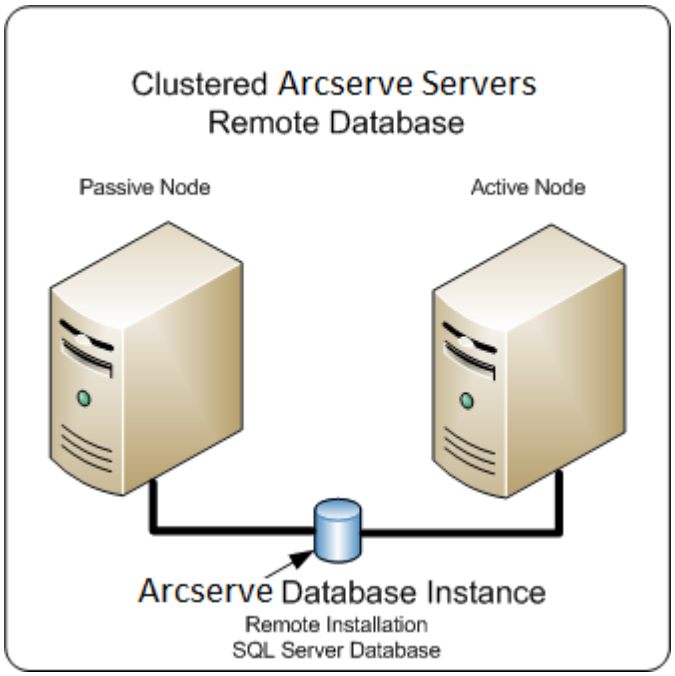
Current Configuration - Multiple Arcserve Servers in a Cluster-IMPW (see page 336)
Recommended Configuration - Arcserve Primary and Members Servers Installed in a Cluster-aware Environment (see page 337)
New Components You Must Install (see page 339)
Components You Must Upgrade (see page 340)
How to Upgrade an Arcserve Cluster-aware Environment to this Release-IMPW (see page 340)
How to Verify a Cluster-aware Upgrade (see page 341)

Current Configuration - Multiple Arcserve Servers in a Cluster-IMPW

The following diagram illustrates the architecture of multiple Arcserve Backup servers in a cluster-aware environment in previous releases. The Arcserve Backup database is hosted by a RAIMA database and the Arcserve Backup database instance resides on the Arcserve Backup server.



The following diagram illustrates the architecture of multiple Arcserve Backup servers in a cluster-aware environment in previous releases. The Arcserve Backup database is hosted by Microsoft SQL Server and the Arcserve Backup database instance resides on a remote system.



Recommended Configuration - Arcserve Primary and Members Servers Installed in a Cluster-aware Environment

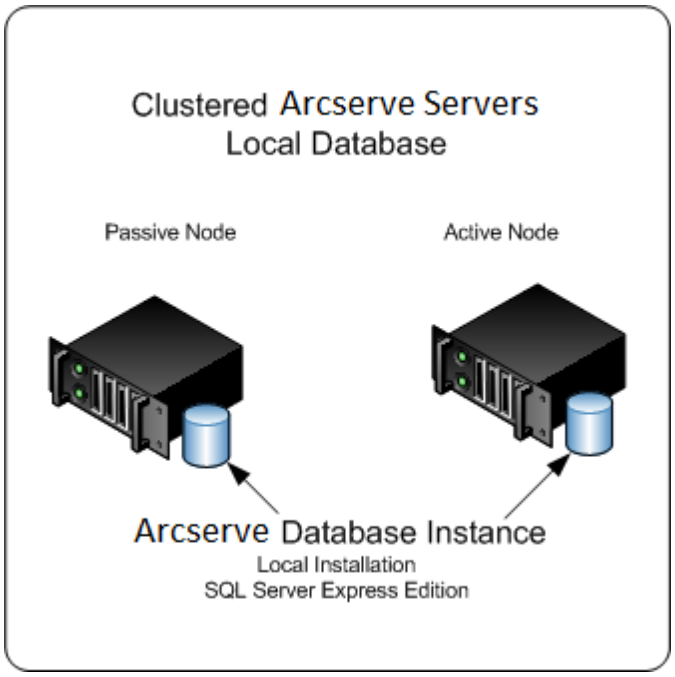
If your current configuration consists of multiple Arcserve Backup servers in a cluster-aware environment, the best practice is to upgrade to multiple Arcserve Backup Primary Servers or multiple Arcserve Backup Stand-alone Servers.

