CA ARCserve® Backup for Windows

Implementation Guide

r15

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

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

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

The right to print 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 CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA 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 is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

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

Copyright © 2010 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Product References

This document references the following CA products:

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

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

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At CA ARCserve Backup Support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Documentation Changes

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

- Updates the entire Implementation Guide to reflect changes relating to Microsoft SQL Server 2008 Express Edition as the default CA ARCserve Backup database.
- Added Global Dashboard Considerations (see page 75). Describes things to consider when deploying Global Dashboard in your environment.
- Updated How the Installation Process Affects Operating Systems (see page 40) to reflect the list of applications installed by CA ARCserve Backup.
- Updated Unsigned CA ARCserve Backup Files (see page 47) to reflect the affects of CA ARCserve Backup on operating systems.
- Updated Supported Upgrades (see page 77) to reflect upgrades supported by this release of CA ARCserve Backup.
- Updated Backward Compatibility (see page 78) to reflect how this release of CA ARCserve Backup supports previous versions of CA ARCserve Backup components.
- Updated Manager Console Support for Previous Releases (see page 79) to reflect how this release of the CA ARCserve Backup Manager Console can be used with previous releases of CA ARCserve Backup.
- Updated CA ARCserve Backup File System Agents Release Levels (see page 82) to reflect the release numbers of CA ARCserve Backup files system agents packaged with this release of CA ARCserve Backup.
- Updated CA ARCserve Backup Home Page (see page 203) to include information about new CA ARCserve Backup components.
- Updated Configure the Windows Firewall to Optimize Communication (see page 216) to include support for Windows Server 2008 R2.
- Added Configure Global Dashboard (see page 223). Topic and its child topics describe how to configure the central sites and branch sites.
- Added chapter Uninstalling CA ARCserve Backup (see page 265). This chapter describes how to uninstall CA ARCserve Backup, agents, and options from Windows Control Panel, uninstall CA ARCserve Backup using the command line, and uninstall Agent Deployment setup files.

Contents

Chapter 1: Introducing CA ARCserve Backup 13

Introduction 13
Purpose of This Guide 14

Chapter 2: Planning Your Storage Environment 15

Preliminary Tasks 15
Enterprise Storage Requirements 16
- Budget Considerations 16
- Network and Computer Infrastructure Requirements 17

Data Transfer Requirements 17
- Backup Schedule Requirements 18
- Data Backup Window Considerations 18
- Hardware Data Transfer Rates 18
- Network Bandwidth Considerations 20
- Data Transfer Requirements and Resources Calculations 21
- Data Path Considerations 22
- Alternate Data Path Considerations 23
- Parallel Storage Operations (Multiple Streaming) 25

Storage Capacity Requirements 26
- Online Recovery Data Storage Requirements 26
- Backup Data Storage Requirements 26
- Global Dashboard Data Storage Requirements 27
- Storage Capacities and Resources 28
- Testing Plans and Assumptions 29

Catastrophic Events 29
- Risk Assessment 30
- Off-Site Repository Considerations 30
- Disaster Recovery Archive Considerations 31
- Disaster Recovery Testing 31

Sample Calculations 32
- Transfer Rate for Clients and Servers on a 100Base-T Ethernet LAN With No Subnets 33
- Transfer Rate for Clients and Servers on Two 100Base-T Ethernet Subnets 34
- Transfer Rate for Clients and Servers on a Gigabit Ethernet Network 35
- Transfer Rate for a Server With No Clients 35
- Transfer Rate For Server With SAN Option 36
- Storage Capacity for Two Sets of Recovery Data, One Full and One Incremental Backup 37

Chapter 3: Planning Your CA ARCserve Backup Installation 39

Supported Platforms . . . 39
Supported Devices . . . 39
Tape Library Installations . . . 40
Storage Area Network (SAN) Installations . . . 40
How the Installation Process Affects Operating Systems . . . 40
Unsigned Binary Files . . . 47
Binary Files Containing Incorrect File Version Information . . . 53
Binary Files that are not Uninstalled Completely . . . 54
Binary Files that do not Contain an Embedded Manifest . . . 56
CA ARCserve Backup MSI Installer Package Identification . . . 58
Windows MSI Installer Package Custom Columns . . . 59
Amount of Disk Space Required to Install CA ARCserve Backup . . . 60
Installation Methods . . . 61
Types of CA ARCserve Backup Server Installations . . . 62
CA ARCserve Backup Server Options . . . 66
caroot User Account . . . 66
Database Requirements . . . 67
Microsoft SQL Server 2008 Express Edition Considerations . . . 67
Microsoft SQL Server Database Considerations . . . 69
Agent for ARCserve Database . . . 72
Installation Progress Logs . . . 74
Global Dashboard Considerations . . . 75
Upgrade Considerations . . . 76
Supported Upgrades . . . 77
Backward Compatibility . . . 78
Manager Console Support for Previous Releases . . . 79
Global Dashboard Upgrades . . . 79
Data Migration from a Previous Release . . . 80
Product License Requirements . . . 81
ALP Key Certificate . . . 81
CA ARCserve Backup File System Agents Release Levels . . . 82

Chapter 4: Installing and Upgrading CA ARCserve Backup 83

How to Complete Prerequisite Tasks . . . 83
Install CA ARCserve Backup . . . 88
Upgrade CA ARCserve Backup from a Previous Release . . . 97
Create a Silent Installation Response File . . . 105
CA ARCserve Backup Agent Deployment . . . 111
Deploy Agents to Remote Hosts Using Automatic Upgrade . . . 114
Deploy Agents to Remote Hosts Using Custom Deployment . . . 116

Deploy Agents to VMs Using Virtual Machine Deployment 120
Upgrade CA ARCserve Backup Agents Silently to the Current Release 123
How to Install CA ARCserve Backup Using Unicenter Software Delivery 126
Register CA ARCserve Backup on the Unicenter Software Delivery Server 126
Components and Prerequisites 127
Install CA ARCserve Backup Components Using Unicenter Software Delivery 132
Post-Installation Tasks 133

Chapter 5: Installing and Upgrading CA ARCserve Backup in a Cluster-aware Environment 135

Introduction to Cluster-aware Installations 135
Deployment Considerations 135
Plan Your CA ARCserve Backup HA Deployment 136
Deploy CA ARCserve Backup Server on MSCS 138
MSCS Hardware Requirements 139
MSCS Software Requirements 139
MSCS Cluster Resource Preparation 139
Install CA ARCserve Backup in an MSCS Cluster-aware Environment 140
Upgrade CA ARCserve Backup from r11.5 to r15 in an MSCS Cluster Environment 151
Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an MSCS Cluster Environment 157
Uninstall CA ARCserve Backup from an MSCS Cluster 161
Delete CA ARCserve Backup Cluster Resources 162
Deploy CA ARCserve Backup Server on NEC Cluster 163
NEC CLUSTERPRO/ExpressCluster Hardware Requirements 163
NEC CLUSTERPRO/ExpressCluster Software Requirements 164
NEC CLUSTERPRO/ExpressCluster Resource Preparation 164
Install CA ARCserve Backup in an NEC Cluster-aware Environment 165
Upgrade CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO Environment 180
Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an NEC CLUSTERPRO Environment 193
Uninstall CA ARCserve Backup from a NEC CLUSTERPRO/ExpressCluster 197
How to Verify a Cluster-aware Installation and Upgrade 198

Chapter 6: Integrating CA ARCserve Backup with Other Products 199

CA Antivirus Integration 199
CA ARCserve Replication Integration 199
CA ARCserve Backup Patch Manager Integration 200

Chapter 7: Configuring CA ARCserve Backup 201

Open the Manager or Manager Console 201
CA ARCserve Backup Home Page 203

First-Time Home Page and User Tutorial . . . 207
Service State Icons . . . 208
Log in to CA ARCserve Backup . . . 208
Specify CA ARCserve Backup Manager Preferences . . . 210
Code Pages . . . 212
How CA ARCserve Backup Supports Multiple Code Pages . . . 212
Specify Code Pages in the Backup Manager Window . . . 213
Specify Code Pages in the Restore Manager Window . . . 214
CA ARCserve Backup System Account . . . 214
How CA ARCserve Backup Manages Authentication . . . 215
How to Use the System Account for Job Security . . . 215
Configure the Windows Firewall to Optimize Communication . . . 216
Allow Database Agents that Reside on Remote Subnets to Communicate with the ARCserve Server . . . 218
Start the CA ARCserve Backup Database Protection Job . . . 219
Fine-Tune the CA ARCserve Backup SQL Server Database . . . 220
How to Calculate the Number of Required SQL Connections . . . 221
Database Consistency Checks . . . 221
Specify ODBC Communication for Remote Database Configurations . . . 221
Configure Devices Using the Device Wizard . . . 222
Configure Enterprise Module Components . . . 223
Configure Global Dashboard . . . 223
Configure the Central Site . . . 225
Configure a Branch Site . . . 228
Create File System Devices . . . 232
How to Define Include and Skip Parameters for CA ARCserve Backup Database Agents . . . 235
Configuring Your Firewall to Optimize Communication . . . 236
Ports Configuration File Guidelines . . . 237
Modify the Ports Configuration File . . . 238
Ports Used by CA ARCserve Backup Components . . . 239
Test Communication Through a Firewall . . . 264

Chapter 8: Uninstalling CA ARCserve Backup 265

Uninstall CA ARCserve Backup . . . 265
Uninstall CA ARCserve Backup Components Using the Command Line . . . 268
Uninstall Agent Deployment Setup Files . . . 271

Appendix A: Troubleshooting Your Installation 273

Setup Cannot Communicate with Remote Microsoft SQL Server Databases . . . 273
Unable to Log In to CA ARCserve Backup After Installing This Release . . . 275
CA ARCserve Backup Services Fail to Initialize . . . 276

The Tape Engine Does Not Start on Member Server Upgrades 277
Unable to Log in to CA ARCserve Backup After Upgrading to This Release 278
Unable to Determine What Devices Are Supported by CA ARCserve Backup 279
Cluster HA Resources Not Created 280

Appendix B: Using Best Practices to Install and Upgrade CA ARCserve Backup 281

Best Practices for Installing CA ARCserve Backup 281
How to Complete Prerequisite Tasks for Installing CA ARCserve Backup 282
Installing CA ARCserve Backup into a Single-server Environment 283
Installing a Primary Server with Member Servers 287
Installing a Primary Server with Member Servers and Devices 294
Installing a Primary Server with Member Servers and Shared Devices in a SAN 301
Installing Multiple Primary Servers with Member Servers in a SAN 309
Installing CA ARCserve Backup into a Cluster-aware Environment 317
Best Practices for Upgrading CA ARCserve Backup from a Previous Release 323
How to Complete Prerequisite Tasks for Upgrading CA ARCserve Backup 324
Upgrading a Stand-alone Server or Primary Server 326
Upgrading Multiple Stand-alone Servers in a Domain 332
Upgrading Multiple Stand-alone Servers Sharing a Remote Database 340
Upgrading Servers in a SAN Using a Local or Remote Database 347
Upgrading Multiple Servers in a SAN and Non-SAN Environment to this Release 356
Upgrading Multiple Servers Using a Central Database 364
Upgrading Multiple Servers in a Cluster-aware Environment 372
General Best Practices 380
Where to Install the Manager Console 381
How to Install and Manage Licenses 381
How to Install CA ARCserve Backup Server-Based Options 385

Appendix C: Acknowledgements 387

RSA Data Security, Inc. Acknowledgement 387

Index 389

Chapter 1: Introducing CA ARCserve Backup

This section contains the following topics:

Introduction (see page 13)
Purpose of This Guide (see page 14)

Introduction

CA 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 CA ARCserve Backup for Windows is the next generation in the CA 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. CA 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 CA ARCserve Backup installation
- Perform prerequisite installation tasks
- Install CA ARCserve Backup
- Upgrade CA ARCserve Backup from a previous release
- Uninstall CA ARCserve Backup
- Set up alternate installation methods
- Perform post-installation tasks
- Integrate with other CA products
- Use best practices to install CA ARCserve Backup and upgrade CA ARCserve Backup from a previous release

Chapter 2: Planning Your Storage Environment

This section contains the following topics:

Preliminary Tasks (see page 15)
Enterprise Storage Requirements (see page 16)
Data Transfer Requirements (see page 17)
Storage Capacity Requirements (see page 26)
Catastrophic Events (see page 29)
Sample Calculations (see page 32)

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 CA 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 CA ARCserve Backup.

After you have a clear idea of your storage needs, this chapter can help you to develop a comprehensive 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 chapter 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 CA 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 chapter.

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:

$$datatransferred = backupwindow \times minbandwidth$$

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:

$$datatransferred = 5\ hrs \times 36\ GB/hour = 180\ GB$$

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 CA 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 CA ARCserve Backup can help you take advantage of a SAN, see the *Storage Area Network (SAN) Option 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 CA ARCserve Backup servers on different subnets.

- In the absence of subnets, all backup data has to cross a single network to reach the CA 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 back up window and would economize on media.

CA 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.

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.

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. CA 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 (CA 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 CA 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 CA 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 CA 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 CA 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 CA 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 CA ARCserve Backup servers.
- A current, complete backup of the file systems, databases, and mail servers supported by CA ARCserve Backup.

You may want to include CA 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.

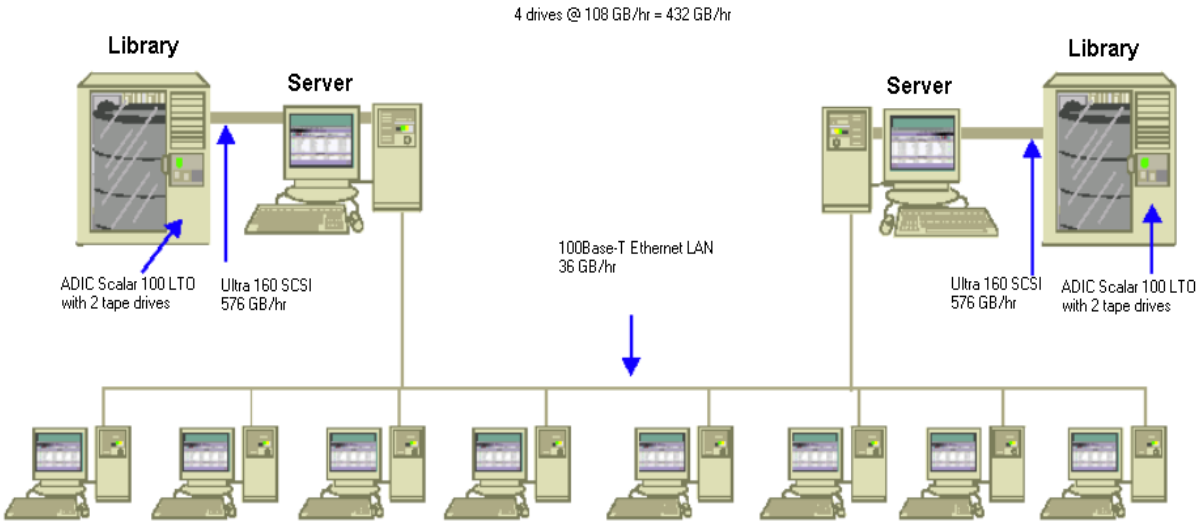
Sample Calculations

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

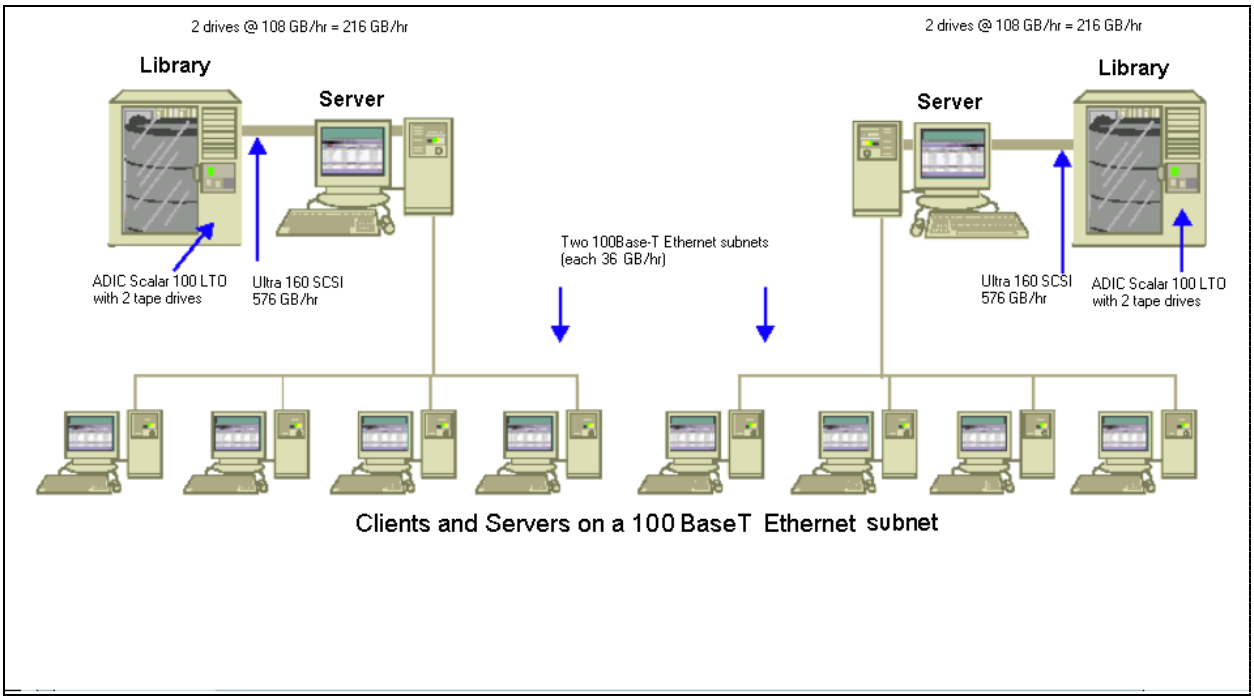
In this configuration, data cannot move across the network faster than 36 GB per hour, regardless of the number of servers and libraries available. To back up 1 Terabyte of data, the backup operation must run for 28 hrs.



Clients and Servers on a 100 BaseT Ethernet LAN

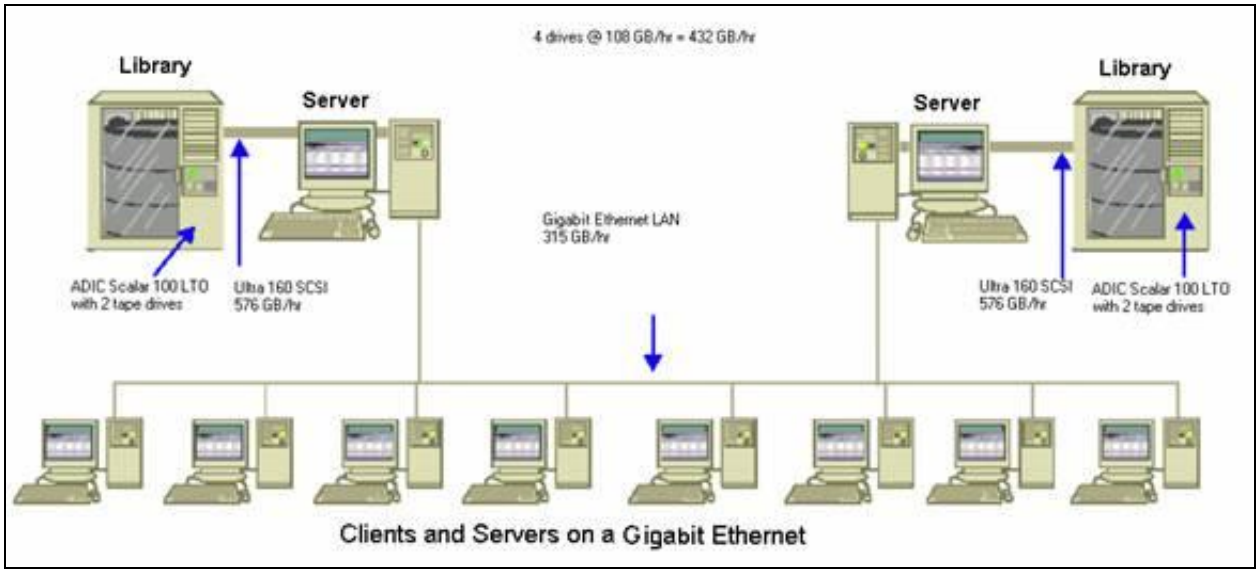
Transfer Rate for Clients and Servers on Two 100Base-T Ethernet Subnets

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.



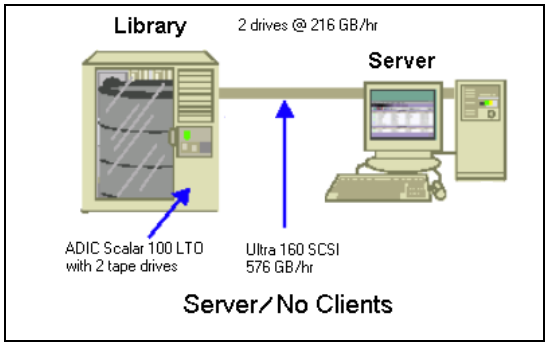
Transfer Rate for Clients and Servers on a Gigabit Ethernet Network

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.