This architecture lets you centrally manage your Arcserve Backup environment and maintain the high availability capabilities of a cluster-aware environment.

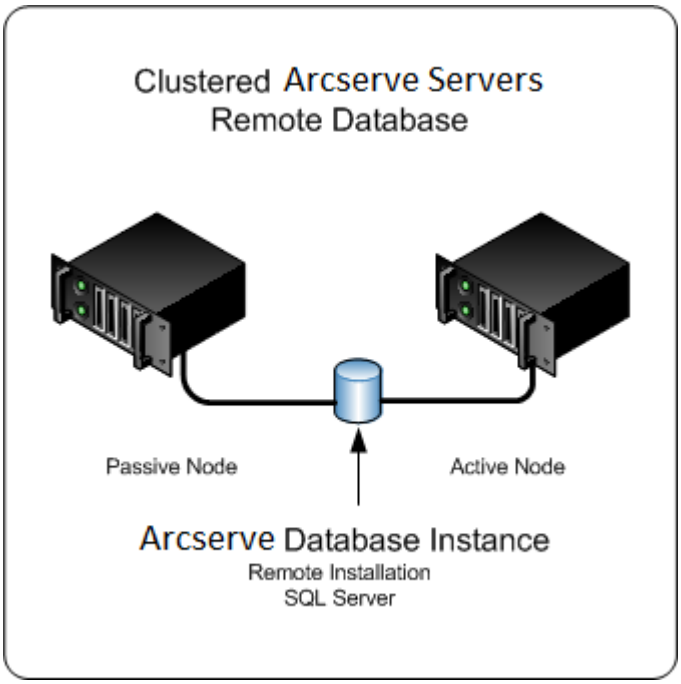
To deploy this configuration in your environment, you can use Microsoft SQL Server 2008 Express Edition or Microsoft SQL Server to host the Arcserve Backup database.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install Arcserve Backup using Microsoft SQL Server 2008 Express Edition, the installation wizard installs the database application and the Arcserve database instance on the primary server. To host the Arcserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of multiple Arcserve Backup servers in a cluster-aware environment in this release. The Arcserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the Arcserve Backup database instance resides on the Arcserve Backup server.



The following diagram illustrates the architecture of multiple Arcserve servers in a cluster-aware environment in this release. The Arcserve database is hosted by Microsoft SQL Server and the Arcserve database instance resides on a remote system.



New Components You Must Install

To deploy this configuration in your environment, you must install the following Arcserve Backup components:

Arcserve Backup Primary Server

Lets you install Arcserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.

Arcserve Backup Central Management Option

Lets you manage the primary server and all member servers in a Arcserve Backup domain from a central computer.

Note: The Arcserve Backup Primary Server is a prerequisite component.

Arcserve Backup Agent for Microsoft SQL Server

Lets you protect the Arcserve Backup database.

Note: A modified version of the agent called the Agent for ARCserve Database is installed with all ARCserve Primary Server and ARCserve Stand-alone Server installations.

Important! The uninstallation routine does not uninstall the Arcserve Backup database instance from your computer. If you find it necessary to reinstall Arcserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the Arcserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Arcserve Backup Client Agent for Windows

Lets you back up data locally to the Arcserve Backup server.

Arcserve Backup Member Server

Lets servers in an ARCserve domain receive instructions about jobs and devices from a primary server.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following Arcserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade an Arcserve Cluster-aware Environment to this Release-IMPW

You can upgrade Arcserve Backup to a cluster environment with job failover capability on the following cluster platforms:

- Microsoft Cluster Server (MSCS) in x86/AMD64 Windows Server
- NEC CLUSTERPRO/ExpressCluster X 2.1 for Windows
- NEC CLUSTERPRO/ExpressCluster X 3.0 for Windows
- NEC CLUSTERPRO/ExpressCluster X 3.1 for Windows

To upgrade an Arcserve cluster-aware environment to this release

1. Upgrade Arcserve Backup using one of the following procedures:
   - Upgrade Arcserve Backup from r12, r12.5, r15, r16 to r16.5 in an MSCS Cluster Environment. (see page 143)
   - Upgrade Arcserve Backup from r12, r12.5, r15, r16 to r16.5 in an NEC CLUSTERPRO Environment. (see page 167)
2. Verify the upgrade.
3. (Optional) Arcserve Backup does not support recovering the Arcserve Backup database when the last backup of the Arcserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the Arcserve Backup database as soon as possible after the upgrade is complete. For information about backing up the Arcserve Backup database, see the *Administration Guide*.