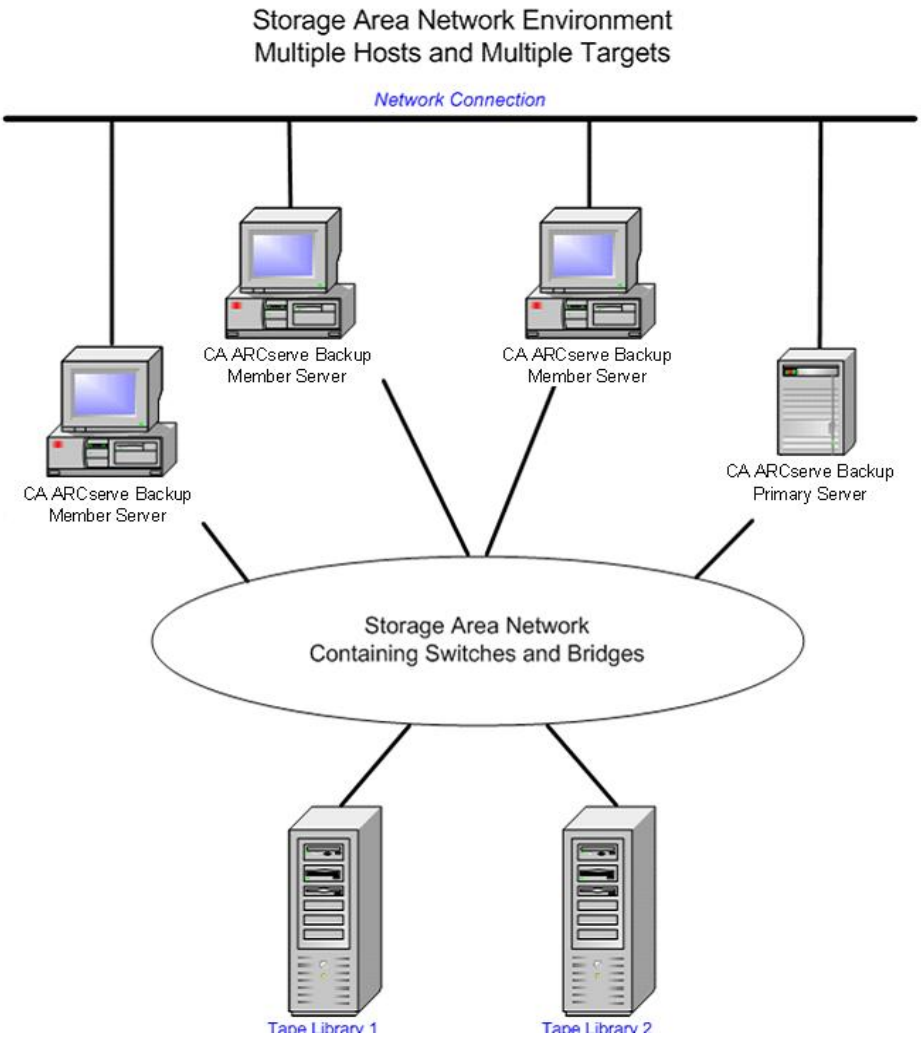
Transfer Rate for a Server With No Clients

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 Your CA ARCserve Backup Installation

This section contains the following topics:

Supported Platforms (see page 39)
Supported Devices (see page 39)
How the Installation Process Affects Operating Systems (see page 40)
Amount of Disk Space Required to Install CA ARCserve Backup (see page 60)
Installation Methods (see page 61)
Types of CA ARCserve Backup Server Installations (see page 62)
caroot User Account (see page 66)
Database Requirements (see page 67)
Global Dashboard Considerations (see page 75)
Upgrade Considerations (see page 76)
Product License Requirements (see page 81)
CA ARCserve Backup File System Agents Release Levels (see page 82)

Supported Platforms

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

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

For the most current list of supported operating systems, see the readme file or access the CA website at ca.com.

Supported Devices

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

Tape Library Installations

The CA ARCserve Backup base product includes support for single-drive tape and optical libraries. If you are using a tape or optical library with more than one drive, a separately installed Tape Library Option is required and you must license it on each ARCserve Primary Server or ARCserve Stand-alone Server with an attached multi-drive library.

CA ARCserve Backup automatically configures single-drive and multiple-drive tape and optical 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 CA 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.

How the Installation Process Affects Operating Systems

The CA 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 CA ARCserve Backup perform custom actions that let you install, upgrade, and uninstall CA ARCserve Backup. The following table describes the custom actions and the affected components.

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

Component	Description
CallAllowInstall	Lets the installation process check for conditions relating to the current CA ARCserve Backup installation.

Component	Description
CallPreInstall	Lets the installation process read and write MSI properties. For example, read the CA ARCserve Backup installation path from the MSI.
CallPostInstall	Lets the installation process perform various tasks relating to installation. For example, registering CA ARCserve Backup into the Windows Registry.
CallAllowUninstall	Lets the uninstallation process check for conditions relating the current CA ARCserve Backup installation.
CallPreUninstall	Lets the uninstallation process perform various tasks relating to uninstallation. For example, un-registering CA ARCserve Backup from the Windows Registry.

Directories Updated

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

CA 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 IA64 Systems

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

Client Agent for Windows for x64-Based Systems

- C:\Program Files\CA\ARCserve Backup Client Agent for Windows
- 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 IA64 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 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 IA64 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 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 Oracle for IA64 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

Enterprise Option for SAP R/3 for Oracle for IA64 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

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

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

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

C:\Windows\system

CA ARCserve Backup copies configuration files to the following directory:

C:\Documents and Settings\<user name>

Note: To view a list of CA ARCserve Backup unsigned files, see Unsigned CA ARCserve Backup Files (see page 47).

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:

- CA Licensing
- CA CAPKI (encryption)
- Microsoft Visual C++ 2005 SP1 Redistributable
- Microsoft Windows Installer 3.1 Redistributable (v2)
- Scan Engine 8.1 (eTrust Antivirus)

  Note: Setup does not install antivirus protection on IA64 operating systems.
- If you are installing CA ARCserve Backup server, the installation process also installs these applications:
  - Microsoft .NET Framework 3.5 SP1
  - Java Runtime Environment (JRE) 1.6.0.
  - Microsoft XML 4.0 SP2
- If you are installing Microsoft SQL Express Edition as the CA ARCserve Backup database, the following applications are also installed:
  - Microsoft SQL Server 2008 Express Edition SP1
  - Microsoft Windows Installer 4.5 Redistributable
- If you are installing the CA ARCserve Backup Agent for Oracle (x86/x64/IA64) or Enterprise Option for SAP R/3 for Oracle (x86/x64/IA64), the following applications are also installed:
  - Microsoft XML 4.0 SP2
  - Microsoft XML 6.0
  - Java Runtime Environment (JRE) 1.6.0.

Data Mover Servers

If you are installing CA ARCserve Backup UNIX and Linux Data Mover on a UNIX or Linux server, CA ARCserve Backup installs the following components on the data mover server:

- For Sun, HPUX, and Linux operating systems, CA ARCserve Backup installs Java Runtime Environment (JRE) 1.6.0 into the following directory on data mover servers:

  /opt/CA/SharedComponents/jre

- For AIX operating systems, CA ARCserve Backup installs IBM Java Runtime Environment (IBM JRE) 1.6.0 and Sun JRE 1.6.0 into the following directories on data mover servers:

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

Unsigned Binary Files

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

Binary Name	Source
C:\Program Files (x86)\CA\ARCserve Backup\CATALOG.DB\	CA ARCserve Backup **Note:** The binaries for this file are created dynamically. The installation location varies based on the implementation.
BaofNtNw.msi	CA ARCserve Backup
BrightStorSAK.msi	CA ARCserve Backup
CADiag.msi	CA ARCserve Backup
CADS.msi	CA ARCserve Backup
DBAExch.msi	CA ARCserve Backup
DBAExch12.msi	CA ARCserve Backup
DBASQL.msi	CA ARCserve Backup
NTAgent.msi	CA ARCserve Backup
ofant.sys	CA ARCserve Backup
OPTIO.msi	CA ARCserve Backup
OPTSBO.msi	CA ARCserve Backup

Binary Name	Source
RMANAgent.msi	CA ARCserve Backup
SetupCommon.msi	CA ARCserve Backup
SP2K7Agent.msi	CA ARCserve Backup
UniAgent.msi	CA ARCserve Backup
VMAgent.msi	CA ARCserve Backup
CALicense.msi	CA License
xalan-c_1_10.dll	Apache Software Foundation
xalan_messages_1_10.dll	Apache Software Foundation
xerces-c_2_7.dll	Apache Software Foundation
xsec_1_2_0.dll	Apache Software Foundation
roboex32.dll	Blue Sky Software Corporation
CFX2032.DLL	ChartFX
GX1142R.dll	Classworks
ccme_base.dll	EMC (RSA)
ccme_ecc.dll	EMC (RSA)
ccme_eccaccel.dll	EMC (RSA)
cryptocme2.dll	EMC (RSA)
libetpki_openssl_crypto.dll	EMC (RSA)
Data1.cab	Flexera Software (formerly Acresso Software). It is generated by InstallShield.
icudt34.dll	IBM
icuin34.dll	IBM
icuio34.dll	IBM
icule34.dll	IBM
iculx34.dll	IBM
icutest.dll	IBM
icutu34.dll	IBM
icuuc34.dll	IBM
unzip.exe	Info-ZIP
awt.dll	Java Runtime Environment

Binary Name	Source
axbridge.dll	Java Runtime Environment
cmm.dll	Java Runtime Environment
dcpr.dll	Java Runtime Environment
deploy.dll	Java Runtime Environment
dt_shmem.dll	Java Runtime Environment
dt_socket.dll	Java Runtime Environment
eula.dll	Java Runtime Environment
fontmanager.dll	Java Runtime Environment
hpi.dll	Java Runtime Environment
hprof.dll	Java Runtime Environment
instrument.dll	Java Runtime Environment
ioser12.dll	Java Runtime Environment
j2pcsc.dll	Java Runtime Environment
j2pkcs11.dll	Java Runtime Environment
jaas_nt.dll	Java Runtime Environment
java.dll	Java Runtime Environment
java.exe	Java Runtime Environment
java_crw_demo.dll	Java Runtime Environment
javac.exe	Java Runtime Environment
javacpl.cpl	Java Runtime Environment
javacpl.exe	Java Runtime Environment
java-rmi.exe	Java Runtime Environment
javaw.exe	Java Runtime Environment
javaws.exe	Java Runtime Environment
jawt.dll	Java Runtime Environment
JdbcOdbc.dll	Java Runtime Environment
jdwp.dll	Java Runtime Environment
jli.dll	Java Runtime Environment
jpeg.dll	Java Runtime Environment
jpicom.dll	Java Runtime Environment

Binary Name	Source
jpiexp.dll	Java Runtime Environment
jpinscp.dll	Java Runtime Environment
jpioji.dll	Java Runtime Environment
jpishare.dll	Java Runtime Environment
jsound.dll	Java Runtime Environment
jsoundds.dll	Java Runtime Environment
jusched.exe	Java Runtime Environment
jvm.dll	Java Runtime Environment
keytool.exe	Java Runtime Environment
kinit.exe	Java Runtime Environment
klist.exe	Java Runtime Environment
ktab.exe	Java Runtime Environment
management.dll	Java Runtime Environment
net.dll	Java Runtime Environment
nio.dll	Java Runtime Environment
npjava11.dll	Java Runtime Environment
npjava12.dll	Java Runtime Environment
npjava13.dll	Java Runtime Environment
npjava14.dll	Java Runtime Environment
npjava32.dll	Java Runtime Environment
npoji610.dll	Java Runtime Environment
npt.dll	Java Runtime Environment
orbd.exe	Java Runtime Environment
pack200.exe	Java Runtime Environment
policytool.exe	Java Runtime Environment
regutils.dll	Java Runtime Environment
rmi.dll	Java Runtime Environment
rmid.exe	Java Runtime Environment
rmiregistry.exe	Java Runtime Environment
servertool.exe	Java Runtime Environment

Binary Name	Source
splashscreen.dll	Java Runtime Environment
sunmscapi.dll	Java Runtime Environment
tnameserv.exe	Java Runtime Environment
unpack.dll	Java Runtime Environment
unpack200.exe	Java Runtime Environment
verify.dll	Java Runtime Environment
w2k_lsa_auth.dll	Java Runtime Environment
wsdetect.dll	Java Runtime Environment
zip.dll	Java Runtime Environment
ansiatl.dll	Microsoft
ATL80.dll	Microsoft
cdcdrom.sys	Microsoft
cdrom.sys	Microsoft
COMPRESS.EXE	Microsoft
dbghelp.dll	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

Binary Name	Source
msstkprp.dll	Microsoft
msvcm80.dll	Microsoft
msvcp60.dll	Microsoft
msvcp80.dll	Microsoft
msvcr71.dll	Microsoft
msvcr80.dll	Microsoft
Msvcrt40.dll	Microsoft
msxml4.dll	Microsoft
msxml4r.dll	Microsoft
rsfx.msi	Microsoft
sql_common_core.msp	Microsoft
sql_engine_core_inst.msp	Microsoft
sql_engine_core_inst_loc.msp	Microsoft
sql_engine_core_shared.msp	Microsoft
sql_engine_core_shared_loc.msp	Microsoft
sqlbrowser.msp	Microsoft
sqlncli.msi	Microsoft
sqlsqm.msp	Microsoft
sqlsupport.msi	Microsoft
sqlwriter.msp	Microsoft
tpcdrom.sys	Microsoft
vcomp.dll	Microsoft
vcredist_IA64.exe	Microsoft
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
C:\Program Files (x86)\Microsoft SQL Server\100\Setup Bootstrap\Log\	Microsoft **Note:** The binaries for this file are created dynamically. The installation location varies based on the implementation.
libeay32.dll	OpenSSL
Vim25Service2005.XmlSerializers.dll	VMware

Binary Name	Source
VimService2005.XmlSerializers.dll	VMware
zlib1.dll	Zlib Compression Library

Binary Files Containing Incorrect File Version Information

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

Binary Name	Source
ASMBO.dll	CA ARCserve Backup
CAVMPROP.dll	CA ARCserve Backup
dmoption.dll	CA ARCserve Backup
InstAlrt.dll	CA ARCserve Backup
rdsetup.dll	CA ARCserve Backup
setuprd.exe	CA ARCserve Backup
inocboot.exe	CA AVEngine
Cazipxp.exe	CA License
UpdateData.exe	CA License
xalan_messages_1_10.dll	Apache Software Foundation
ccme_base.dll	EMC (RSA)
ccme_ecc.dll	EMC (RSA)
ccme_eccaccel.dll	EMC (RSA)
cryptocme2.dll	EMC (RSA)
libetpki_openssl_crypto.dll	EMC (RSA)
icutest.dll	IBM
icutu34.dll	IBM
unzip.exe	Info-ZIP
a0fkyeum.dll	Microsoft
MSClusterLib.dll	Microsoft
sqlwvss_xp.dll	Microsoft
WindowsServer2003-KB942288-v4-x	Microsoft

Binary Name	Source
64.exe	
WindowsServer2003-KB942288-v4-x86.exe	Microsoft
WindowsXP-KB942288-v3-x86.exe	Microsoft
libeay32.dll	OpenSSL
casmgmtsvc.exe	Tanuki Software
wrapper.dll	Tanuki Software
Vim25Service2005.XmlSerializers.dll	VMware
VimService2005.XmlSerializers.dll	VMware
zlib1.dll	Zlib compression library

Binary Files that are not Uninstalled Completely

CA ARCserve Backup installs binary files developed by third parties, other CA products, and CA 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	CA 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
C:\$Mft	Microsoft

Binary Name	Source
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
C:\Windows\SoftwareDistribution\DataStore\	Microsoft

Binary Name	Source
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

CA ARCserve Backup installs binary files developed by third parties, other CA products, and CA 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	CA ARCserve Backup
ca_vcbpopulatedb.exe	CA ARCserve Backup
VCBUI.exe	CA ARCserve Backup
inocboot.exe	CA AVEngine
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
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

Binary Name	Source
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
SQLPS.ni.exe	Microsoft
vcredist_IA64.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

CA ARCserve Backup installs binary files developed by other CA products and CA 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	CA ARCserve Backup
Cazipxp.exe	CA License

CA ARCserve Backup MSI Installer Package Identification

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

Windows MSI Installer Package Custom Columns

The MSI installer for Windows lets applications add Custom Columns to the MSI Standard Tables. However, CA ARCserve Backup installer packages contain a Custom Column named "Assembly_" that is not included in the MSI Standard Table.

This behavior occurs because CA ARCserve Backup r15 was developed using InstallSheild 2008, which does not support adding the "Assembly_" table to the MSI Standard Tables.

The following list identifies the affected CA ARCserve Backup installer packages:

- AgentDeploy.msi
- ARCserve.msi
- BaofNtNw.msi
- BrightStorSAK.msi
- CADiag.msi
- CADS.msi
- CentralDashboard.msi
- DBAExch.msi
- DBAExch12.msi
- DBAIFX.msi
- DBANotes.msi
- DBASQL.msi
- DBASYB.msi
- EBSAgent.msi
- NASAgent.msi
- NTAgent.msi
- OPTDRO.msi
- OPTEO.msi
- OPTIO.msi
- OPTSBO.msi

- PM.msi
- RMANAgent.msi
- SAPAgent.msi
- SetupCommon.msi
- SP2K7Agent.msi
- UniAgent.msi
- VMAgent.msi

Amount of Disk Space Required to Install CA ARCserve Backup

You can install CA 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 CA ARCserve Backup server that you install.

The information that follows describes the amount of free disk space required to install the CA ARCserve Backup for Windows base product, CA ARCserve Backup Client Agent for Windows, and CA 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 CA ARCserve Backup using the following methods:

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

  The installation wizard lets you specify the following installation options:

  Installation or Upgrade Type

  Lets you install CA 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 CA ARCserve Backup on one or more remote systems simultaneously. With remote installations, the target remote systems can consist of different CA ARCserve Backup server types, different CA 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. CA 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 CA ARCserve Backup Server Installations (see page 62).

  CA ARCserve Backup Products

  Lets you specify the CA 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 CA 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 CA ARCserve Backup. Microsoft SQL Server 2008 Express Edition must be installed on the CA ARCserve Backup server. For more information, see Microsoft SQL Server 2008 Express Edition Considerations (see page 67).

  Microsoft SQL Server is a highly scalable database application that can be installed on the CA ARCserve Backup server or on any other system in your environment. For more information see, Microsoft SQL Server Database Considerations (see page 69).

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

  Important! CA 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 105) and Install CA ARCserve Backup Using Unicenter Software Delivery (see page 126).

Types of CA ARCserve Backup Server Installations

CA ARCserve Backup supports the following types of installations:

Express

Lets you simplify the installation process by installing the CA 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 CA 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	c:\program files (x86)\CA\ARCserve

Product/Component	Default Installation Location (x86)	Default Installation Location (x64)
	Backup\GlobalDashboard	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
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

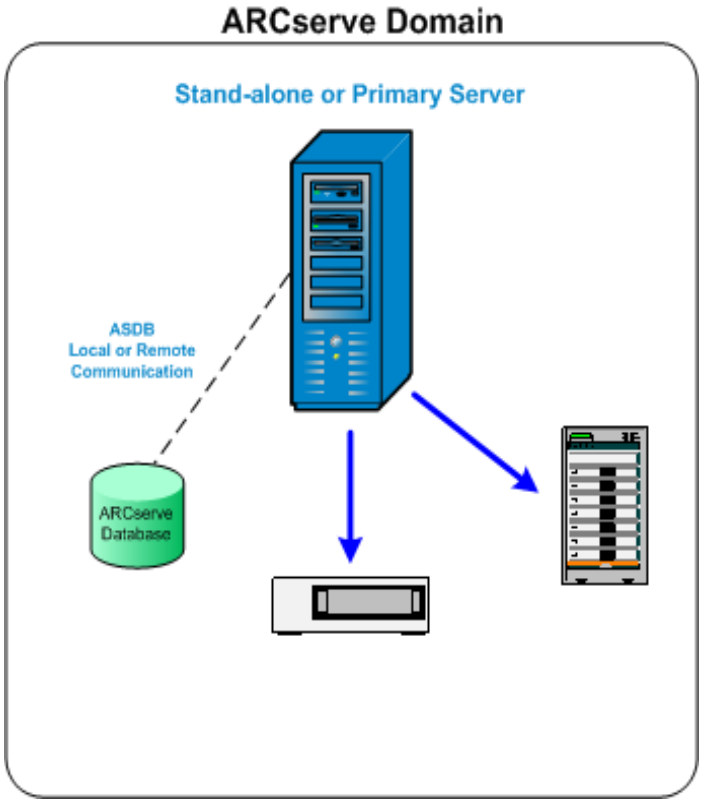
Lets you specify individual components, agents, and options that you want to install.

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 CA 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 CA 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.

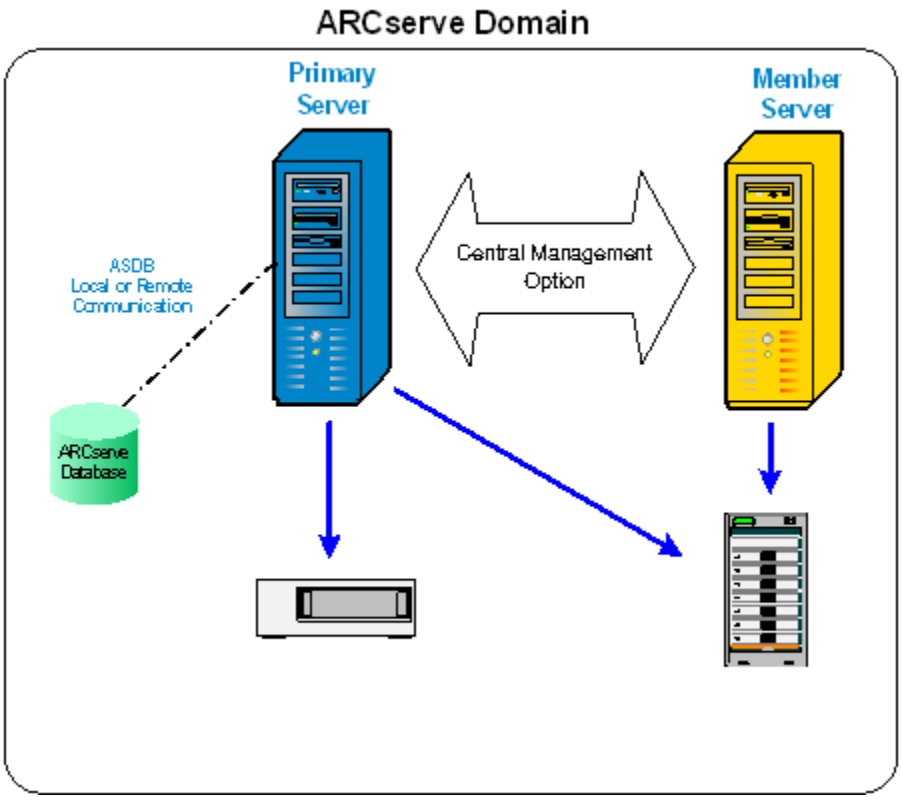
Note: For information about using primary servers to manage daily activities, see Central Management.

ARCserve Member Server

Consists of a server in a CA 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 CA 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 CA ARCserve Backup Servers, Agents, and Options.

CA ARCserve Backup Server Options

The following table describes the CA ARCserve Backup options that you can install on each type of CA 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 CA ARCserve Backup server-based options after you install CA ARCserve Backup, use the Server Admin Manager to complete the task. For more information, see the *Administration Guide*.

caroot User Account

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

The default caroot user account has root privileges for all CA 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: CA ARCserve Backup user names control access to only CA ARCserve Backup functions, and should not be confused with the operating system-required login name and password.

Database Requirements

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

- Microsoft SQL Server 2008 Express Edition (see page 67)
- Microsoft SQL Server (see page 69)

If you are upgrading to this release of CA 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 77).

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 CA ARCserve Backup. Review the following information if you are considering using Microsoft SQL Server 2008 Express Edition to support the CA 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 CA 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 CA ARCserve Backup on a system that functions as a domain controller, Setup configures the CA 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 CA 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 CA 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.
- Microsoft SQL Server 2008 Express Edition is not supported on IA-64 (Intel Itanium) operating systems.

- 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 CA ARCserve Backup and is provided for you on the CA ARCserve Backup installation media.
- If you determine that Microsoft SQL Server 2008 Express Edition does not meet the needs of your CA ARCserve Backup environment, you can use the Server Configuration Wizard to convert the CA 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 CA ARCserve Backup.

  Note: For information about upgrading from Microsoft SQL Server 2008 Express Edition to Microsoft SQL Server, see the *Administration Guide*.
- CA 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 CA ARCserve Backup database.
- For Global Dashboard, you cannot configure the CA 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 CA support web site can help you determine the applicable updates for your implementation.

  Important! You should always check the Compatibility Matrix on the CA support website before you apply Microsoft SQL Server 2008 Express Edition service packs to your CA 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 CA ARCserve Backup database. The name of the CA ARCserve Backup database instance is ARCSERVE_DB (default). This scenario also includes situations where a previous release of CA 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 CA ARCserve Backup database. The name of the CA ARCserve Backup database instance is not ARCSERVE_DB.

  When you upgrade to this release, Setup searches for the default CA ARCserve Backup database instance. If Setup detects an instance named ARCSERVE_DB, Setup upgrades the instance to Microsoft SQL Server 2008 Express Edition, and CA 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 CA 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 CA ARCserve Backup database:

- If you are upgrading to this release and currently running Microsoft SQL Server for the CA ARCserve Backup database, you must continue using Microsoft SQL Server for the CA ARCserve Backup database.
- CA ARCserve Backup does not support using Microsoft SQL Server 7.0 for the CA ARCserve Backup database.
- By default, CA ARCserve Backup creates the CA 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 CA ARCserve Backup database to run locally or remotely to your CA ARCserve Backup server.

  Note: For more information, see Remote Database Considerations.
- By default, CA 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 CA 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 CA 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 CA ARCserve Backup primary server.

- To install CA 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 CA ARCserve Backup Database (SQL) System Account during installation of CA 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, or Microsoft SQL Server 2008 as the CA 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 CA 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 CA ARCserve Backup Database Engine, as follows:

  HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\Base\Database\MSSQL\SQLLoginTimeout

- CA ARCserve Backup does not support local Microsoft SQL Server installations on CA ARCserve Backup servers in NEC CLUSTERPRO environments. In NEC CLUSTERPRO environments, you must install the CA 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 CA 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 CA ARCserve Backup server in your environment.
- To ensure that CA 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 72).

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, Microsoft SQL Server 2005, or Microsoft SQL Server 2008, and the CA 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 ensure that the installation wizard can communicate with the remote system, you should enable TCP/IP communication between the CA ARCserve Backup server and the server that will host the CA ARCserve Backup database before you install CA 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 Microsoft SQL Server 2008--**To enable TCP/IP communication on Microsoft SQL Server 2005 and Microsoft SQL Server 2008 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.

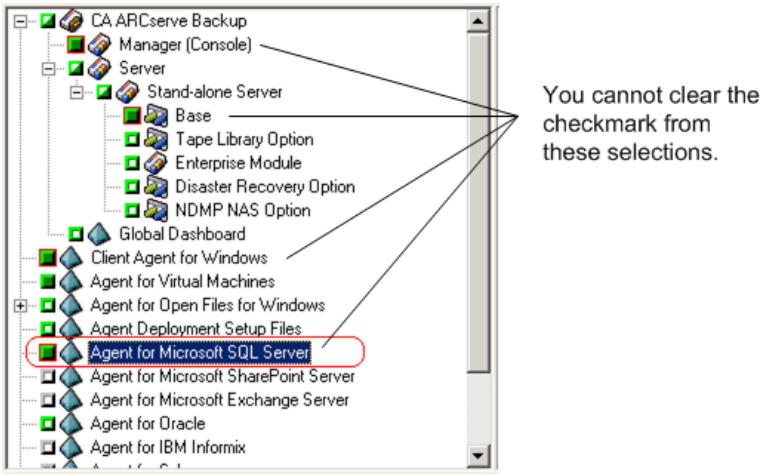
Agent for ARCserve Database

The CA ARCserve Backup Agent for ARCserve Database is a form of the CA ARCserve Backup Agent for Microsoft SQL Server. The agent is either installed automatically when you install CA ARCserve Backup, or manually using a special utility, either after the location of the CA 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 CA ARCserve Backup home directory, in a folder named ASDBSQLAgent, when you install CA ARCserve Backup. If you need to install the agent on a computer that is not a CA 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 CA ARCserve Backup database, and the system databases and Disaster Recovery Elements from the Microsoft SQL Server instance that contains the CA 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 CA ARCserve Backup database, and to work with CA ARCserve Backup to provide the special recovery mechanisms that are available for the CA ARCserve Backup database.

When upgrading from a previous release of CA ARCserve Backup, you must upgrade the Agent for ARCserve Database. This behavior is designed to help ensure that the current version of the CA 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 as illustrated by the following:



Because the Agent for ARCserve Database is a form of the Agent for Microsoft SQL Server, it will appear as the CA 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 CA 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 CA ARCserve Backup installer is unable to do so directly

Installation Progress Logs

After you install CA ARCserve Backup and any agents and options, CA 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 CA Customer Support personnel if you need to contact us about an installation problem.

- **Interactive installations--**If installation of the CA 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, CA 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 CA ARCserve Backup.

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

    For example, ARCSERVE.log is the log file created when you installed the CA 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 CA ARCserve Backup base product includes support for Global Dashboard operations.

Configuration of Global Dashboard can be performed during or after installation of CA 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. 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 CA ARCserve Backup domain (not a domain member server).

- During the configuration process, the CA 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 CA 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 CA 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 CA ARCserve Backup.

This section contains the following topics:

Supported Upgrades (see page 77)
Backward Compatibility (see page 78)
Manager Console Support for Previous Releases (see page 79)
Global Dashboard Upgrades (see page 79)
Data Migration from a Previous Release (see page 80)

Supported Upgrades

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

- CA ARCserve Backup r12.5 for Windows --includes the General Availability (GA) release and all of the latest service packs.
- CA ARCserve Backup r12 for Windows --includes the GA release and all of the latest service packs.
- BrightStor ARCserve Backup r11.5 for Windows--includes the GA release and all of the latest service packs.
- BrightStor ARCserve Backup r11.1 for Windows--includes the GA release and all of the latest service packs.

  Note: CA ARCserve Backup does not support upgrading BrightStor ARCserve Backup r11.1 for Windows in a cluster-aware environment to this release. To upgrade to this release, you must uninstall BrightStor ARCserve Backup r11.1 for Windows and then install this release into a cluster-aware environment.

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

Backward Compatibility

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

- **Agents--**Using the CA ARCserve Backup r15 server component you can manage agents from the releases that follow:
  - CA ARCserve Backup r12.5--includes the General Availability (GA) release and the latest service packs.
  - CA ARCserve Backup r12--includes the GA release and the latest service packs.
  - BrightStor ARCserve Backup r11.5--includes the GA release and the latest service packs.

  Be aware of the following:
  - When backing up agent computers, the version of the CA 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 CA ARCserve Backup with any previous release of the CA ARCserve Backup server component.
  - For optimal performance, you should upgrade all CA ARCserve Backup agents and options installed in your backup environment to this release.
  - All CA ARCserve Backup products installed on a computer must be the same release.

    Example: The CA 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 CA 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.
- **Manager Console--**You must retain the previous manager interface to access and manage CA ARCserve Backup servers running the releases that follow:
  - CA ARCserve Backup r12.5
  - CA ARCserve Backup r12
  - BrightStor ARCserve Backup r11.5
  - BrightStor ARCserve Backup r11.1

  Note: For more information, see Manager Console Support for Previous Releases (see page 79).
- **CA ARCserve Backup Domains--**All CA ARCserve Backup servers in a domain must be running the same version of the CA ARCserve Backup Server component. CA ARCserve Backup servers with different versions of the CA ARCserve Backup server component must reside in different CA 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.

Manager Console Support for Previous Releases

To manage other CA ARCserve Backup servers in your environment that are running older releases of CA ARCserve Backup, (for example, BrightStor ARCserve Backup r11.5 and BrightStor ARCserve Backup r11.1) you must keep the current Manager Console.

When you upgrade from a previous release, the installation wizard presents you with the following Manager Console installation options:

Note: The Manager Console Options dialog will not appear when you upgrade from CA ARCserve Backup r12, CA ARCserve Backup r12 SP1, and CA ARCserve Backup r12.5 to this release.

- **Remove the Current Manager Console--**Requires you to upgrade all CA ARCserve Backup servers in your environment to this release.

  When you choose this option, Setup installs Manager Console into the following directory.

  <ARCserve_HOME>\CA\ARCserve Backup\ARCserveMgr.exe

- **Keep the Current Manager Console--**Lets you keep the current Manager Console so that you can manage CA ARCserve Backup servers running an older release. For example:

  - BrightStor ARCserve Backup r11.5
  - BrightStor ARCserve Backup r11.1

  To accommodate the files to support both versions of the Manager Console, Setup prompts you to specify an alternate path for the new CA ARCserve Backup installation directory, and does not uninstall the following directory from your system:

  <ARCserve_HOME>\CA\ARCserve Backup\ARCserveMgr.exe

  Important! CA ARCserve Backup does not support retaining the Manager Console from the previous release when you are performing a remote upgrade and a silent upgrade using a response file.

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

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

Authentication

The upgrade process migrates all CA 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, CA 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

CA 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 CA 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 CA 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 CA 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 CA 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 CA software. To simplify the process, you can obtain your current ca.olf file by going to ca.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 CA 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.

CA 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 CA ARCserve Backup, and the release level of each agent:

File System Agent	Release Level
CA ARCserve Backup Client Agent for UNIX	r15
CA ARCserve Backup Client Agent for Linux	r15
CA ARCserve Backup Client Agent for Mainframe Linux OS/390	r15
CA ARCserve Backup Client Agent for Windows	r15
BrightStor ARCserve Backup Client Agent for NetWare	r11.1 SP3
CA ARCserve Backup Client Agent for Mac OS X (Supported on Windows Only)	r15
BrightStor ARCserve Backup Client Agent for OpenVMS (Supported on Windows Only)	r11.5 SP3
CA ARCserve Backup Agent for Oracle (UNIX)	r15
CA ARCserve Backup Agent for Oracle (Linux)	r15
BrightStor ARCserve Backup Enterprise Option for AS400	r11.5 SP3

Chapter 4: Installing and Upgrading CA ARCserve Backup

This section contains the following topics:

How to Complete Prerequisite Tasks (see page 83)
Install CA ARCserve Backup (see page 88)
Upgrade CA ARCserve Backup from a Previous Release (see page 97)
Create a Silent Installation Response File (see page 105)
CA ARCserve Backup Agent Deployment (see page 111)
Upgrade CA ARCserve Backup Agents Silently to the Current Release (see page 123)
How to Install CA ARCserve Backup Using Unicenter Software Delivery (see page 126)
Post-Installation Tasks (see page 133)

How to Complete Prerequisite Tasks

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

Installation and System Requirements

Review the CA ARCserve Backup readme file. The readme file contains the operating system requirements, hardware and software prerequisites, last-minute changes, and known issues with CA 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 CA ARCserve Backup and identify the following:

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

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

  Note: For more information, see Types of CA ARCserve Backup Server Installations (see page 62).
- If you are installing CA ARCserve Backup, agents, and options on remote systems, you must specify the host names of the target systems. CA ARCserve Backup does not support specifying IP addresses when you are performing a remote installation or upgrade.

CA ARCserve Backup Database

Determine the database application that you will use for your CA ARCserve Backup installation. For more information, see Database Requirements (see page 67).

Administrative Privileges

Ensure that you have administrator privileges or the proper authority to install software on the servers where you are installing CA 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 76).

Primary Server Installations

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

Note: To install a CA 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 CA ARCserve Backup authentication credentials to allow the member servers to join the primary servers' domain (for example, *caroot* and the CA ARCserve Backup password that you specified when you installed the primary server). The process of allowing a member server to join a CA 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 CA 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

- CA 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.

- CA 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).
- Not applicable for any Windows IA64 platforms.
- Sufficient CA 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 27).

Branch Primary Servers

- CA ARCserve Backup (Primary or Stand-alone server) installed.
- CA ARCserve Backup database must have Microsoft SQL Server 2000 or later installed or SQL Server Express 2008 or later installed.

Global Dashboard Console

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

  Be aware of the following:

  - You can install the Global Dashboard Console on member servers; however, member servers cannot function as Branch Primary Servers.
  - Not applicable for Windows 2000 and any Windows IA64 platforms.

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 CA ARCserve Backup. For more information, see Primary Server and Member Server Communication Ports (see page 243).

Cluster Installations

When you install CA 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: CA 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 CA 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 CA ARCserve Backup primary servers and member servers, and the SAN. CA ARCserve Backup detects and configures libraries that are connected directly to the CA 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 CA 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 CA 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 CA ARCserve Backup server has a SCSI/Fibre controller or adapter supported by both Windows and CA ARCserve Backup. CA ARCserve Backup can support most installed SCSI controllers.

Note: To ensure that your hardware devices are compatible and that CA ARCserve Backup can communicate with your system, you can get the latest Certified Device List from ca.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 CA ARCserve Backup server component and the CA 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 CA 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 CA ARCserve Backup primary server on the system that is functioning as the SAN primary and you must install the CA ARCserve Backup Member Server on the systems that are functioning as SAN distributed servers.

Antivirus

If you are installing CA ARCserve Backup database backup agents on a system where you are running CA Antivirus, you must apply the following driver update to both the CA 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 CA 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 CA ARCserve Backup installation media available to you while you run the installation wizard.

Install CA ARCserve Backup

You can install CA ARCserve Backup on a local or remote system using the installation wizard.

To install CA ARCserve Backup

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

   Note: If the CA 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 CA 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 CA ARCserve Backup Prerequisite Components installed on the target computer.
   - You must restart your computer and repeat the above steps if Setup installs Microsoft SQL Server 2008 Express Edition.

     Note: If you are installing CA 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 CA ARCserve Backup.

   Select Install/Upgrade Type dialog

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

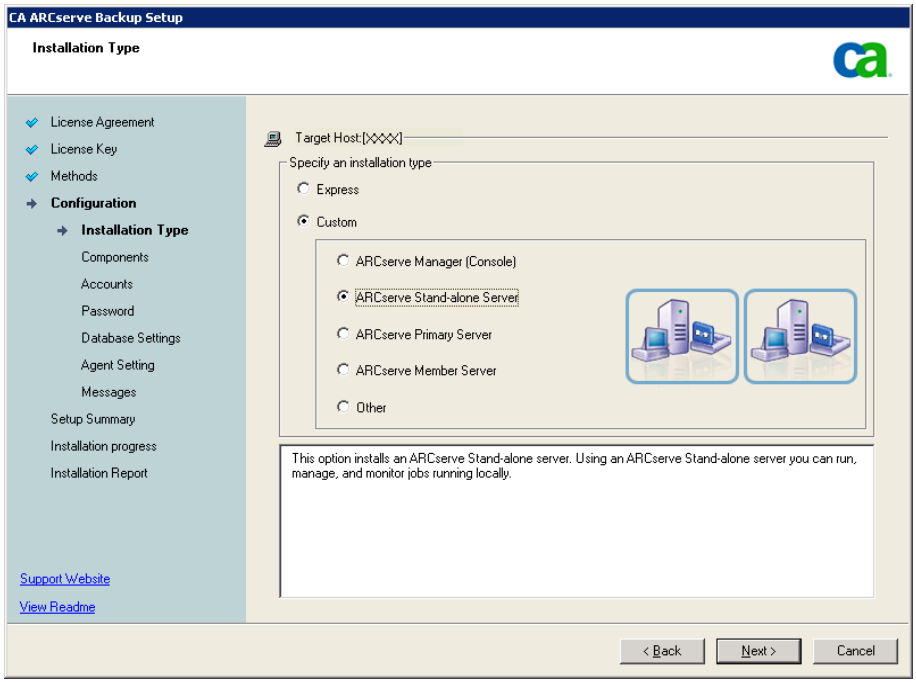
   With remote installations, the target remote systems can consist of different ARCserve server types, different CA ARCserve Backup agents and options, or both.

   Note: The setup program for cluster machines does not support remote installation of the CA ARCserve Backup base product or the CA ARCserve Backup agents. This remote install limitation for the CA 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 CA ARCserve Backup agents using the physical hosts of clusters is supported.

Installation Type dialog

Lets you specify the type of CA 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 CA ARCserve Backup Server Installations (see page 62) and CA ARCserve Backup Server Options (see page 66).



Components dialog

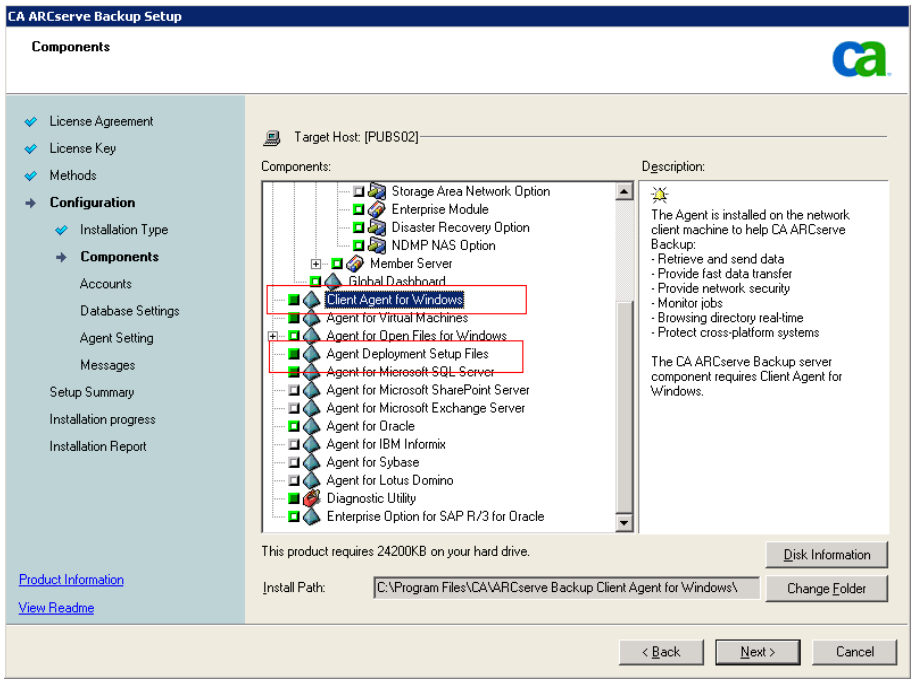
Lets you specify the CA ARCserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the CA ARCserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the CA 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 CA 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 CA 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 CA ARCserve Backup agents on multiple remote systems, after you install CA ARCserve Backup. To support this capability, Setup must copy Setup source files to the CA ARCserve Backup server. To copy the contents of the installation media to the CA 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 CA ARCserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA 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*.

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

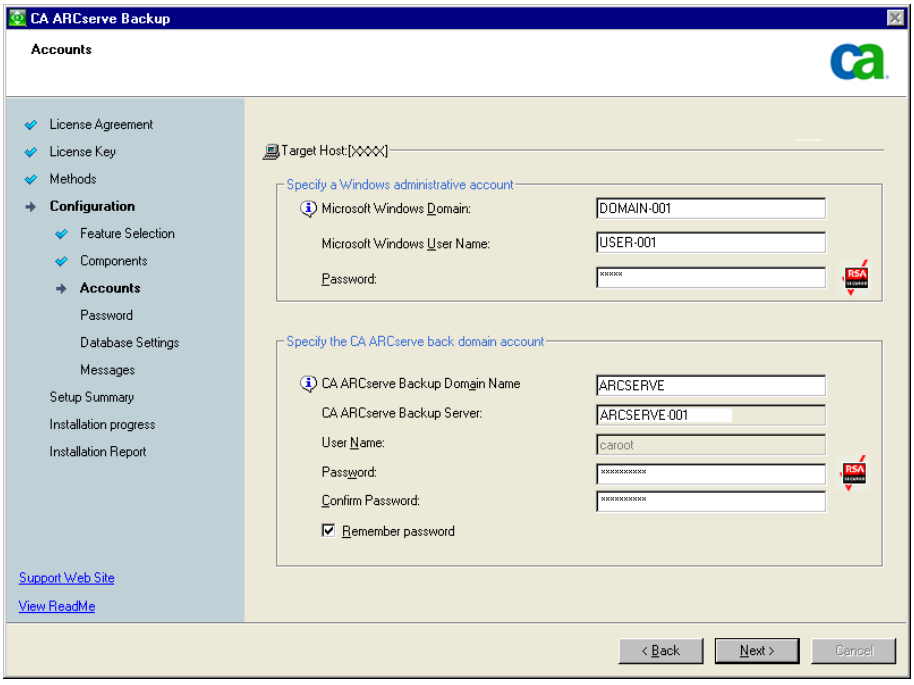


Accounts dialog

Lets you set up your CA ARCserve Backup accounts.

If Setup detects a cluster-aware application running in your environment, and you want to install CA 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 CA ARCserve Backup.