How to Verify a Cluster-aware Upgrade

To ensure that your Arcserve Backup installation functions properly, complete the following tasks:

1. Open the Arcserve Backup Manager Console on a stand-alone server.
2. Connect to the upgraded Arcserve Server using the virtual name.
3. If you can successfully connect to the upgraded server, move the Arcserve cluster group to a different node.

   Ensure that all Arcserve services started successfully.

   Note: The Manager Console may stop responding intermittently while the cluster group is moving to a different node.
4. Open the Server Admin.

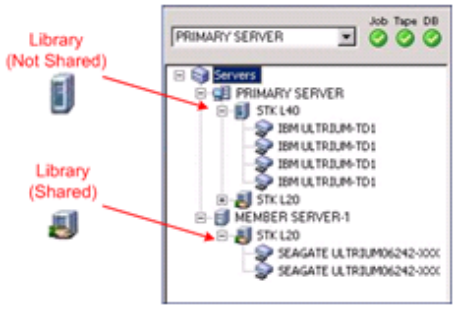
   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.
5. Open the Job Status Manager.

   Ensure that all data from the previous installation migrated to the new primary server. Arcserve Backup migrates information about jobs, logs, and user information from the previous servers to the new primary server.

6. Open the Device Manager.

   Ensure that the Device Manager detects all devices attached to the primary server and all member servers.

   The following diagram illustrates the Device Manager window with a primary server with attached devices and a member server and attached device. The primary server is attached to a library that is not shared, and the member server is attached to a library that is shared.



   If the Device Manager does not detect all of your devices, complete the following tasks:

   - Ensure that the device is properly attached to the server.
   - Ensure that you have proper device drivers installed.
   - Configure the devices using Device Configuration.

   If Arcserve Backup cannot detect the devices after you complete these tasks, contact Technical Support.

   Note: For information about configuring devices, see the *Administration Guide*.

7. Submit a simple backup job on a primary server.

   Ensure that the job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

8. Submit a simple backup job on a member server.

   Ensure that the backup job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

9. Submit a simple restore job on a primary server.

   Ensure that the restore job completes successfully.

   If the job fails, perform the following troubleshooting tasks:

   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit the job.

10. Submit a simple restore job on a member server.

    Ensure that the restore job completes successfully.

    If the job fails, perform the following troubleshooting tasks:

    - From the Job Status Manager, review the Activity Log details for the job.
    - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
    - After you correct the problem, resubmit the job.

General Best Practices

The following sections describe general best practices that can help you install and use Arcserve Backup.

This section contains the following topics:

Where to Install the Manager Console (see page 344)
How to Install and Manage Licenses (see page 344)
How to Install Arcserve Backup Server-Based Options (see page 348)

Where to Install the Manager Console

The Arcserve Backup Manager Console is a graphical user interface (GUI) that lets you log in to Arcserve Primary and Stand-alone servers from a remote system. With the Manager Console you can manage and monitor backup, restore, and other jobs that run from any Arcserve server. For example, a stand-alone server and a primary server and its member servers.

The Manager Console installation option lets you install the components that you need to manage you backup operations. You do not need to allocate storage space for backup data, logs, reports, and so on. This type of information is stored on primary and stand-alone servers.

You can install the Manager Console on any computer that is running an operating system that Arcserve Backup supports.

To determine best location where to install the Manager Console, consider the following general guidelines:

- The target system is a portable computer. For example, a notebook computer. You will use the portable computer to manage backup operations, but you will not store backup data on the portable computer.
- The target system resides in a remote location from your backup environment. Due to the bandwidth limitations manifested by your environment, it may not be practical to manage and back up data to the remote system.
- The target system does not meet the minimum system requirements to install the Arcserve Backup Server components. Refer to the readme file for a description of the minimum system requirements that your system needs to install the Arcserve Backup Server and Manager components.
- The target system is turned off periodically. Backup servers must be running at all times to achieve the highest level of data protection.

How to Install and Manage Licenses

The following sections describe how to install and manage Arcserve Backup licenses.