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

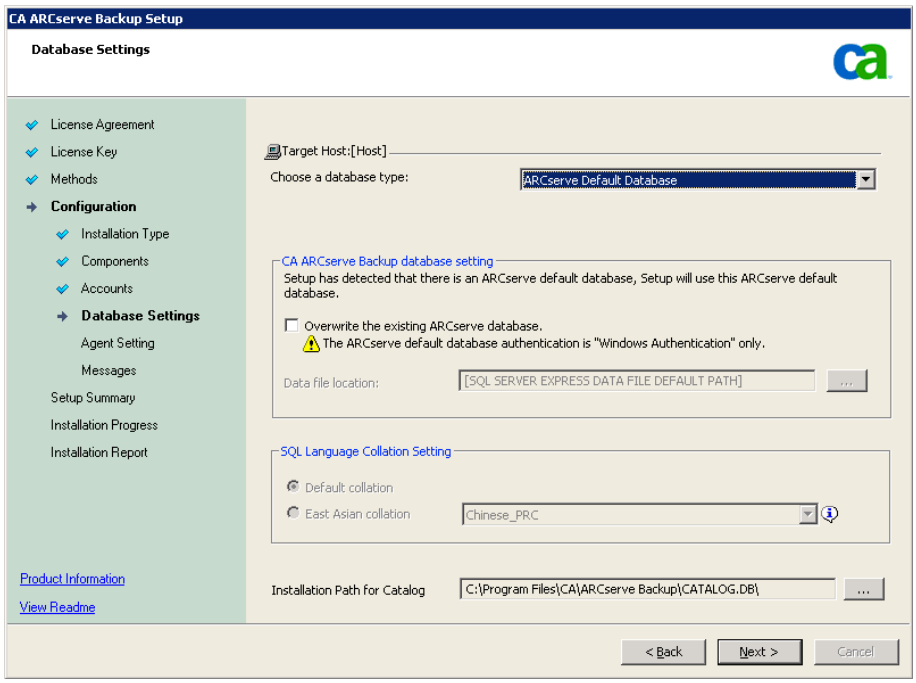


Database Settings dialog

Lets you configure the CA 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.

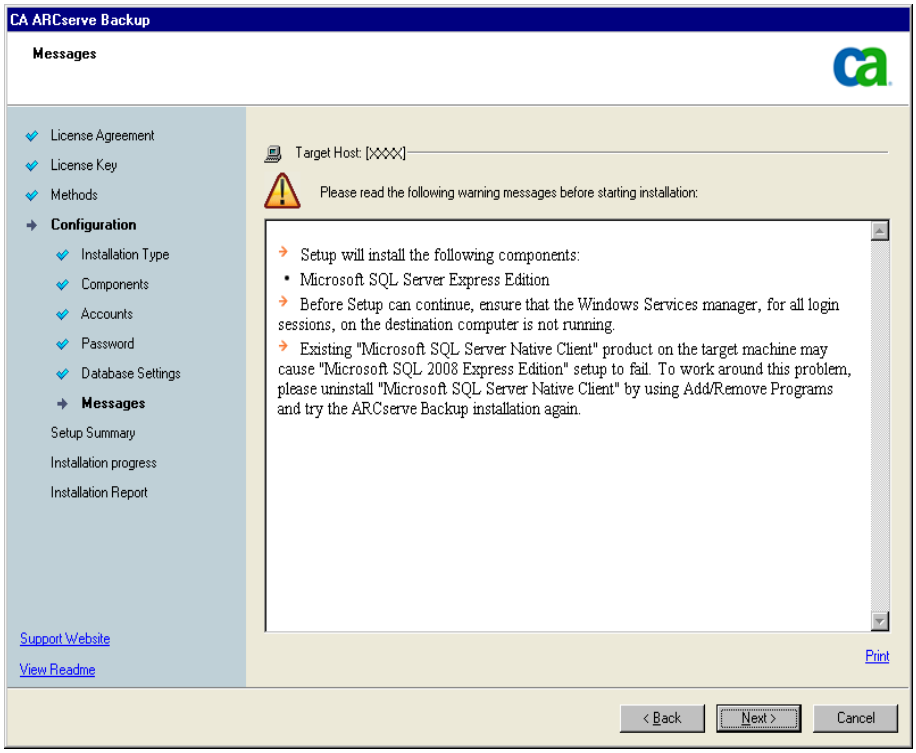
Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that CA ARCserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



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:



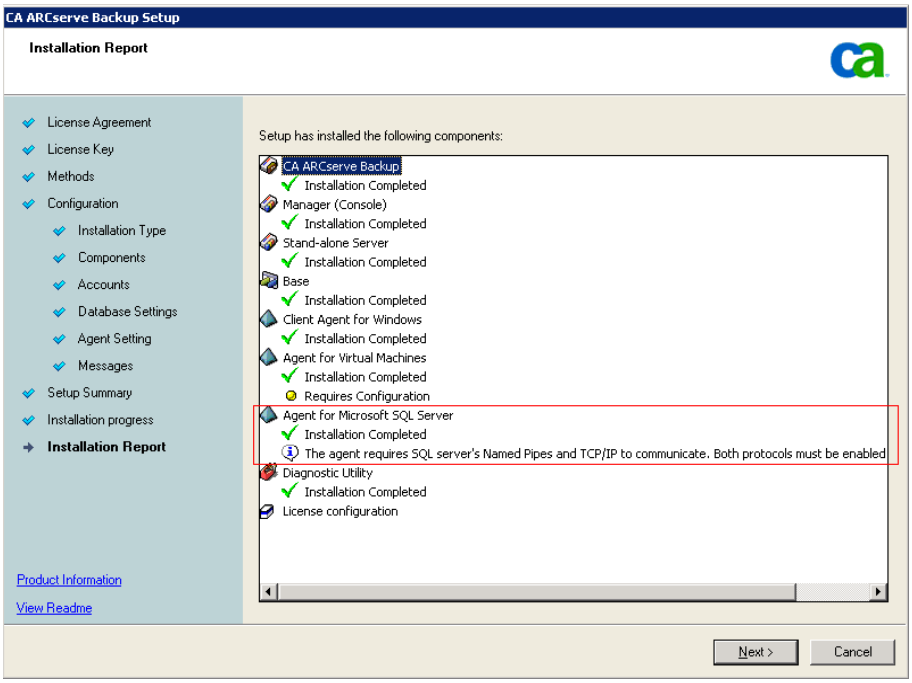
Setup Summary dialog

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 CA 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 CA ARCserve Backup from a Previous Release

To upgrade an installation means to reinstall features or components to higher release or build numbers 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 database to the new ARCserve database.

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

- CA ARCserve Backup r12.5 for Windows --includes the General Availability (GA) release and all of the latest service packs.
- CA ARCserve Backup r12 for Windows --includes the GA release and all of the latest service packs.

- BrightStor ARCserve Backup r11.5 for Windows--includes the GA release and all of the latest service packs.
- BrightStor ARCserve Backup r11.1 for Windows--includes the GA release and all of the latest service packs.

  Note: CA ARCserve Backup does not support upgrading BrightStor ARCserve Backup r11.1 for Windows in a cluster-aware environment to this release. To upgrade to this release, you must uninstall BrightStor ARCserve Backup r11.1 for Windows and then install this release into a cluster-aware environment.

Important! If you wish to upgrade from BrightStor ARCserve Backup v9 and BrightStor Enterprise Backup v10.5, you must uninstall the previous release and then install this release of CA ARCserve Backup. However, if you wish to retain the database information from your previous implementation, you must upgrade BrightStor ARCserve Backup v9 or BrightStor Enterprise Backup v10.5 to CA ARCserve Backup r12.5 GA Build (with no SP), and then upgrade from CA ARCserve Backup r12.5 to this release. To obtain CA ARCserve Backup r12.5 installation media, contact CA Support. For all other previous releases of BrightStor ARCserve Backup 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 76).

To upgrade CA ARCserve Backup from a previous release

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

   Note: If the CA 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 CA 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 CA 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 CA ARCserve Backup from a previous release.

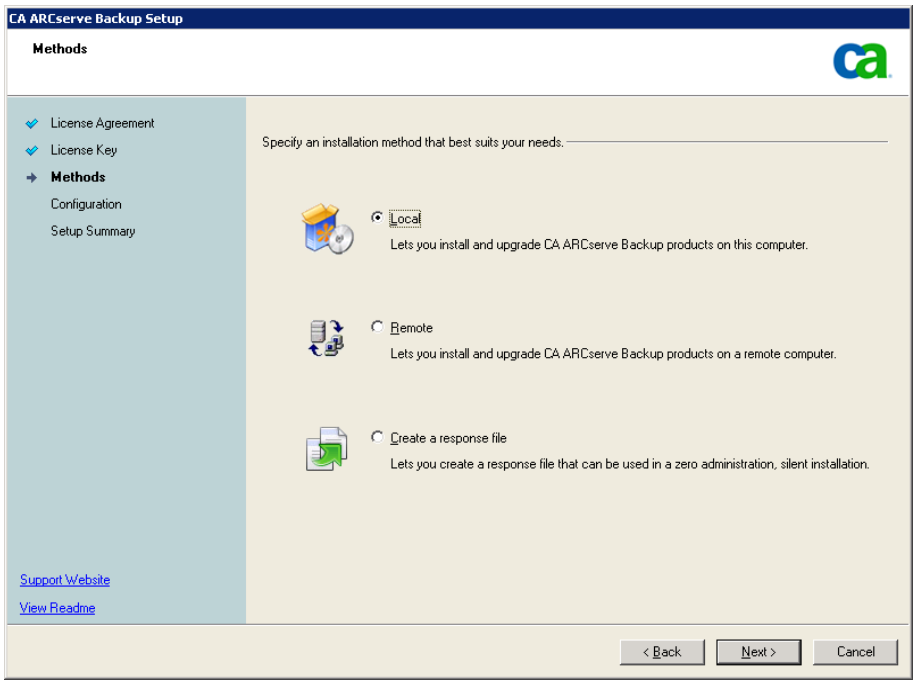
Methods dialog

If you are upgrading from a previous release to an ARCserve Primary Server, you must select the Local Installation/Upgrade option. CA 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.
- Upgrade from a previous release on a remote system and retain the previous Manager.
- Silent upgrade from a previous release using a response file and retain the previous Manager.

Note: For more information, see Manager Console Support for Previous Releases (see page 79).

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



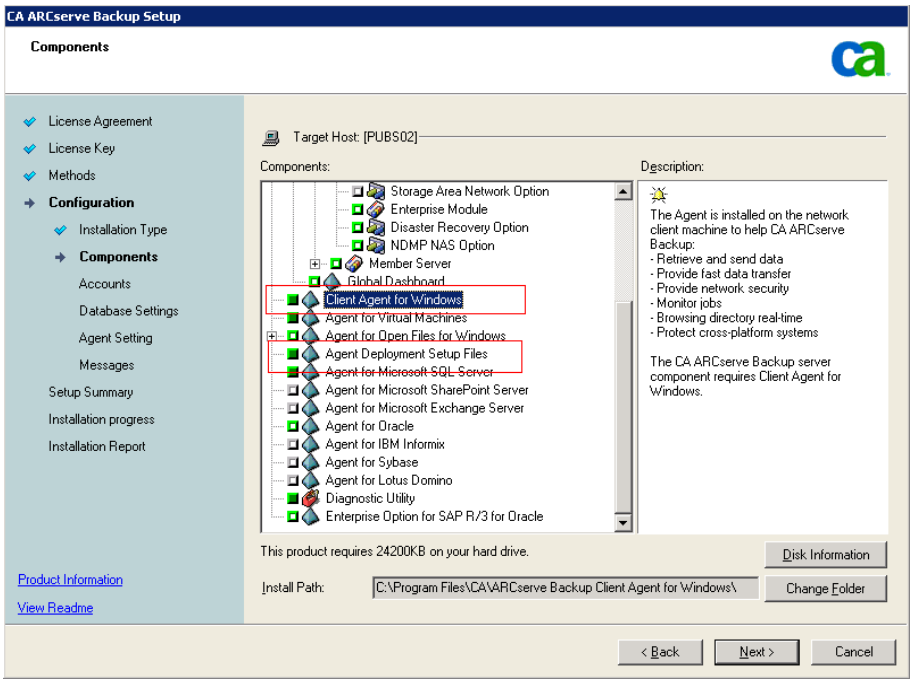
Components dialog

Lets you specify the CA 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 CA ARCserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the CA 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 CA 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 CA 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 CA ARCserve Backup agents on multiple remote systems, after you install CA ARCserve Backup. To support this capability, Setup must copy Setup source files to the CA ARCserve Backup server. To copy the contents of the installation media to the CA 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 CA ARCserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA 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*.

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



Manager Console Options dialog

Select the Keep the current ARCserve Manager Console option only if there are ARCserve servers in your environment that are running a previous release of BrightStor ARCserve Backup. When you select this option, Setup prompts you to install CA ARCserve Backup into an alternate location on your computer.

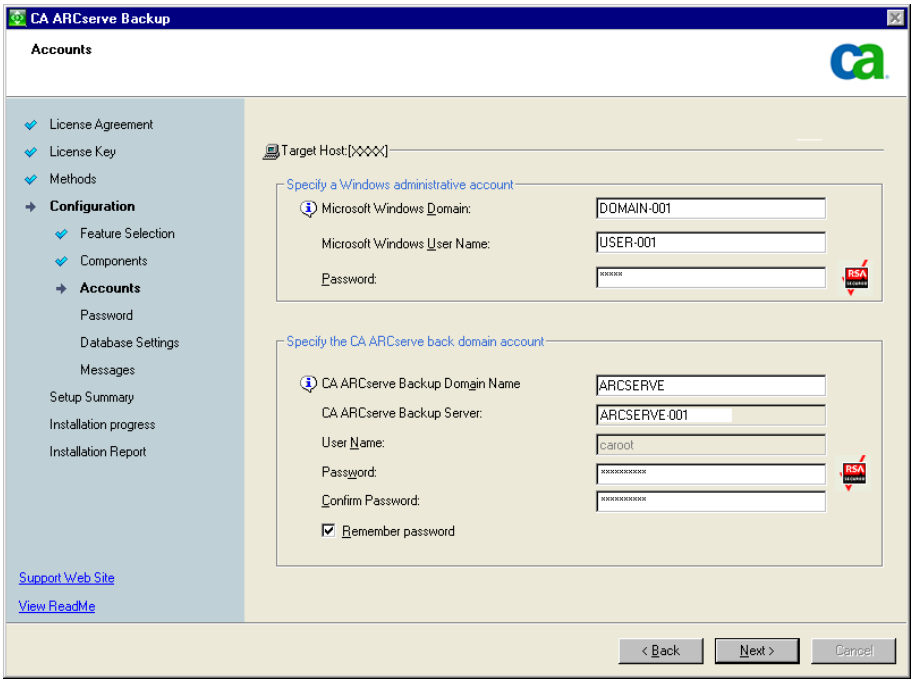
When you specify to install the new Manager Console support files into the same directory where previous manager support files reside, the installation wizard prompts to install the Manager Console support files into an alternate location.

Note: CA ARCserve Backup does not support retaining the Manager console from the previous release when you are performing a remote upgrade and a silent upgrade using a response file.

Accounts dialog

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

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

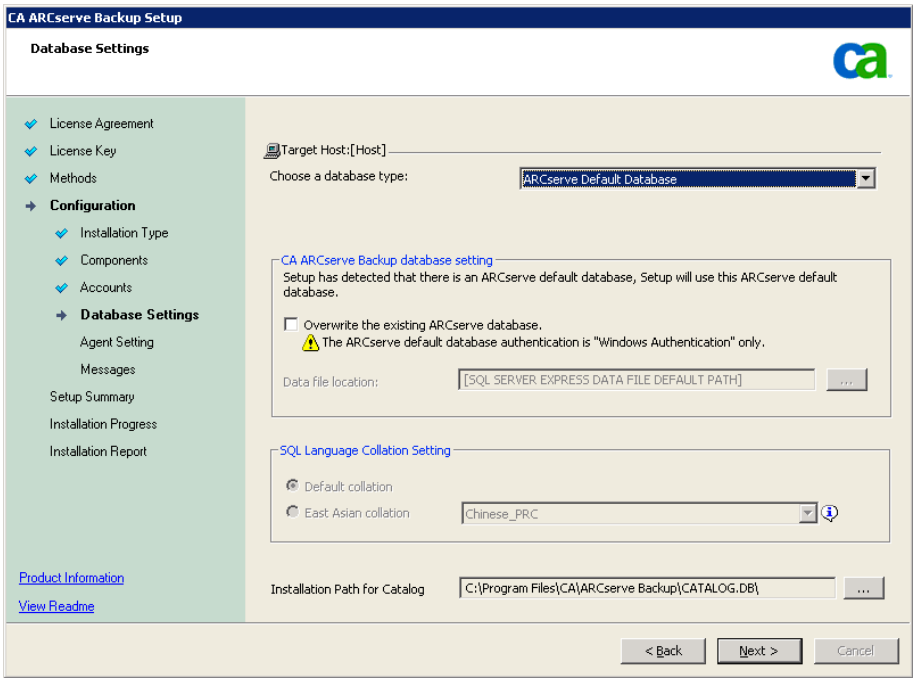


Database Settings dialog

Lets you configure the CA 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 CA 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 CA ARCserve Backup Server Migration dialog.

CA 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 80).

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

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

Be aware of the following limitations and considerations:

- CA ARCserve Backup does not support recovering the CA ARCserve Backup database when the last backup was before you upgraded to this release. As a best practice, you should back up the CA 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 CA ARCserve Backup services start properly in a cluster-aware environment, you must execute the cstop and cstart scripts on the CA ARCserve Backup server before you open the CA ARCserve Backup Manager Console. You must complete this task when you upgrade from CA ARCserve Backup r12 (includes the GA release and the latest service packs) to this release.

Create a Silent Installation Response File

During an interactive installation, many CA 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.

Note: CA ARCserve Backup does not support creating a silent installation response file for CA ARCserve Backup Primary Server installations. You can create a silent installation response file for CA ARCserve Backup Stand-alone Server and CA ARCserve Backup Member Server installations.

To create a silent installation response file

1. Insert the CA 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 CA ARCserve Backup dialog.

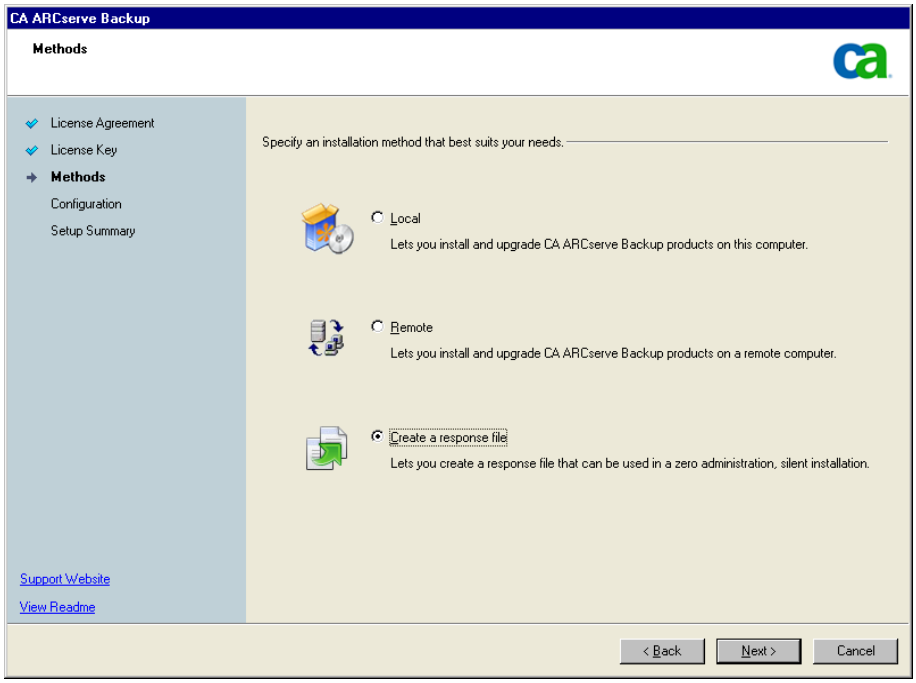
2. On the License Agreement dialog, accept the terms of the Licensing Agreement and complete the fields on the Customer and Information dialog.

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

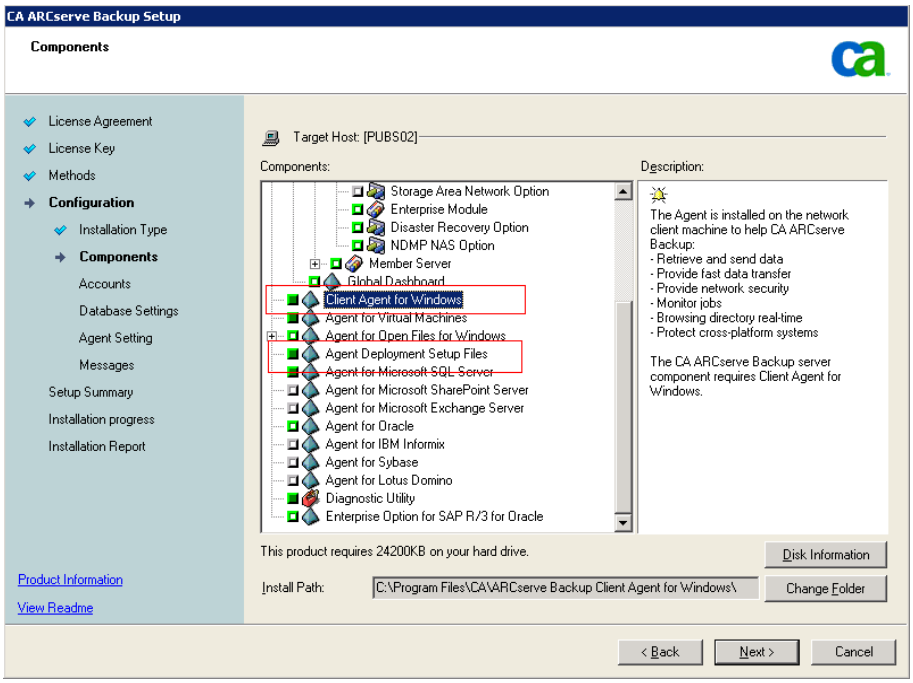
Lets you specify the CA ARCserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the CA ARCserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the CA 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 CA 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 CA ARCserve Backup server that you want to install, and check the check boxes corresponding to the components that you want to install.

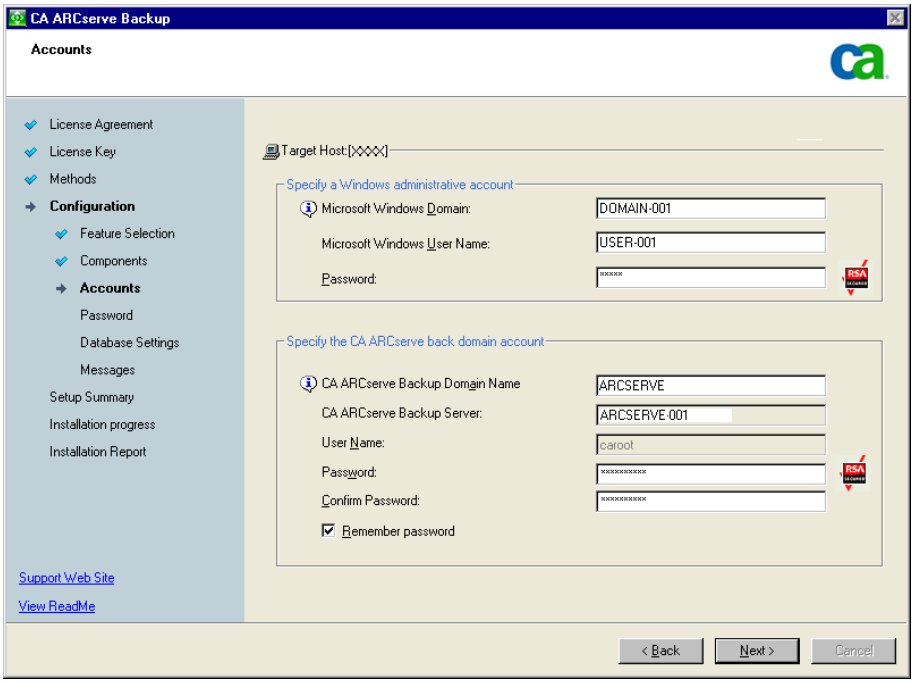
- Agent Deployment is a wizard-like application that lets you install or upgrade CA ARCserve Backup agents on multiple remote systems, after you install CA ARCserve Backup. To support this capability, Setup must copy Setup source files to the CA ARCserve Backup server. To copy the contents of the installation media to the CA 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 CA ARCserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA 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*.

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



Accounts dialog

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

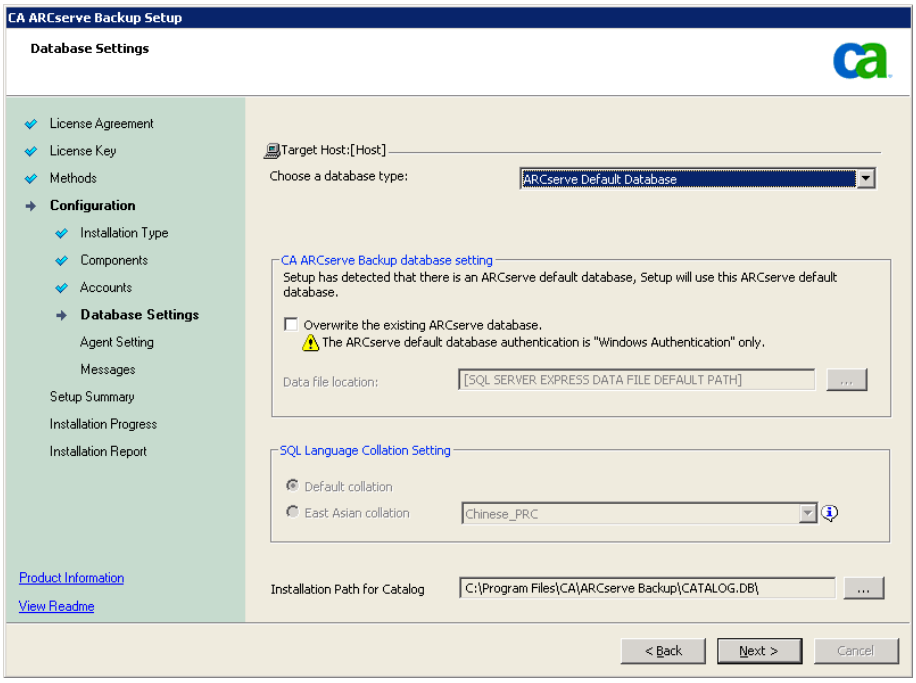


Note: If you do not retain the domain name from your previous installation, CA ARCserve Backup changes your previous caroot password to a blank password. You can change the blank password after the installation is complete.

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 CA 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 CA ARCserve Backup components that you selected.

   By default, CA ARCserve Backup saves the response file in the directory that follows.

   C:\My 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 CA ARCserve Backup, see Upgrade CA ARCserve Backup Agents Silently to the Current Release (see page 123).

CA ARCserve Backup Agent Deployment

CA ARCserve Backup Agent Deployment is a wizard-like application that lets you install and upgrade a collection of CA ARCserve Backup agents on multiple remote hosts simultaneously. Agent Deployment was designed to help you ensure that you are running the most current version of a select group of CA ARCserve Backup agents in your backup environment.

Agent Deployment requires installation files that you can install on the CA ARCserve Backup server. This eliminates the need to provide the CA ARCserve Backup installation media when you run Agent Deployment. However, Agent Deployment requires approximately 1.3 GB of hard disk space, and can significantly increase the length of time required to install CA ARCserve Backup. To eliminate the need to provide the installation media, you must explicitly select Agent Deployment Setup Files when you install CA ARCserve Backup.

The list that follows describes the methods that you can use to deploy agents on remote hosts:

- **Automatic upgrade--**Lets you upgrade agents on remote hosts that previously communicated with the CA ARCserve Backup server. Agent Deployment automatically detects the agents running on remote hosts that are registered to the CA ARCserve Backup server and lets you upgrade the agents to this release. This method ensures that all agents running in your CA ARCserve Backup environment are the same release as the CA ARCserve Backup server.

  Note: Using Automatic upgrade you cannot manually specify remote agent host names.

  Using this method, you can deploy the agents and components that follow:

  - CA ARCserve Backup Agent for Microsoft Exchange Server
  - CA ARCserve Backup Agent for Microsoft SQL Server
  - CA ARCserve Backup Agent for Microsoft SharePoint Server
  - CA ARCserve Backup Agent for Open Files
  - CA ARCserve Backup Agent for Oracle
  - CA ARCserve Backup Agent for Virtual Machines
  - CA ARCserve Backup Client Agent for Windows
  - CA ARCserve Backup Diagnostic Utilities

  Note: For information about how to deploy agents to remote hosts using Automatic upgrade see Deploy Agents to Remote Hosts Using Automatic Upgrade (see page 114).

- **Custom deployment--**Lets you install agents and upgrade agents on any remote host. Hosts of this type may or may not have a previous version of an agent installed.

  Using this method, you can deploy the agents and components that follow:

  - CA ARCserve Backup Agent for Microsoft Exchange Server
  - CA ARCserve Backup Agent for Open Files
  - CA ARCserve Backup Agent for Virtual Machines
  - CA ARCserve Backup Client Agent for Windows
  - CA ARCserve Backup Diagnostic Utilities

  Note: For information about how to deploy agents to remote hosts using Custom deployment, see Deploy Agents to Remote Hosts Using Custom Deployment (see page 116).

- **Virtual Machine deployment--**Lets you install agents and upgrade agents on any VM. The target VMs may or may not have a previous version of an agent installed.

  Using this method you can deploy the agents and components that follow:

  - CA ARCserve Backup Agent for Open Files
  - CA ARCserve Backup Agent for Virtual Machines
  - CA ARCserve Backup Client Agent for Windows
  - CA ARCserve Backup Diagnostic Utilities

  Note: For information about how to deploy agents to remote hosts using Custom installation, see Deploy Agents to VMs Using Virtual Machine Deployment (see page 120).

Review the considerations that follow before you use Agent Deployment:

- Agent Deployment lets you deploy the CA ARCserve Backup products that follow:

  - CA ARCserve Backup Agent for Microsoft Exchange Server
  - CA ARCserve Backup Agent for Microsoft SQL Server
  - CA ARCserve Backup Agent for Microsoft SharePoint Server
  - CA ARCserve Backup Agent for Open Files
  - CA ARCserve Backup Agent for Oracle
  - CA ARCserve Backup Agent for Virtual Machines
  - CA ARCserve Backup Client Agent for Windows
  - CA ARCserve Backup Diagnostic Utilities

  Note: If Agent Deployment detects an agent on the remote host that not listed above, Agent Deployment terminates.

- You should not use Agent Deployment to install the Agent for Microsoft Exchange Server on Exchange Client Access Servers and Hub Transport Servers.
- Agent Deployment requires you to specify the host names of the target systems. CA ARCserve Backup does not support specifying IP addresses when you are deploying agents to remote systems.
- Agent Deployment installs the agents into their default installation path. For example, Agent Deployment installs or upgrades the Client Agent for Windows in the path that follows (x86 systems):

  C:\Program Files\CA\ARCserve Backup Client Agent for Windows

- You must log in to your computer with an administrative account or an account with administrative privileges to deploy agents to remote hosts.
- You should ensure that the administrative share on the remote hosts (for example, C$, Admin$, and so on) is accessible from the server that pushes the agents.
- You should ensure that the firewall exception rule for File and Printing Service on the remote hosts is enabled. You must complete this task 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, you should use Domain level group policy to enable an exception to File and Print Sharing communication on all servers in your backup environment.
- You must disable simple file sharing on Windows XP systems to ensure that you can successfully install agents on remote hosts. Use the steps that follow to disable simple file sharing on remote hosts:

  1. Log in to the remote Windows XP host system.

     Double-click My Computer on the desktop.

     My Computer opens.

  2. Click Folder Options on the Tools menu.

     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.

Deploy Agents to Remote Hosts Using Automatic Upgrade

CA ARCserve Backup Agent Deployment lets you install and upgrade CA ARCserve Backup agents on remote hosts. Automatic upgrade lets you deploy agents to detected hosts with agents that require an upgrade to this release. This method helps to ensure that all agents running in your CA ARCserve Backup environment are the same release number as the CA ARCserve Backup server.

The automatic upgrade method must detect an agent from a previous release installed on the target host to upgrade the agent to this release. If the automatic upgrade method does not detect an agent from a previous release installed on the target system, you must use the Custom deployment method to install the agents on the target system.

To deploy CA ARCserve Backup agents to remote hosts using Automatic upgrade

1. Open the CA ARCserve Backup Manager Console.

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

   CA ARCserve Backup Agent Deployment starts and the Login Server dialog opens.

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

   The Methods dialogs opens.

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

   The Components dialog opens displays a list of hosts detected by Agent Deployment that are running CA ARCserve Backup agents from a previous release.

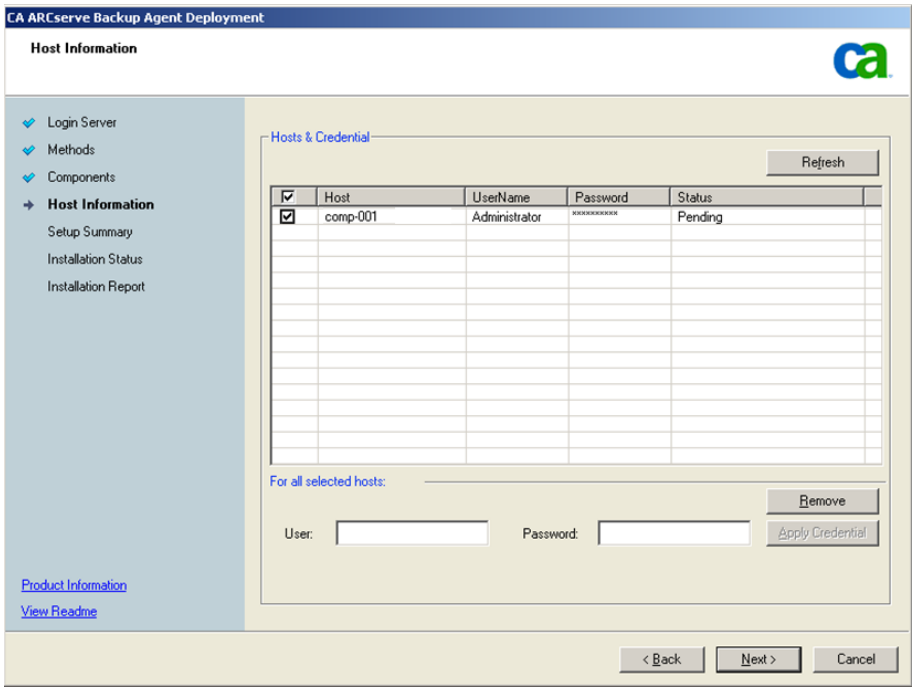
4. Click Next.

   The Host Information dialog opens and populates the Hosts and Credentials list with the host names, user names, and passwords for the detected hosts.

5. Specify the User Name and Password for the hosts by doing the following:

   a. Specify the user name in the User field (<domain>\<user name>) and specify the password in the Password field.

   b. Ensure that the check box next to the target host is checked. To specify all hosts, click the Select all check box.



   c. Click Apply Credentials.

   The user name and the password are applied to all remote hosts in the list.

   Note: To remove a host from the Host and Credentials list, place a check mark in the check box next to the host that you want to remove and click Remove.

   Click Next to continue.

   Agent Deployment validates the host name, user name, and password specified for all specified hosts. If Agent Deployment does not detect an authentication error, pending appears in the Status field. If Agent Deployment detects an authentication error, Failed appears in the Status field. Click Failed to discover the reason for the error. You must correct all Failed messages continue.

   Click Next.

6. After the Status field for all remote hosts displays Verified, click Next.

   The Setup Summary dialog opens.

7. From the Setup Summary dialog, verify the components and the host names specified.

   Click Next.

   The Installation Status dialog opens.

8. From the Installation Status dialog, click Install.

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

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

   Click Next.

9. From 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 hosts now.

   Click Restart.

   Agent Deployment restarts all remote hosts now.

   Note: If you want to create a list of remote hosts that require a restart, click Export Restart Report.

10. After the Status field for all remote hosts displays complete, click Finish.

The CA ARCserve Backup agents are deployed on the remote hosts.

More information:

CA ARCserve Backup Agent Deployment (see page 111)
Deploy Agents to Remote Hosts Using Custom Deployment (see page 116)

Deploy Agents to Remote Hosts Using Custom Deployment

CA ARCserve Backup Agent Deployment lets you install and upgrade CA ARCserve Backup agents on remote hosts. Custom deployment lets you specify the agents that you want to install and upgrade on remote hosts. This method helps to ensure that all agents running in your CA ARCserve Backup environment are the same release number as the CA ARCserve Backup server.

To deploy CA ARCserve Backup agents to remote hosts using Custom deployment

1. Open the CA ARCserve Backup Manager Console.

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

   CA ARCserve Backup Agent Deployment starts and the Login Server dialog opens.

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

   The Methods dialogs opens.

3. From the Methods dialog, click Custom installation and click Next.

   The Components dialog opens.

4. From the Components dialog, select the agents that you want to install on all remote hosts and click Next.

   The Host Information dialog opens.

5. Specify the names of remote hosts by doing one of the following:

   - Click Import to import a list of remote hosts 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 hosts must be less than or equal to 1000.

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

   - 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 hosts. To deploy agents to more than 1000 remote hosts, you can restart Agent Deployment and repeat this task, or, run Agent Deployment from an alternate CA ARCserve Backup primary server or stand-alone server.

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

   a. Click the UserName field (next to the host name) and specify the user name using the following format:

      <domain>\<user name>

   b. Click the Password field and specify the corresponding password.

   c. Repeat this step as required until you specify the user name and password for all remote hosts.

   Optionally, if the user name and password are the same for all remote hosts, specify the user name in the User field (<domain>\<user name>), specify the password in the Password field, ensure that all the check boxes are checked, and then click Apply Credentials.

   The user name and the password are applied to all remote hosts in the list.

   Note: To remove a host from the Host and Credentials list, click the check box next to the host that you want to remove and click Remove.

   Click Next to continue.

   Agent Deployment validates the host name, user name, and password specified for all specified hosts. If Agent Deployment does not detect an authentication error, pending appears in the Status field. If Agent Deployment detects an authentication error, Failed appears in the Status field. Click Failed to discover the reason for the error. You must correct all Failed messages continue.

   Click Next.

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

   The Setup Summary dialog opens.

8. From the Setup Summary dialog, verify the components and the host names specified.

   Click Next.

   The Installation Status dialog opens.

9. From the Installation Status dialog, click Install.

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

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

10. Do one of the following:

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

      The Restart dialog opens to identify the remote hosts that require a restart.

      Click Restart.

      Continue to the next step.

    - If there are no remote hosts that require a restart, click Finish to complete this task.

11. From 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 hosts now.

    Click Restart.

    Agent Deployment restarts all remote hosts now.

    Note: If you want to create a list of remote hosts that require a restart, click Export Restart Report.

12. After the Status field for all remote hosts displays complete, click Finish.

The CA ARCserve Backup agents are deployed on the remote hosts.

More information:

CA ARCserve Backup Agent Deployment (see page 111)
Deploy Agents to Remote Hosts Using Automatic Upgrade (see page 114)

Deploy Agents to VMs Using Virtual Machine Deployment

CA ARCserve Backup Agent Deployment lets you install and upgrade CA ARCserve Backup agents on local or remote VMs. The virtual machine deployment method lets you specify the agents that you want to install and upgrade on local or remote VMs. This method helps to ensure that all agents running on the VMs in your CA ARCserve Backup environment are the same release number as the CA ARCserve Backup server.

Be aware of the considerations that follow:

- 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.

To deploy CA ARCserve Backup agents to VMs using Virtual Machine deployment

1. Open the CA ARCserve Backup Manager Console.

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

   CA ARCserve Backup Agent Deployment starts and the Login Server dialog opens.

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

   The Methods dialogs opens.

3. From the Methods dialog, select Virtual Machine deployment and click Next.

   The Components dialog opens.

4. From the Components dialog, select the agents that you want to install on all remote hosts and click Next.

   The Host Information dialog opens.

5. Specify the names of remote hosts that contain the VMs by doing one of the following:

   - Click Import to import a list of remote hosts 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 hosts must be less than or equal to 1000.

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

   - Click Refresh to import the existing VMs from the CA ARCserve Backup database.

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

   - Specify the remote host name in the Host Name field and click Add.

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

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

   a. Click the UserName field (next to the host name) and specify the user name using the following format:

      <domain>\<user name>

   b. Click the Password field and specify the corresponding password.

   c. Repeat this step as required until you specify the user name and password for all remote hosts.

   Optionally, if the user name and password are the same for all remote hosts, specify the user name in the User field (<domain>\<user name>), specify the password in the Password field, ensure that all the check boxes are checked, and then click Apply Credentials.

   The user name and the password are applied to all remote hosts in the list.

   Note: To remove a host from the Host and Credentials list, click the check box next to the host that you want to remove and click Remove.

   Click Next to continue.

   Agent Deployment validates the host name, user name, and password specified for all specified hosts. If Agent Deployment does not detect an authentication error, pending appears in the Status field. If Agent Deployment detects an authentication error, Failed appears in the Status field. Click Failed to discover the reason for the error. You must correct all Failed messages continue.

   Click Next.

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

   The Setup Summary dialog opens.

8. From the Setup Summary dialog, verify the components and the host names specified.

   Click Next.

   The Installation Status dialog opens.

9. From the Installation Status dialog, click Install.

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

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

10. Do one of the following:

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

      The Restart dialog opens to identify the remote hosts that require a restart.

      Click Restart.

      Continue to the next step.

    - If there are no remote hosts that require a restart, click Finish to complete this task.

11. From 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 hosts now.

    Click Restart.

    Agent Deployment restarts all remote hosts now.

    Note: If you want to create a list of remote hosts that require a restart, click Export Restart Report.

12. After the Status field for all remote hosts displays complete, click Finish.

    The CA ARCserve Backup agents are deployed on the VMs.

Upgrade CA 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 CA 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 CA ARCserve Backup base product and CA ARCserve Backup options.