This section contains the following topics:

Manage Arcserve Backup Component Licenses (see page 345)
Release Licenses from Servers (see page 347)

Manage Arcserve Backup Component Licenses

The Arcserve Backup Server Admin lets you perform the following license management tasks:

- View the Arcserve Backup products installed on a primary server, stand-alone server, member servers, and agent servers in a Arcserve Backup domain.
- Identify the total number of licenses applied and the number of active licenses for each component in a Arcserve Backup domain.
- View the names of the servers using the component licenses in a Arcserve Backup domain.
- Release licenses from servers to make the licenses available to other servers in your domain.

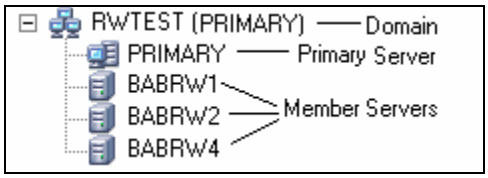
  Note: For information about releasing licenses from servers, see Release Licenses from Servers (see page 347).

To manage Arcserve Backup component licenses

1. From the Arcserve Backup Manager Console, open the Server Admin by clicking Server Admin in the Quick Start menu.

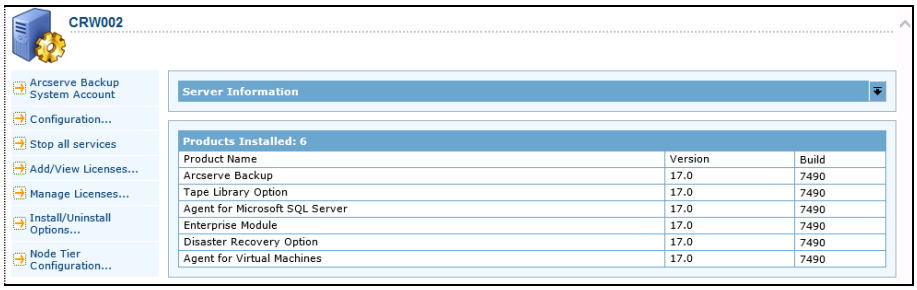
   The Server Admin opens.

   The Arcserve Backup primary server and its member servers display in a directory tree structure as illustrated by the following:



2. To view the Arcserve Backup products installed on a primary server and a member server, select the server in the directory tree.

   The components and licenses for the selected server display in the properties view, as illustrated by the following:



3. To view the component and licensing relationships in a Arcserve Backup domain, right-click the primary server and select Manage Licenses from the pop-up menu.

   The License Management dialog opens.

   The License Management dialog provides you with the following information:

   - **Version**--Specifies the release number of the license for the selected component.
   - **Active Licenses**--Specifies the number licenses that are currently active for the selected component. The total includes purchased licenses and trial licenses.
   - **Available Licenses**--Specifies the number of licenses available for use for the selected component. The total includes only purchased licenses.
   - **Total Licenses**--Specifies the total number of licenses purchased for the selected component.
   - **Licenses Needed**--Specifies the number of additional licenses that you need to use the selected component.

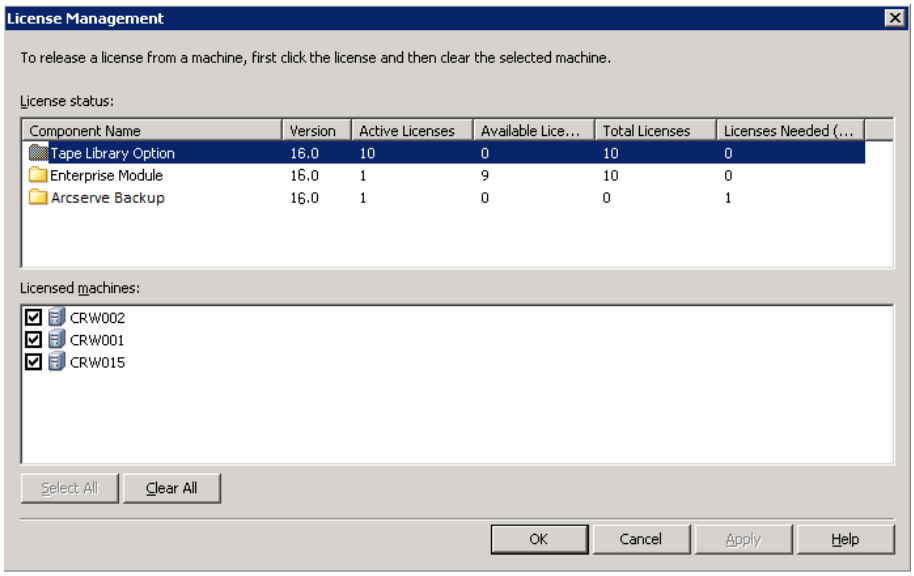
     Examples:

     - You are using one purchased license and one trial license for a component. Arcserve Backup recommends purchasing one license to replace the trial license so that you have uninterrupted use of selected component.
     - You are protecting six Windows computers using the Client Agent for Windows. You purchased four Client Agent for Windows licenses. In the past, backups may have failed due to an insufficient number licenses. Arcserve Backup recommends purchasing two additional licenses to help ensure that you have uninterrupted use of the Client Agent for Windows.

- **Licensed machines**--Specifies the names of the computers using the active licenses for the selected component.

  Example:

  - The following dialog illustrates that there are 10 active licenses and zero available licenses for the Tape Library Option. The host names of the computers using the Tape Library Option licenses display in the Licensed machines field.



Release Licenses from Servers

Arcserve Backup licensing functions on a count-based mechanism. Count-based licensing lets you grant a single overall license to the application with a predetermined number of active license rights included in the overall license pool. Each server that uses the license is granted an active license from the pool, on a first-come basis, until the total number of available license rights has been reached. If all the active license rights have already been applied and you need to add a license to a different member server, you must remove the license rights from one of servers to reduce the count before the different member server can use the license.

To release licenses from servers

1. From the Arcserve Backup Manager Console, open the Server Admin by clicking Server Admin in the Quick Start menu.

   The Server Admin opens.

2. From the server directory tree, right-click the primary server and select Manage Licenses from the pop-up menu.

   The License Management dialog opens.

3. From the License status section, select the component containing the license that you want to release.

   The machines using the license display in the Licensed machines field.

4. Clear the check box next to the machine name with the license that you want to release and click Apply.

   The active license is released from the selected server. The license is now available to other servers running the Arcserve Backup product in your Arcserve domain.

   Note: After you click the Apply button, the selected machine no longer appears in the Licensed machines field.

How to Install Arcserve Backup Server-Based Options

The following options are installed on the primary server or stand-alone server:

- Central Management Option

  Note: To install this option, you must install the Arcserve Backup Primary Server.

- Tape Library Option
- Storage Area Network (SAN) Option

There are two methods that you can use to install the Arcserve Backup server-based options:

- Install these options when you install Arcserve Backup.
- Install these options using the Server Admin.

From the Server Admin, you can install and uninstall server-based options.

Note: For more information about using the server Admin to install and uninstall server-based options, see the *Administration Guide*.

Appendix C: Acknowledgements

Portions of this product include software developed by third-party software providers. The following section provides information regarding this third-party software.

This section contains the following topics:

MD5 Message Digest Algorithm (see page 349)
VMware VDDK 5.1 (see page 350)
JRE v.1.7 (see page 350)
Amazon Web Services SDK for Java 1.3 (see page 351)
Windows Azure SDK for Java 2.0 (see page 352)

MD5 Message Digest Algorithm

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm.

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

VMware VDDK 5.1

This Arcserve product contains certain VDDK technology licensed by CA from VMware, Inc. and its licensors (the "VDDK Software"). The VDDK Software contains certain third party information and terms which identifies various third-party components that may be used with the VDDK Software and sets out certain notices, attributions and/or terms that VMware is required to provide to you by the third party licensors of those components. Such information is provided in the file open_source_license_VMware_Virtual_Disk_Development_Kit_5.0.txt, which accompanies the VDDK Software. In addition, Arcserve makes the source code of certain of these third party components available under their respective open source licenses at http://opensrcd.ca.com/ips/08384_6/.

JRE v.1.7

This Product is distributed with JRE v.1.7. Use of the Commercial Features of the JRE for any commercial or production purpose requires a separate license from Oracle. "Commercial Features" means those features identified Table 1-1 (Commercial Features In Java SE Product Editions) of the Software documentation accessible at http://www.oracle.com/technetwork/java/javase/documentation/index.html. Oracle has provided additional copyright notices and information that may be applicable to portions of the JRE in the THIRDPARTYLICENSEREADME.txt file that accompanies the JRE files and at http://www.oracle.com/technetwork/java/javase/documentation/index.html."