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

<drive>\Install\mastersetup.exe

To upgrade CA ARCserve Backup agents to the current release

1. Complete the steps described in Upgrade CA ARCserve Backup from a Previous Release (see page 97).
2. Create a response file using the steps described in Create a Silent Installation Response File (see page 105).
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 CA 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
```

How to Install CA ARCserve Backup Using Unicenter Software Delivery

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

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

This section contains the following topics:

Register CA ARCserve Backup on the Unicenter Software Delivery Server (see page 126)
Components and Prerequisites (see page 127)
Install CA ARCserve Backup Components Using Unicenter Software Delivery (see page 132)

Register CA 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 CA 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 CA ARCserve Backup, you must register the software on the Unicenter Software Delivery server. The following procedure describes how to register CA ARCserve Backup on the Unicenter Software Delivery server.

To register CA ARCserve Backup on the Unicenter Software Delivery server

1. Insert the CA 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 CA ARCserve Backup components you can register with Unicenter Software Delivery.

CA ARCserve Backup Client Agents for Windows

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

CA ARCserve Backup Agents

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

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

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

CA ARCserve Backup Options

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

Component	Prerequisites
CA 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 ■ CA ARCserve Installer Assistance Utility
CA ARCserve Backup Agent for Virtual Machines	■ CA ETPKI for Windows ■ Microsoft Installer and Microsoft Visual C++ Redistributable Package ■ CA License ■ CA ARCserve Installer Assistance Utility
CA 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 ■ CA 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 CA ARCserve Backup Components Using Unicenter Software Delivery

To install CA 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 105).

To install CA 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 CA 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 CA ARCserve Backup documentation from the installation media or from the Help menu on the CA 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 CA ARCserve Backup servers in your domain.
- Set up the CA ARCserve Backup Database Protection Job. For more information, see Start the CA ARCserve Backup Database Protection Job (see page 219), or the *Administration Guide*.

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

This section contains the following topics:

Introduction to Cluster-aware Installations (see page 135)
Deployment Considerations (see page 135)
Plan Your CA ARCserve Backup HA Deployment (see page 136)
Deploy CA ARCserve Backup Server on MSCS (see page 138)
Deploy CA ARCserve Backup Server on NEC Cluster (see page 163)
How to Verify a Cluster-aware Installation and Upgrade (see page 198)

Introduction to Cluster-aware Installations

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

- Microsoft Cluster Server (MSCS) in x86/x64/IA64 Windows Server
- NEC CLUSTERPRO/ExpressCluster for Windows 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, and CLUSTERPRO/ExpressCluster X 2.0 for Windows.

Deployment Considerations

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

- **Supported operating systems--**CA ARCserve Backup does not support cluster-aware installations on Windows Server 2008 systems. For more information about supported operating systems, see the CA ARCserve Backup Readme file.
- **Required Cluster Resource Considerations--**As with other cluster-aware applications, the CA 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 CA 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 CA ARCserve Backup deployment.

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

  Note: The setup program for cluster machines does not support remote installation of the CA ARCserve Backup base product or the CA ARCserve Backup agents. This remote install limitation for the CA 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 CA ARCserve Backup agents using the physical hosts of clusters is supported.

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

- **Upgrade Considerations--**To ensure that all CA ARCserve Backup services start properly, you must execute the cstop and cstart scripts after you complete the upgrade process and before you open the CA ARCserve Backup Manager Console. You must perform this task when you upgrade from BrightStor ARCserve Backup r11.5 (includes the GA release and all of the latest service packs), CA ARCserve Backup r12 (includes the GA release and all of the latest service packs), and CA ARCserve Backup r12.5 (includes the GA release and all of the latest service packs) to this release.

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

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

Plan Your CA 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 CA 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 CA ARCserve Backup domain.

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

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

Usually in a central management environment, the CA 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 CA ARCserve Backup base product or the CA ARCserve Backup agents. This remote install limitation for the CA 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 CA ARCserve Backup agents using the physical hosts of clusters is supported.

Which cluster nodes will be deployed as a CA 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 CA 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 CA ARCserve Backup deployment:

- Install CA 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 CA 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 CA ARCserve Backup server failover will not impact a SQL Server.

- Install CA 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 CA ARCserve Backup to share these groups with existing applications by installing CA ARCserve Backup into the shared disk in the same group.

Which CA ARCserve Backup database type to use?

CA 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 (ASDB) is SQLE, the CA 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 CA ARCserve Backup.

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

- Remote Microsoft SQL Server

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

Deploy CA ARCserve Backup Server on MSCS

This section contains the following topics:

MSCS Hardware Requirements (see page 139)
MSCS Software Requirements (see page 139)
MSCS Cluster Resource Preparation (see page 139)
Install CA ARCserve Backup in an MSCS Cluster-aware Environment (see page 140)
Upgrade CA ARCserve Backup from r11.5 to r15 in an MSCS Cluster Environment (see page 151)
Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an MSCS Cluster Environment (see page 157)
Uninstall CA ARCserve Backup from an MSCS Cluster (see page 161)
Delete CA ARCserve Backup Cluster Resources (see page 162)

MSCS Hardware Requirements

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

- CA ARCserve Backup supports cluster-aware configurations on the following operating systems:
  - Windows Server 2003 x86
  - Windows Server 2003 x64

  Note: Windows Server 2008 and Windows Server 2008 r2 operating systems do not support cluster-aware implementations.
- HA platform is configured for a MSCS cluster

MSCS Cluster Resource Preparation

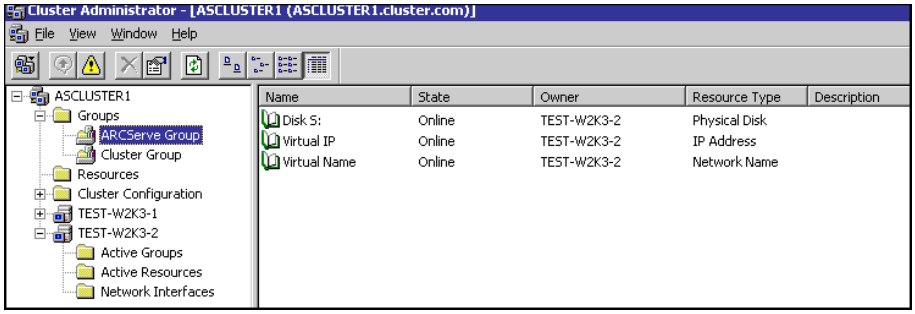
If you are installing CA ARCserve Backup into a dedicated group, you need to create the required resources into the new dedicated group, including a virtual IP address, virtual name, and a shared disk.

Note: Cluster Administrator 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.

In following screen example, a group named "ARCserve Group" is created for CA ARCserve Backup installation with three related resources:

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

Later you can select to install CA 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 CA 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.

Install CA ARCserve Backup in an MSCS Cluster-aware Environment

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

To install CA ARCserve Backup in an MSCS cluster-aware environment

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

   Note: If the CA 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 CA 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 CA ARCserve Backup Prerequisite Components installed on the target computer.
   - You must restart your computer and repeat the above steps if Setup installs Microsoft SQL Server 2008 Express Edition.

     Note: If you are installing CA 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 CA ARCserve Backup.

   Select Install/Upgrade Type dialog

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

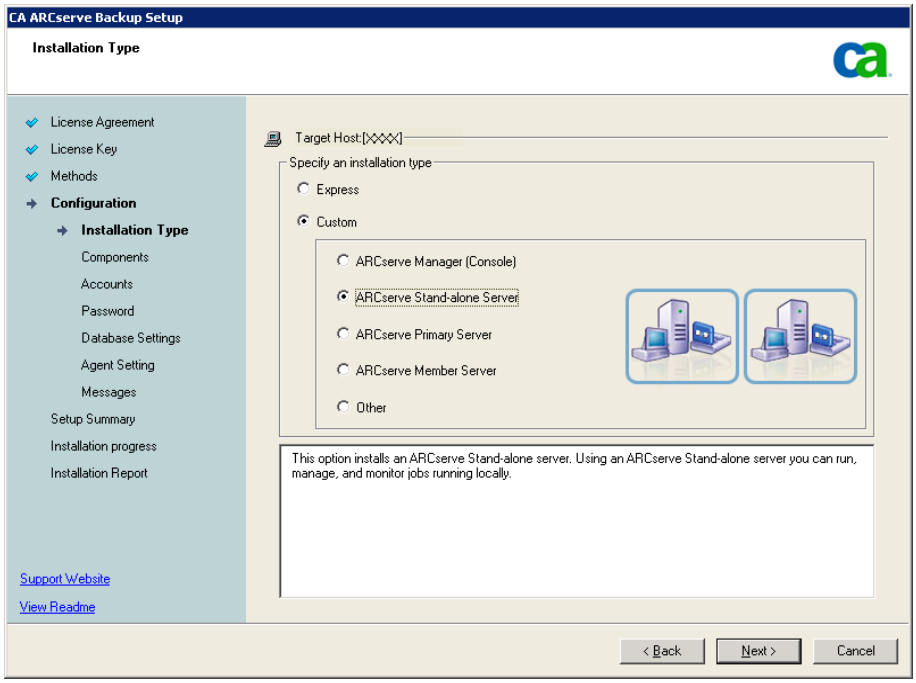
   With remote installations, the target remote systems can consist of different ARCserve server types, different CA ARCserve Backup agents and options, or both.

   Note: The setup program for cluster machines does not support remote installation of the CA ARCserve Backup base product or the CA ARCserve Backup agents. This remote install limitation for the CA 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 CA ARCserve Backup agents using the physical hosts of clusters is supported.

Installation Type dialog

Lets you specify the type of CA 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 CA ARCserve Backup Server Installations (see page 62) and CA ARCserve Backup Server Options (see page 66).



Components dialog

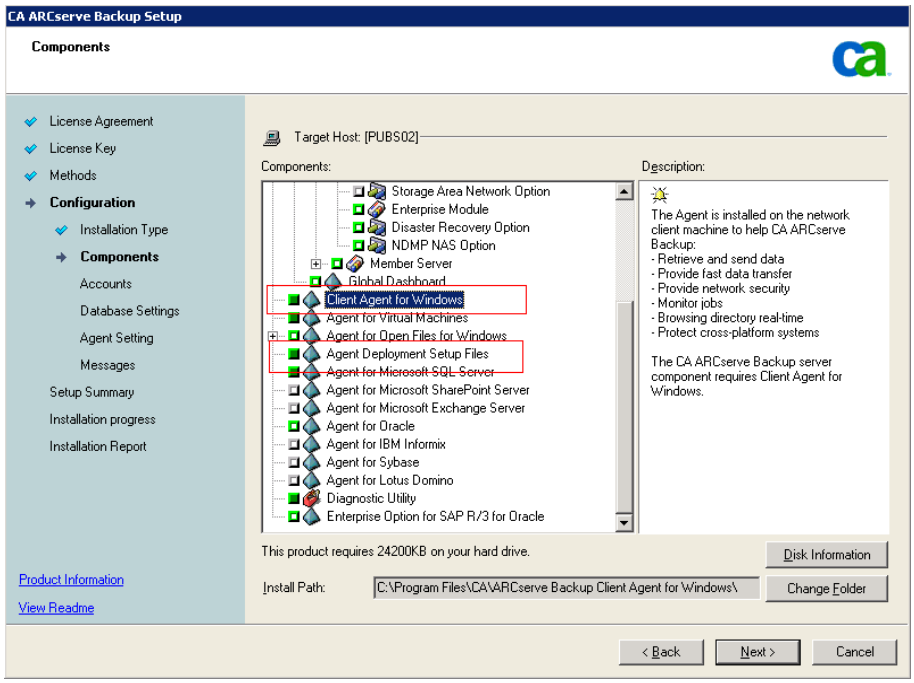
Lets you specify the CA ARCserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the CA ARCserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the CA 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 CA 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 CA 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 CA ARCserve Backup agents on multiple remote systems, after you install CA ARCserve Backup. To support this capability, Setup must copy Setup source files to the CA ARCserve Backup server. To copy the contents of the installation media to the CA 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 CA ARCserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA 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*.

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

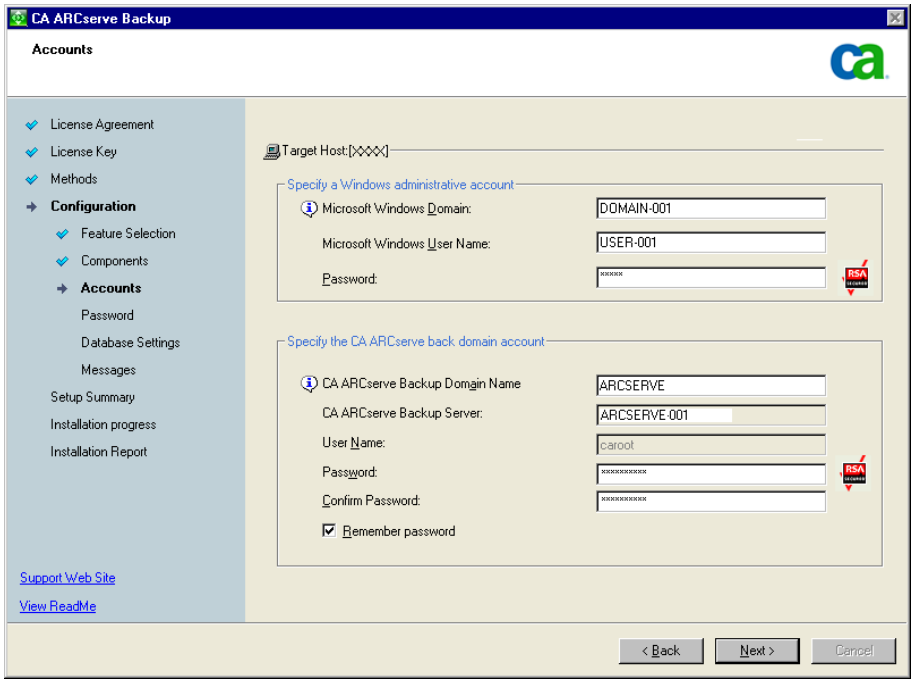


Accounts dialog

Lets you set up your CA ARCserve Backup accounts.

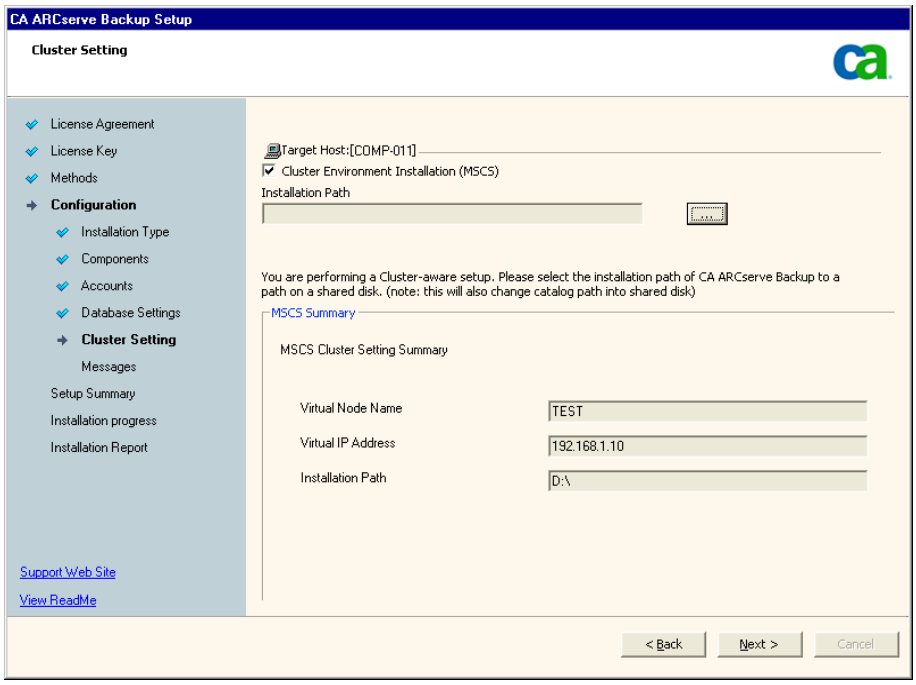
If Setup detects a cluster-aware application running in your environment, and you want to install CA ARCserve Backup in the cluster-aware environment, check the Cluster Environment Installation option and specify the path to the shared disk where you want to install CA ARCserve Backup.

Note: CA ARCserve Backup server names and CA 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 CA 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:

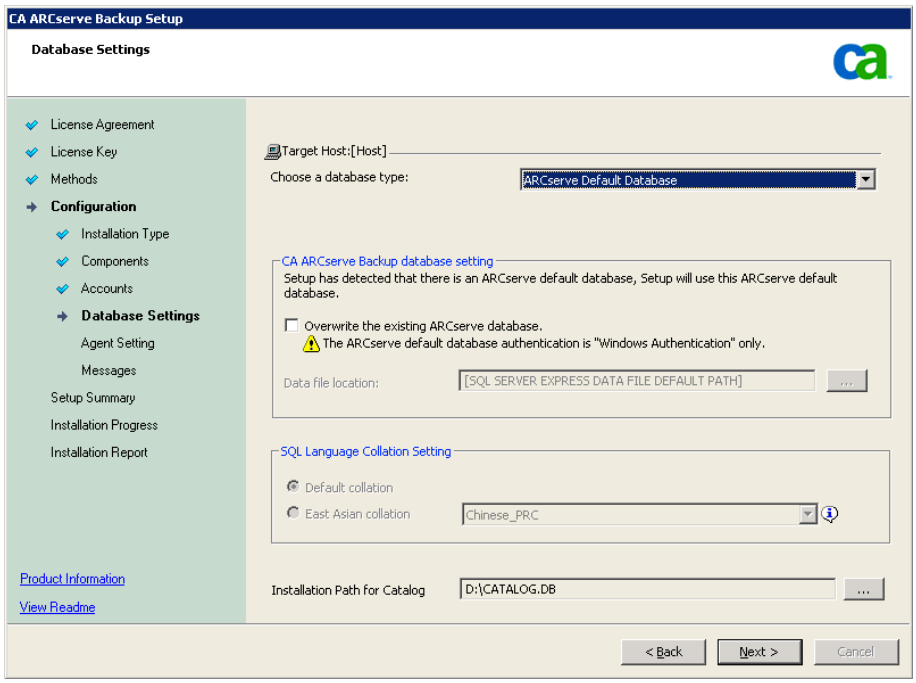
- CA ARCserve Backup does not support local Microsoft SQL Server installations on CA ARCserve Backup servers in NEC CLUSTERPRO environments. Therefore, you must install the ARCserve database instance on a remote system.
- You must specify the Remote SQL Server Type option if the ARCserve database instance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

Database Settings dialog

Lets you configure the CA 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.

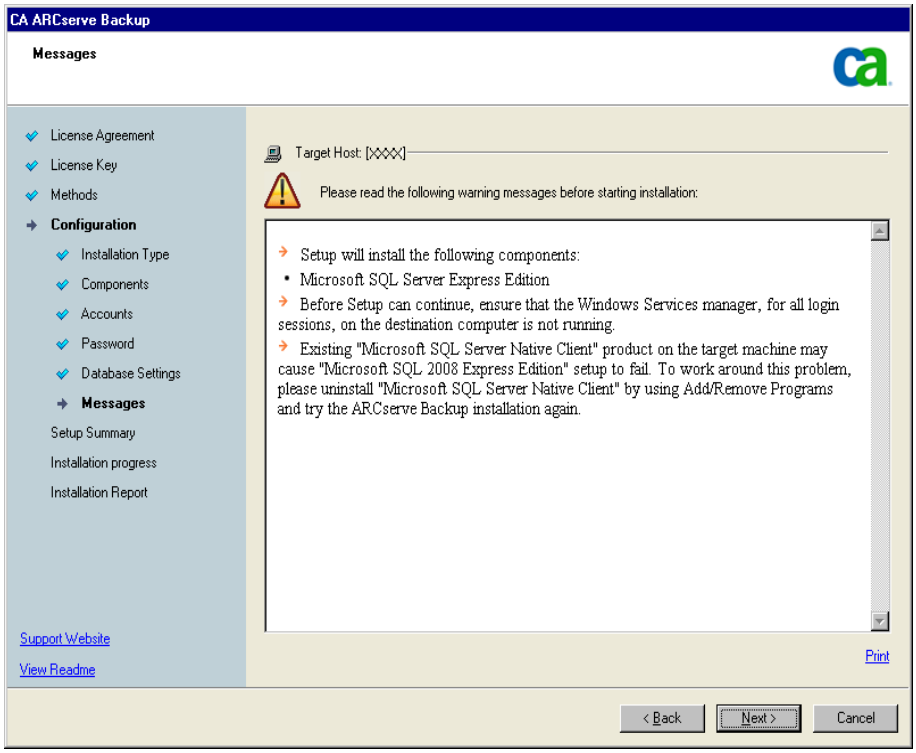
Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that CA ARCserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



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:



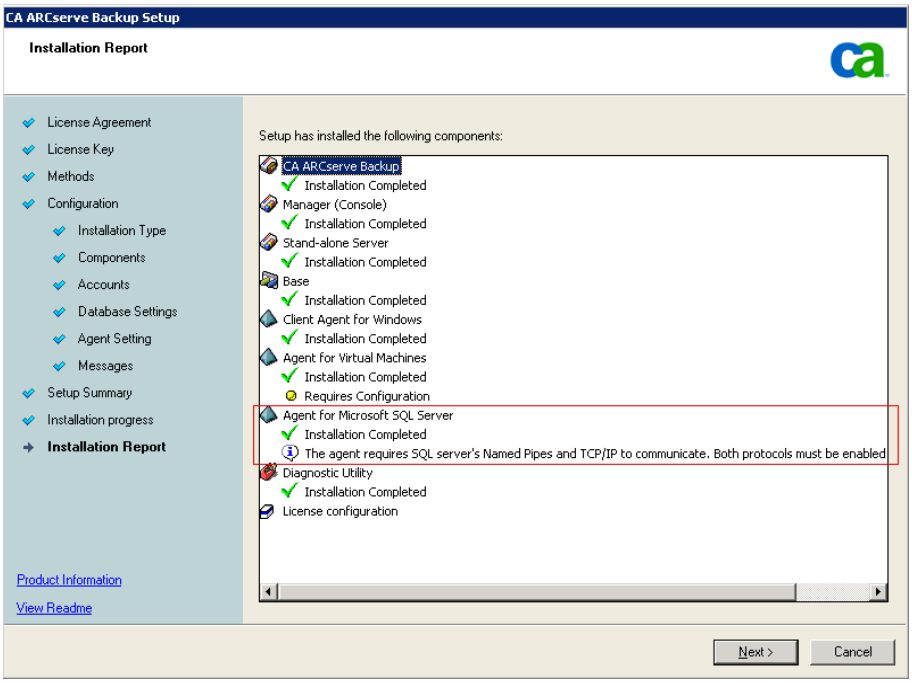
Setup Summary dialog

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 CA 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 CA ARCserve Backup on the passive node.

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

   Be aware of the following:

   - For each cluster node that CA 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 CA ARCserve Backup is installed on the last node in the cluster.

Upgrade CA ARCserve Backup from r11.5 to r15 in an MSCS Cluster Environment

This section describes the steps that you must perform to upgrade earlier software versions to the current release. Upgrade procedures differ depending on the software version you are upgrading:

- If you are upgrading BrightStor ARCserve Backup r11.5, including the latest services packs, in an MSCS cluster-aware environment, directly to CA ARCserve Backup r15, follow this procedure.
- If you are upgrading CA ARCserve Backup r12 or CA ARCserve Backup r12.5, including the latest service packs, in an MSCS cluster-aware environment, follow the steps in Upgrade CA ARCserve Backup from r12 and r12.5 to r15 in an MSCS Cluster Environment (see page 157).

Before you begin, ensure you have read the information in Upgrade CA ARCserve Backup from a Previous Release (see page 97).

When upgrading CA ARCserve Backup from r11.5 to r15 in an MSCS cluster environment, the following procedure must be performed to protect your clustered backup data. If you are not already using CA ARCserve Backup r11.5 in a cluster environment, you do not need to perform this procedure. The procedure supports the following CA ARCserve Backup r11.5 upgrade scenarios in an MSCS cluster environment:

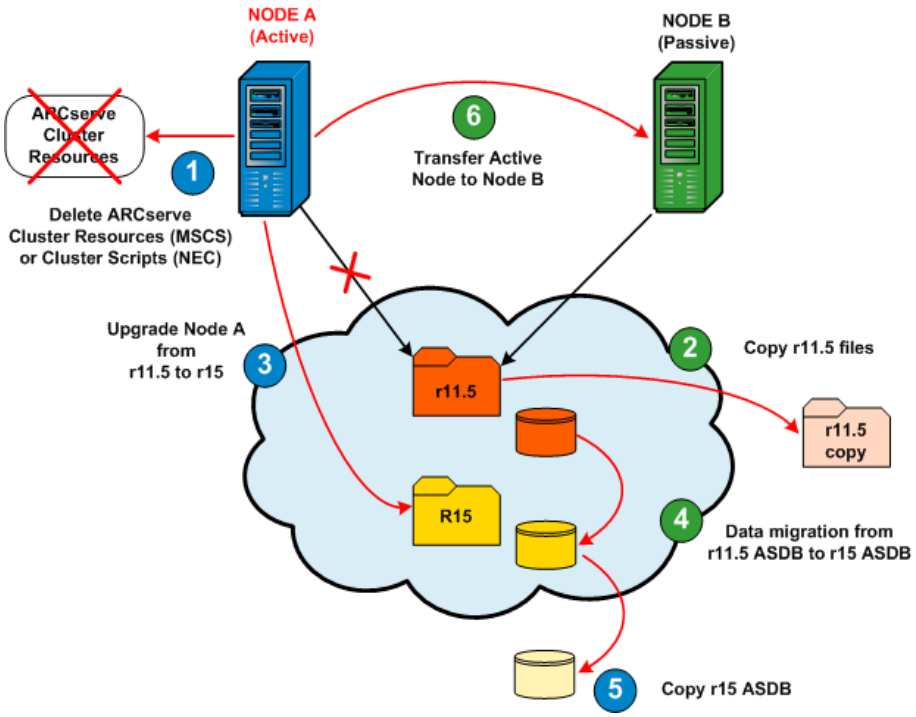
- Primary server upgrade RAIMA to SQL Express
- Primary server upgrade RAIMA to SQL Server
- Primary server upgrade SQL Server to SQL Server
- Member server upgrade RAIMA to r15
- Member server upgrade SQL Server to r15

This upgrade procedure is assuming 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.

To upgrade CA ARCserve Backup from r11.5 to r15 in an MSCS cluster environment

On Node A:

The following diagram provides a graphic overview of the initial tasks being performed for Node A during this upgrade procedure.



1. Delete the ARCserve cluster resources for r11.5 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 r11.5 are deleted.

2. Copy the CA ARCserve Backup r11.5 installation directory files into a temporary location.

   A backup copy of the CA ARCserve Backup r11.5 files is located in another location from the original files.

3. Perform CA ARCserve Backup r15 upgrade installation for Node A. See Upgrade CA ARCserve Backup from a Previous Release (see page 97).

   Important! During the upgrade installation, you will be prompted to specify the installation path location for r15. Do not specify the same location where the r11.5 is currently located. To avoid difficulties during the upgrade and possible loss of information (job scripts saved in the queue), you must select a different location for the CA ARCserve Backup r15 installation.

   Results:

   - CA ARCserve Backup for Node A is upgraded from r11.5 to r15. Do not set up new ARCserve cluster resources at this time.
   - When the upgrade is complete, the Server Data Migration dialog appears. The Server Data Migration dialog allows you to migrate information stored in the previous ARCserve database into a new ARCserve database. Do not launch the data migration process at this time.

   Note: For primary server upgrades, the CA ARCserve Backup database engine must be manually started prior to migrating the data.

4. For primary server upgrades only, do the following:

   a. Open the Windows Computer Management console.

   b. Expand Services and Applications and then click Services.

   c. Right-click CA ARCserve Database Engine, and click Start on the pop-up menu.

   d. Right-click CA ARCserve Domain Server, and click Start on the pop-up menu.

   e. Right-click CA ARCserve Message Engine, and click Start on the pop-up menu.

   f. Close the Windows Computer Management console.

   Note: When CA ARCserve Backup services start, the corresponding status indicates Started.

5. Open the CA ARCserve Backup installation directory on the CA ARCserve Backup server.

   In the CA ARCserve Backup installation directory, locate and double-click servermigration.exe.

   The Server Data Migration dialog opens.

6. From the Server Data Migration dialog, click Start.

   The specified CA ARCserve Backup data is migrated from r11.5 to r15.

7. For SQL Express upgrades only. Using the Windows Service manager, right-click the SQLE instance (mssql$arcserve_db) and from the pop-up window, select Stop.

   When the SQLE instance is stopped, the corresponding status will become blank and no longer indicate Started.

8. For SQL Express primary server upgrades only. Copy the SQL ARCserve database directory (SQLASDB) into a temporary location.

   A backup copy of the SQLASDB directory is located in another location from the original directory.

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

   a. Access the Cluster Administrator.

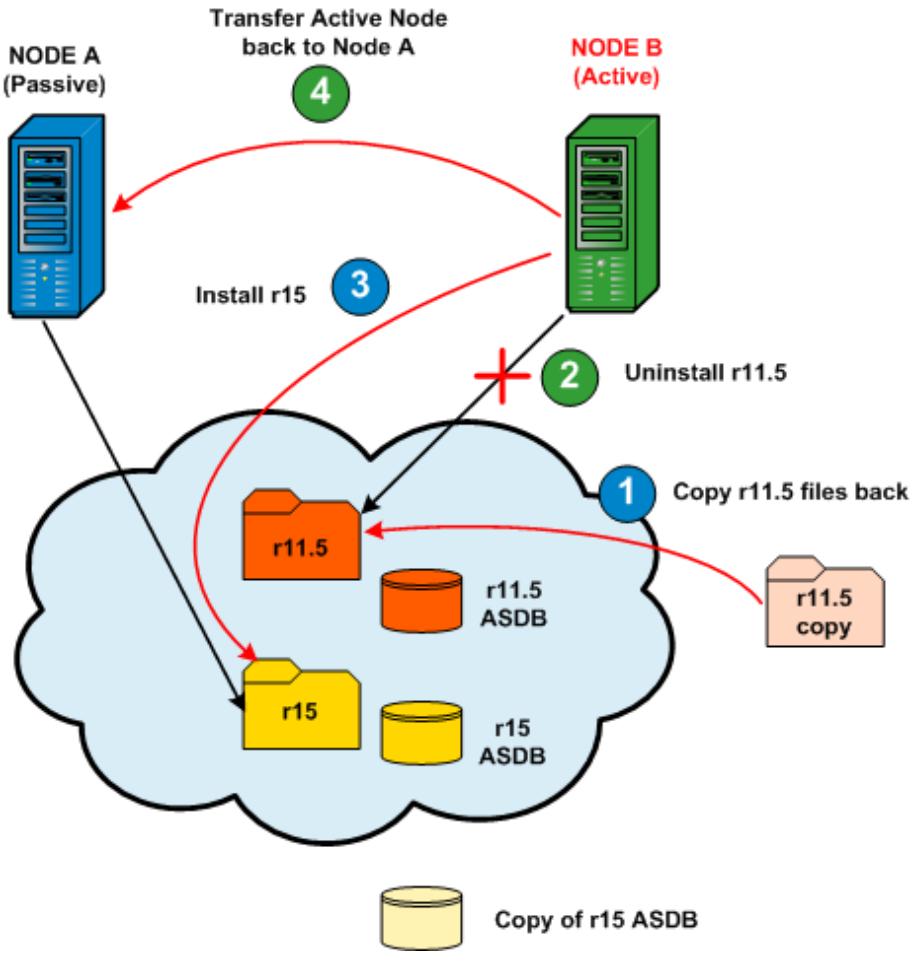
      The Cluster Administrator dialog opens.

   b. Select the ARCserve Group for Node A. Right-click on the group name from the pop-up menu and select Move Group.

      - If there are only two nodes in the cluster, the active node status will automatically be transferred from the initial active node (Node A) to the other node (Node B) and 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 will appear, allowing you to select which node you want to transfer the active status to. When you select the node for transfer, the specified node will become the active node and the previously-selected node will become the passive node. Repeat this procedure for each node in the cluster.

On Node B:

The following diagram provides a graphic overview of the initial tasks being performed for Node B during this upgrade procedure.



1. Copy the CA ARCserve Backup r11.5 installation directory files from the temporary location back into the original location.

   The CA ARCserve Backup r11.5 files are now located back in the original location.

2. Uninstall CA ARCserve Backup r11.5 from Node B.

   CA ARCserve Backup r11.5 is uninstalled.

   Important! During the CA ARCserve Backup r15 new installation on Node B, do not select the "Overwrite DB" option to prevent overwriting the ARCserve database that was migrated during the r15 upgrade to Node A.

3. Perform CA ARCserve Backup r15 new installation for Node B with the same settings selected for Node A (domain name, server type, install path, installed options …). For example, if CA ARCserve Backup r15 was installed on Node A as a primary server, then r15 must be installed on Node B also as a primary server. See Install CA ARCserve Backup.

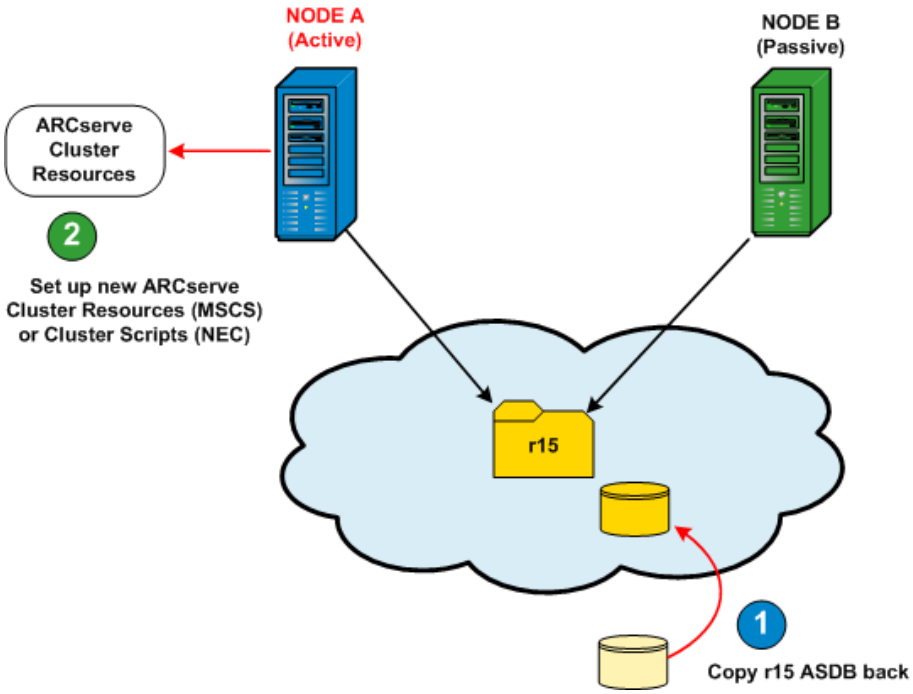
   CA ARCserve Backup r15 is installed on Node B. Do not set up new ARCserve cluster resources at this time.

4. Move the active node from Node B back to Node A as previously described.

   Node B is now the passive node and Node A is the active node.

On Node A:

The following diagram provides a graphic overview of the final tasks being performed for Node A during this upgrade procedure.



1. For SQL Express primary server upgrades only. Copy the SQL ARCserve database directory (SQLASDB) from the temporary location back into the original location.

   The backed-up copy of the SQLASDB directory replaces the SQLASDB directory created during the CA ARCserve Backup r15 installation.

2. 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 (ARCserve HA, ARCserve ASDB, ARCserve Registry, and ARCserve Share) are created.

   To ensure that all CA ARCserve Backup services start properly on the CA ARCserve Backup server, you must execute the cstop and cstart scripts on the CA ARCserve Backup server before you open the CA ARCserve Backup Manager Console. The cstop and cstart batch files are stored in the CA ARCserve Backup installation directory on the CA ARCserve Backup server. For more information about using cstop and cstart, see the *Administration Guide*.

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

More information:

How to Verify a Cluster-aware Installation and Upgrade (see page 198)

Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an MSCS Cluster Environment

This section describes the steps you must perform to upgrade from earlier software versions to the current release. Please ensure you are following the appropriate procedure:

- To upgrade BrightStor ARCserve Backup r11.5, including the latest service packs, in an MSCS cluster-aware environment, directly to CA ARCserve Backup r15, follow the steps in Upgrade CA ARCserve Backup from r11.5 to r15 in an MSCS Cluster Environment (see page 151).
- To upgrade CA ARCserve Backup r12 or r12.5, including the latest service packs, in an MSCS cluster-aware environment, follow this procedure.

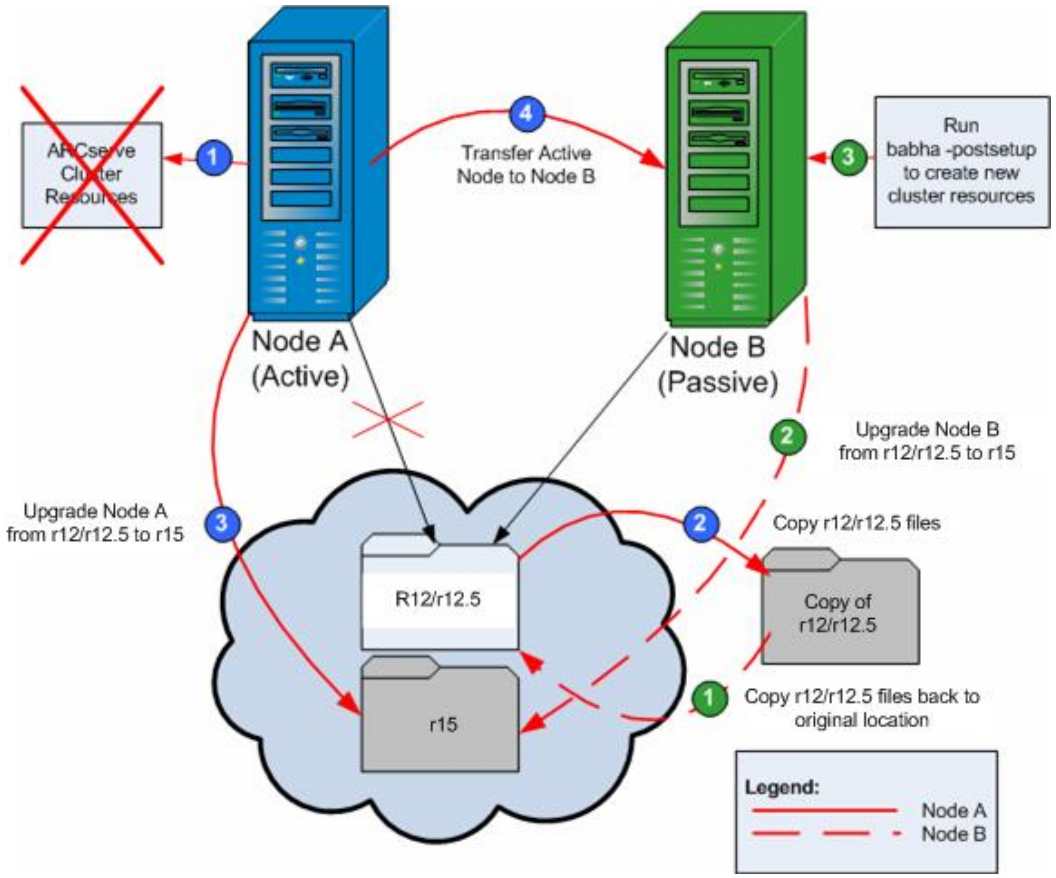
Before you begin, ensure that you read the information in Upgrade CA ARCserve Backup from a Previous Release (see page 97).

When upgrading CA ARCserve Backup to r15 in an MSCS cluster environment, the following procedure must be performed to protect your clustered backup data. If you are not already using CA ARCserve Backup r12 or r12 in a cluster environment, you do not need to perform this procedure. The procedure supports the following CA ARCserve Backup r12 or r12.5 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 r15 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 CA ARCserve Backup from r12 or r12.5 to r15 in an MSCS cluster environment

Important! Before you start the following procedure, verify that you synchronize the CA 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/r12.5 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/r12.5 are deleted.

2. Copy the CA ARCserve Backup r12/r12.5 installation directory files into a temporary location.

   A backup copy of the CA ARCserve Backup r12/r12.5 files is located in another location from the original files.

3. Perform CA ARCserve Backup r15 upgrade installation for Node A. See Upgrade CA ARCserve Backup from a Previous Release (see page 97).

   – The installation path location for CA ARCserve Backup r15 upgrade must be the same location where r12/r12.5 is currently located.

   CA ARCserve Backup for Node A is upgraded from r12/r12.5 to r15. 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 CA ARCserve Backup r12/r12.5 installation directory files from the temporary location back into the original location.

   The CA ARCserve Backup r12/r12.5 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 CA 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 CA ARCserve Backup r15 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 CA 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 (ARCserve HA, ARCserve ASDB, ARCserve Registry, and ARCserve Share) are created.

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

More information:

How to Verify a Cluster-aware Installation and Upgrade (see page 198)

Uninstall CA ARCserve Backup from an MSCS Cluster

Uninstalling CA 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 CA ARCserve Backup from a MSCS Cluster

1. Delete all cluster resources. For more information, see Delete CA ARCserve Backup Cluster Resources (see page 162).

   All CA 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 ARCserve HA 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).

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

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

   CA ARCserve Backup is removed from the current (active) node.

5. Copy the .dll files back into the original location in the ARCserve Backup directory.

   The .dll files for CA 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.

   CA ARCserve Backup is removed from all nodes in the cluster.

Delete CA ARCserve Backup Cluster Resources

Prior to creating new cluster resources, it is necessary to delete all existing cluster resources from the group where CA ARCserve Backup is deployed. The available MSCS cluster resources are:

- ARCserve HA
- ARCserve ASDB
- ARCserve Registry
- ARCserve Share

Delete the ARCserve cluster resources

1. From the Cluster Administrator, right-click on the group name and from the pop-up menu, select Take Offline.

   The state of the ARCserve cluster resources is changed from Online to Offline.

2. Access the Cluster Administrator.

   The Cluster Administrator dialog appears.

   Note: 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.