Amazon Web Services SDK for Java 1.3

This product includes Commons-codec-1.3, Commons-logging-1.1.1, Httpcomponents-client-4.1.1, Jacksoncore-1.8, Stax-api-1.0.1, and Stax-ri-1.20, which were obtained from the Amazon Web Services LLC under various licenses set forth below, and is distributed by CA for use with this CA product in unmodified, object code form, under the CA license agreement. The following information sets out certain notices, attributions and/or other information CA is required to provide to you by the third party licensors of these components. The terms contained in the CA license agreement are offered by CA and not by the third party licensors. The contents set forth below are for informational purposes only and do not modify the terms of the license agreement between you and CA. The third party licensors of these components provide them on an "AS-IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE, and disclaim liability for any claim or loss, including, without limitation, direct, indirect, special, punitive, exemplary or consequential damages. Source code for Java-mail-1.4.3 may be obtained from Java-mail-1.4.3 is distributed by CA for use with this CA product in unmodified, object code form, under the CA End User License Agreement. Any provisions in the CA End User License Agreement that differ from the CDDL are offered by CA alone and not by any other party. CA makes the source code for java-mail-1.4.3 available at http://opensrcd.ca.com/ips/11049_4/ under the terms of the CDDL v.1.0. license.

Windows Azure SDK for Java 2.0

This product contains portions of Windows Azure SDK for Java 2.0, which are distributed in accordance with the following terms:

Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

   "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

    a. You must give any other recipients of the Work or Derivative Works a copy of this License; and

    b. You must cause any modified files to carry prominent notices stating that You changed the files; and

    c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Portions of the Windows Azure SDK for Java were obtained under the following license(s):

dom4j

Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.
4. Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.
5. Due credit should be given to the DOM4J Project - http://www.dom4j.org

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Jaxen

/*

$Id: LICENSE.txt,v 1.5 2006/02/05 21:49:04 elharo Exp $

Copyright 2003-2006 The Werken Company. All Rights Reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Jaxen Project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

*/

Glossary

Arcserve Backup Agent Deployment

Arcserve Backup Agent Deployment is a wizard-like application that lets you install and upgrade a collection of Arcserve Backup agents on multiple remote computers simultaneously.

caroot account

The caroot account is the default account that Arcserve Backup uses as an authentication mechanism for management purposes. The password for the caroot password account can consist of any combination of alphanumeric and special characters, but may not exceed 15 bytes.

Note: A password totaling 15 bytes equates to approximately 7 to 15 characters.

data mover server

Arcserve Backup data mover servers facilitate the transfer of data to local storage devices. The storage devices include shared libraries and file system devices. Data mover servers are supported on UNIX or Linux operating systems. Arcserve Backup manages data mover servers from a single, centralized, primary server. Arcserve Backup data mover servers function in a manner that is similar to member servers.

file system agent

File system agents are Arcserve Backup applications that you install on computers running various operating systems that let you protect the files that reside on the computers.

member server

Member servers function as worker servers to a primary server. Member servers process jobs dispatched by the primary server. Using primary and member servers you can have a single point of management for multiple Arcserve Backup servers in your environment. You can then use the Manager Console on the primary server to manage its member servers.

primary server

Primary servers function as a master server that controls itself and one or more member servers and data mover servers. With primary servers you can manage and monitor backup, restore, and other jobs that run on primary servers, member servers, and data mover servers. Using primary, member, and data mover servers, you can have a single point of management for multiple Arcserve Backup servers in your environment. You can then use the Manager Console to manage the primary server.

response file

Response files are text-based files used with silent installations that contain setup and configuration settings for Arcserve Backup products and components.

virtual machine

A virtual machine is a software based environment that allows a partition to behave like a physical computer. Arcserve Backup supports backing up, restoring, and recovering data that resides on VMware and Microsoft Hyper-V based virtual machines.

Index

A

about this guide • 12
add Arcserve D2D servers (proxy) • 188
Arcserve Backup, introduction • 11
Arcserve D2D
    adding servers • 188
    opening Arcserve D2D from Arcserve Backup • 191
Arcserve database
    data migration from a previous release • 57
    installation methods • 40
    start the Arcserve database protection job • 207
Arcserve servers
    Arcserve server types • 40, 41
    member server • 41
    primary server • 41
    server options • 45
    stand-alone server • 41

B

backwards compatibility • 56

C

CA Antivirus • 183
clusters
    deployment considerations • 127
clusters, MSCS clusters
    cldelete cluster resources • 148
    deployment planning • 128
    hardware requirements • 131
    remove Arcserve Backup from cluster • 147
    resource preparation • 131
    software requirements • 131
clusters, NEC clusters • 150
    deployment planning • 128
    disable cluster scripts • 175
    enable cluster scripts • 177
    hardware requirements • 150
    remove Arcserve Backup from cluster • 172
    resource preparation • 151
    software requirements • 151
    stop cluster groups • 174
clusters, Windows Server 2008 • 127, 131, 134, 147, 148
code pages
    about • 204
    configuration, Backup Manager • 205
    configuration, Restore Manager • 206
communication port, Global Dashboard • 236
communication ports, firewall • 226, 245

D

database
    data migration from a previous release • 57
    MS SQL configuration • 48, 209
    ODBC data source configuration • 209
Device Configuration
    Device Wizard • 210
Device Wizard • 210
devices, supported • 37

E

engines
    service state icons • 200

F

file system agents, release levels • 58
file system devices, creating • 220
firewall configuration • 223, 224, 225

G

Global Dashboard
    configure Branch Primary Server • 216
    configure Central Primary Server • 213
    configure Global Dashboard • 211, 213, 216
    considerations • 53
    installation prerequisites • 81
    server communication • 236

H

home page • 195

I

install Arcserve Backup • 86
installation • 49
installation considerations
    Microsoft SQL Server • 48

Microsoft SQL Server 2008 Express Edition • 46
remote database • 49
supported upgrades • 55
installation methods • 40
installation wizard • 40
installtation progress logs • 52
integrating products
CA Antivirus • 183
introduction, Arcserve Backup • 11

L

language settings • 204
licensing
ALP certificate • 57
managing • 345
release licenses • 347
requirements • 57
log in to Arcserve Backup • 200

M

Manager Console
opening • 193
specify preferences • 202
Mastersetup • 120
member server • 41
Microsoft SQL Server
database consistency check • 209
installation considerations • 48
ODBC configuration • 209
SQL connections • 209
Microsoft SQL Server 2008 Express Edition
installation considerations • 46
MSCS clusters
delete cluster resources • 148
deployment planning • 128
hardware requirements • 131
remove Arcserve Backup from cluster • 147
resource preparation • 131
software requirements • 131

N

NEC clusters • 150
deployment planning • 128
disable cluster scripts • 175
enable cluster scripts • 177
hardware requirements • 150
remove Arcserve Backup from cluster • 172
resource preparation • 151
software requirements • 151
stop cluster groups • 174

O

open the Arcserve D2D home page • 191
options
Discovery Configuration options • 237
global preferences • 202

P

planning your environment
backup window • 16
bandwidth • 18
budget • 14
capacities • 24
data transfer rates • 19
hardware throughput • 16
infrastructure • 15
network enhancements • 20
parallel storage • 24
recovering from a disaster • 29
sample calculations • 30
scheduling • 16
vault accessibility and security • 29
platforms, supported • 37
ports configuration • 224, 225, 249
post-installation tasks • 126, 211
prerequisite installation tasks • 81
primary server • 41
protecting Arcserve D2D data • 184

R

remove Arcserve D2D servers • 190
response file, creating • 101

S

service state icons • 200
silent installation
create a response file • 101
installation methods • 40
specify Manager Console preferences • 202
stand-alone server • 41
start the Arcserve database protection job • 207
Storage Area Network (SAN) • 38
supported devices • 37
supported platforms • 37
supported upgrades • 55

synthetic full backup
backup scope • 22
system account
job security • 207
manage authentication • 207
system requirements • 81

T

tape libraries • 38

U

Unicenter software delivery
install Arcserve Backup • 120
installation methods • 40
uninstall Arcserve Backup
MSCS cluster • 147
NEC cluster • 172
primary, member, and stand-alone server • 253
upgrade, from a previous release • 86
upgrades
backwards compatibility • 56
data migration from a previous release • 57
installation methods • 40
Manager Console • 56
supported • 55
user tutorial • 199