3. 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 selected ARCserve cluster resources are deleted.

Deploy CA ARCserve Backup Server on NEC Cluster

The following sections provide information about deploying CA ARCserve Backup on a NEC cluster. CA ARCserve Backup cluster support is provided for NEC CLUSTERPRO/ExpressCluster for Windows 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, and NEC CLUSTERPRO/ExpressCluster X 2.0 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 163)
NEC CLUSTERPRO/ExpressCluster Software Requirements (see page 164)
NEC CLUSTERPRO/ExpressCluster Resource Preparation (see page 164)
Install CA ARCserve Backup in an NEC Cluster-aware Environment (see page 165)
Upgrade CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO Environment (see page 180)
Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an NEC CLUSTERPRO Environment (see page 193)
Uninstall CA ARCserve Backup from a NEC CLUSTERPRO/ExpressCluster (see page 197)

NEC CLUSTERPRO/ExpressCluster Hardware Requirements

To deploy CA 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 CA ARCserve Backup on NEC CLUSTERPRO/ExpressCluster, your system must meet the following software requirements:

- CA 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

  Note: NEC CLUSTERPRO/ExpressCluster is not supported on IA-64 (Intel Itanium) operating systems.
- HA platform is configured for NEC CLUSTERPRO/ExpressCluster for Windows 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, or NEC CLUSTERPRO/ExpressCluster X 2.0 for Windows.

NEC CLUSTERPRO/ExpressCluster Resource Preparation

If you are installing CA 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.

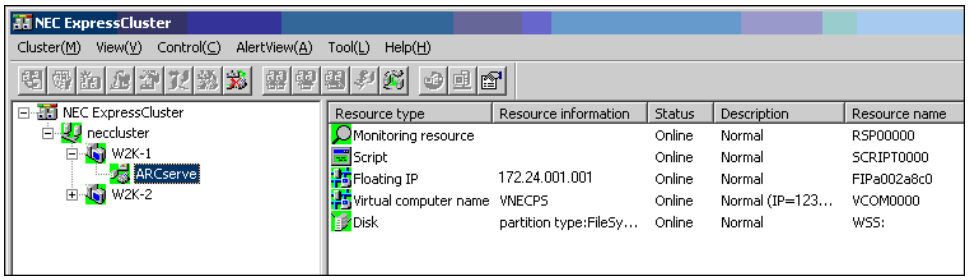
Cluster Manager and Task Manager are utilities provided by NEC and are installed on servers that have NEC CLUSTERPRO/ExpressCluster installed.

- 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 CA ARCserve Backup installation with four related resources:

- Shared Disk
- Floating IP address
- Virtual Name
- Script

Later you can select to install CA 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 CA ARCserve Backup in an NEC Cluster-aware Environment

You can install CA ARCserve Backup in an NEC cluster-aware environment using the installation wizard.

To install CA ARCserve Backup in an NEC cluster-aware environment

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

   Note: If the CA 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 CA 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 CA ARCserve Backup Prerequisite Components installed on the target computer.
   - You must restart your computer and repeat the above steps if Setup installs Microsoft SQL Server 2008 Express Edition.

     Note: If you are installing CA 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 CA ARCserve Backup.

   Select Install/Upgrade Type dialog

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

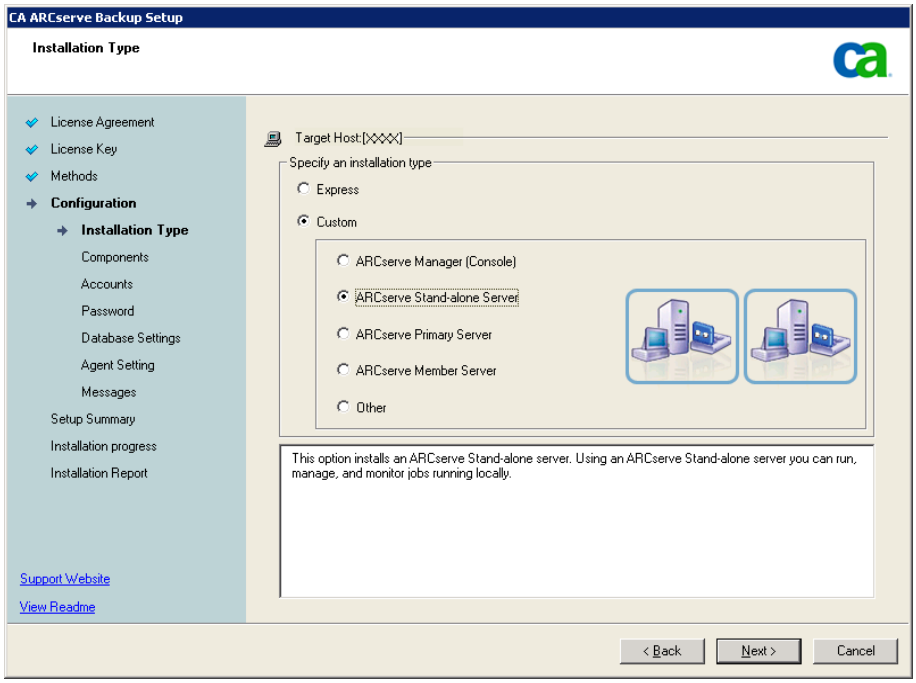
   With remote installations, the target remote systems can consist of different ARCserve server types, different CA ARCserve Backup agents and options, or both.

   Note: The setup program for cluster machines does not support remote installation of the CA ARCserve Backup base product or the CA ARCserve Backup agents. This remote install limitation for the CA 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 CA ARCserve Backup agents using the physical hosts of clusters is supported.

Installation Type dialog

Lets you specify the type of CA 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 CA ARCserve Backup Server Installations (see page 62) and CA ARCserve Backup Server Options (see page 66).



Components dialog

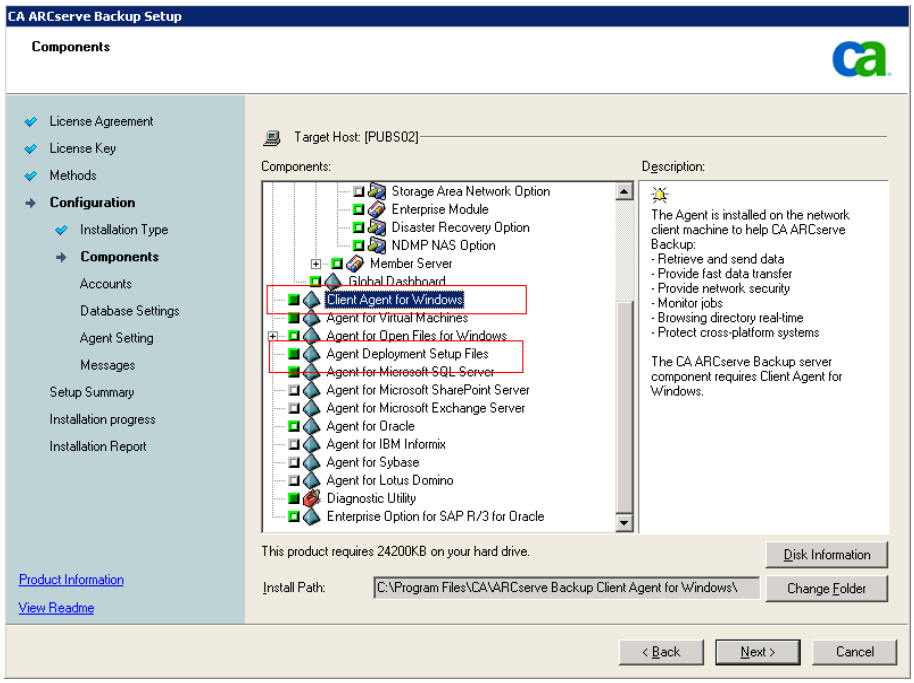
Lets you specify the CA ARCserve Backup components that you want to install on the target system.

Be aware of the following considerations:

- To install a primary server, you must install the CA ARCserve Backup Central Management Option on the primary server.
- To install member servers, the installation wizard must be able to detect the CA 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 CA 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 CA 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 CA ARCserve Backup agents on multiple remote systems, after you install CA ARCserve Backup. To support this capability, Setup must copy Setup source files to the CA ARCserve Backup server. To copy the contents of the installation media to the CA 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 CA ARCserve Backup increases significantly.
- If you are performing a remote installation or a silent installation, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA 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*.

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

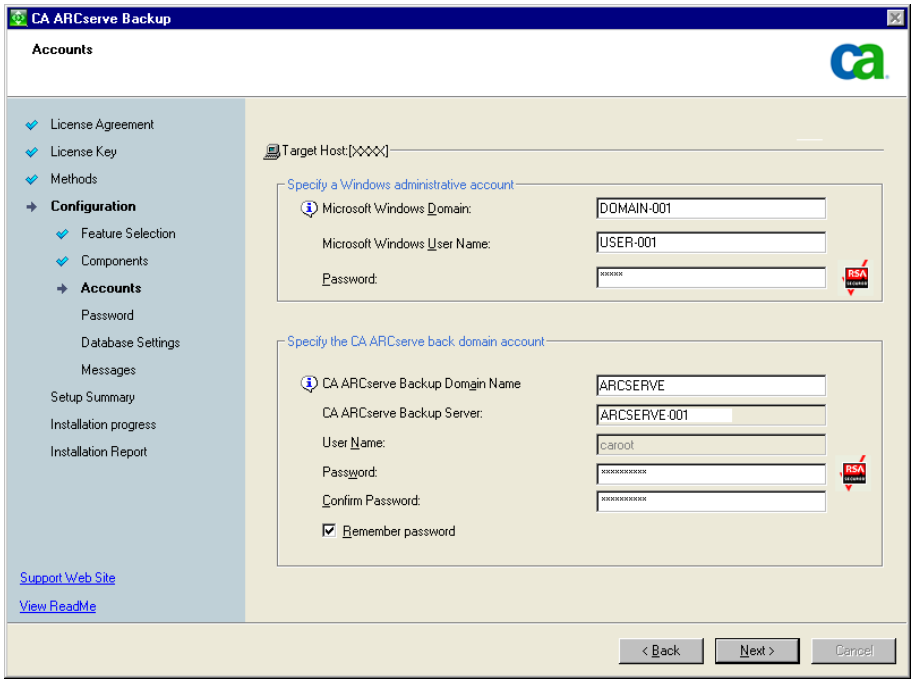


Accounts dialog

Lets you set up your CA ARCserve Backup accounts.

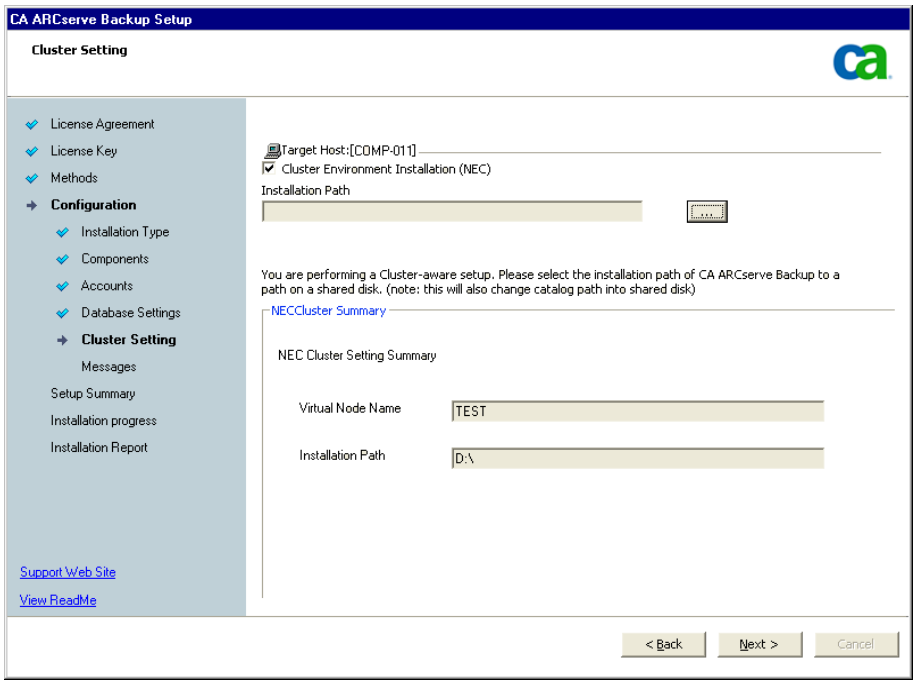
If Setup detects a cluster-aware application running in your environment, and you want to install CA ARCserve Backup in the cluster-aware environment, check the Cluster Environment Installation option and specify the path to the shared disk where you want to install CA ARCserve Backup.

Note: CA ARCserve Backup server names and CA 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 CA ARCserve Backup into a cluster-aware environment. You must complete all fields on this dialog to continue.

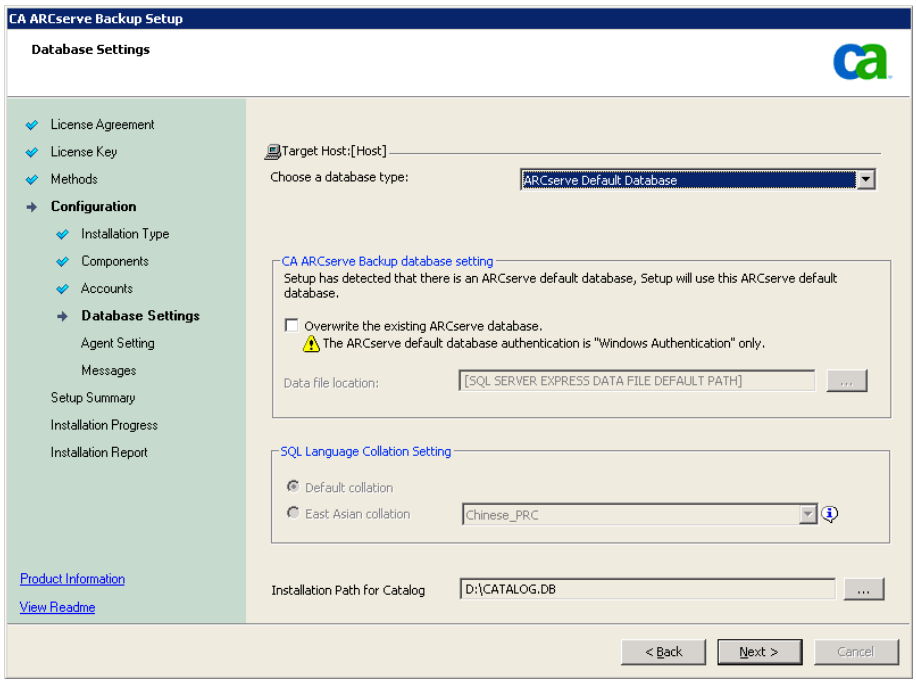


Database Settings dialog

Lets you configure the CA 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.

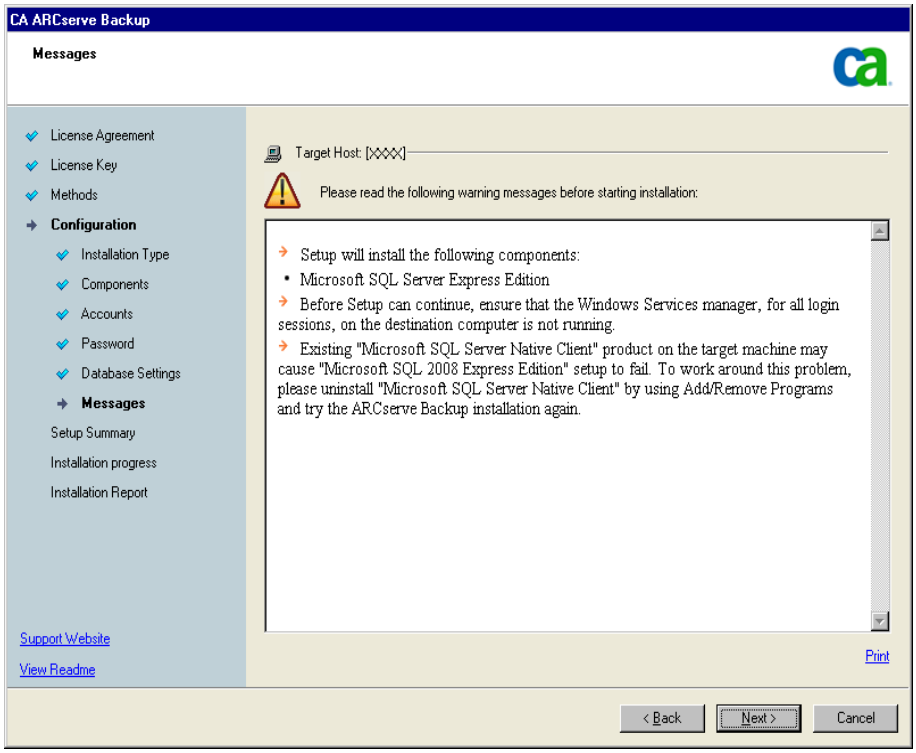
Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that CA ARCserve Backup can search and sort the data. To do this, click East Asian collation and then select a language from the drop-down list.



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:



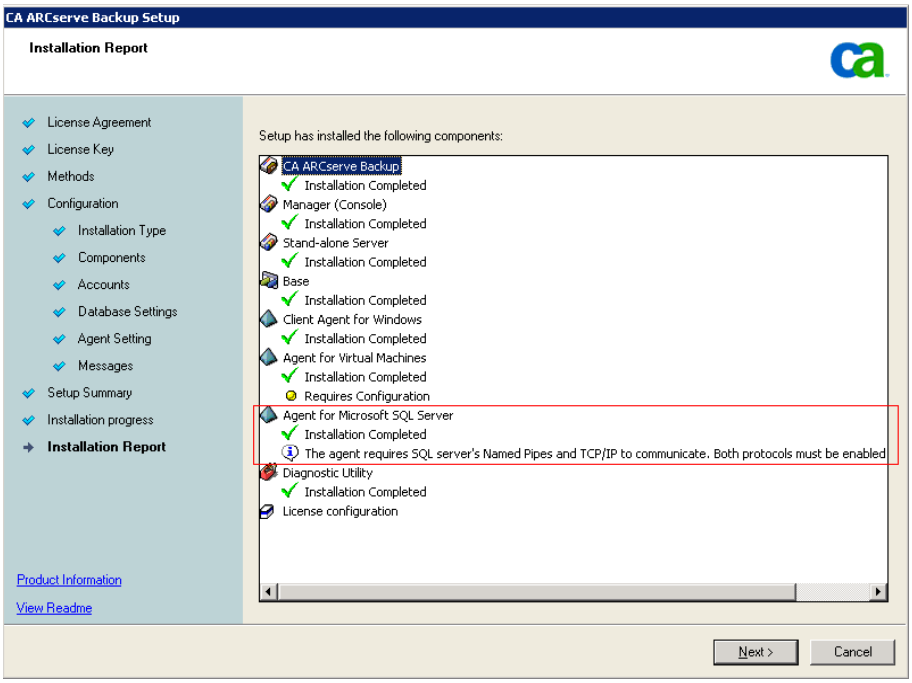
Setup Summary dialog

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 CA 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 CA ARCserve Backup on the passive node.

   Note: Repeat Steps 1 to 5 to install CA ARCserve Backup on the passive node.
7. For each cluster node that CA 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, you need to create new start.bat and stop.bat scripts for the applicable server:

   - For all member servers and non-SQL Express primary servers, use the start.bat scripts contained in start.bat Script Changes for Member Servers and Non-SQL Express Primary Servers (see page 176).
   - For all member servers and non-SQL Express primary servers, use the stop.bat scripts contained in stop.bat Script Changes for Member Servers and Non-SQL Express Primary Servers (see page 177).
   - For SQL Express primary servers only, use the start.bat script contained in start.bat Script Changes for SQL Express Primary Servers (see page 178).
   - For SQL Express primary servers only, use the stop.bat script contained in stop.bat Script Changes for SQL Express Primary Servers (see page 179).

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 CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO Environment

This section describes the steps you must perform to upgrade from earlier software versions to the current release. Please ensure you are following the appropriate upgrade procedure:

- To upgrade BrightStor ARCserve Backup from r11.5, including the latest service packs, in an NEC CLUSTERPRO cluster-aware environment, directly to r15, follow this procedure.
- To upgrade CA ARCserve Backup r12, including the latest service packs, to r15 in an NEC CLUSTERPRO cluster-aware environment, follow the steps in Upgrade CA ARCserve Backup from r12 to r15 in an NEC CLUSTERPRO Environment (see page 193).

This section describes the steps that you must perform to upgrade BrightStor ARCserve Backup r11.5, including the latest service packs, in an NEC CLUSTERPRO cluster-aware environment, to CA ARCserve Backup r15. For information about how to upgrade CA ARCserve Backup r12 in a NEC CLUSTERPRO cluster-aware environment to this release, follow the steps described in Upgrade CA ARCserve Backup from a Previous Release (see page 97).

When upgrading CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO environment, the following procedure must be performed to safely protect your clustered backup data. If you are not already using CA ARCserve Backup r11.5 in a cluster environment, you do not need to perform this procedure. The procedure supports the following CA ARCserve Backup r11.5 upgrade scenarios in an NEC CLUSTERPRO environment:

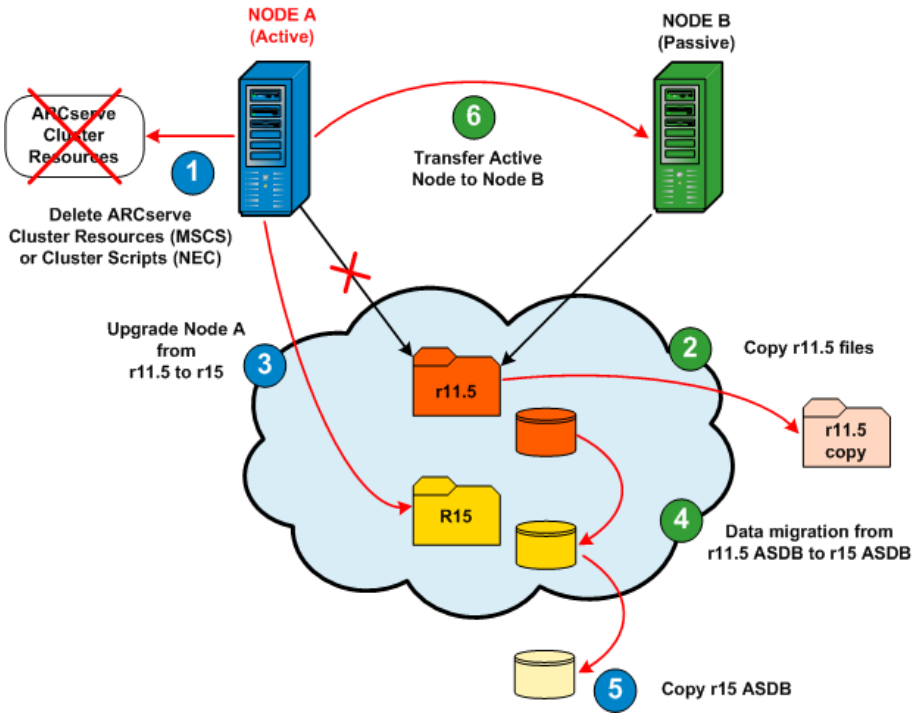
- Upgrade BrightStor ARCserve Backup r11.5 with a RAIMA database to CA ARCserve Backup r15 on a Primary Server with a Microsoft SQL Server 2008 Express Edition database
- Upgrade BrightStor ARCserve Backup r11.5 with a remote Microsoft SQL Server database to CA ARCserve Backup r15 on a Primary Server with a Microsoft SQL Server database
- Upgrade BrightStor ARCserve Backup r11.5 with a RAIMA database to CA ARCserve Backup r15 on a Member Server
- Upgrade BrightStor ARCserve Backup r11.5 with a remote Microsoft SQL Server database to CA ARCserve Backup r15 on a 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.

To upgrade CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO environment

On Node A:

The following diagram provides a graphic overview of the initial tasks being performed for Node A during this upgrade procedure.



1. Disable the NEC Cluster Scripts and delete the Registry Sync. For more information, see Disable CA ARCserve Backup in NEC Cluster Scripts (see page 187).
2. Copy the CA ARCserve Backup r11.5 installation directory files into a temporary location.

   A backup copy of the CA ARCserve Backup r11.5 files is located in different location from the original files.

3. Perform CA ARCserve Backup r15 upgrade installation for Node A. For more information, see Upgrade CA ARCserve Backup from a Previous Release (see page 97).

   Important! During the upgrade installation, you will be prompted to specify the installation path location for r15. Do not specify the same location where the r11.5 is currently located. To avoid difficulties during the upgrade and possible loss of information (job scripts saved in the queue), you must select a different location for the r15 installation.

   - CA ARCserve Backup for Node A is upgraded from r11.5 to r15. Do not set up new ARCserve cluster resources at this time.
   - When the upgrade is complete, the Server Data Migration dialog appears. The Server Data Migration dialog allows you to migrate information stored in the previous ARCserve database into a new ARCserve database. Do not launch the data migration process at this time.

   Note: For primary server upgrades, the CA ARCserve Backup database engine must be manually started prior to migrating the data.

4. For primary server upgrades only, do the following:

   a. Open the Windows Computer Management console.

   b. Expand Services and Applications and then click Services.

   c. Right-click CA ARCserve Database Engine, and click Start on the pop-up menu.

   d. Right-click CA ARCserve Domain Server, and click Start on the pop-up menu.

   e. Right-click CA ARCserve Message Engine, and click Start on the pop-up menu.

   f. Close the Windows Computer Management console.

   Note: When CA ARCserve Backup services start, the corresponding status indicates Started.

5. Open the CA ARCserve Backup installation directory on the CA ARCserve Backup server.

   In the CA ARCserve Backup installation directory, locate and double-click servermigration.exe.

   The Server Data Migration dialog opens.

6. From the Server Data Migration dialog, click Start.

   The specified CA ARCserve Backup data is migrated from r11.5 to r15.

7. For SQL Express upgrades only. Using the Windows Service manager, right-click the SQLE instance (mssql$arcserve_db) and from the pop-up window, select Stop.

   When the SQLE instance is stopped, the corresponding status will become blank and no longer indicate Started.

8. For SQL Express primary server upgrades only. Copy the SQL ARCserve database directory (SQLASDB) into a temporary location.

   A backup copy of the SQLASDB directory is located in a different location from the original directory.

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

   a. Access the Cluster Manager.

      The Cluster Manager dialog appears.

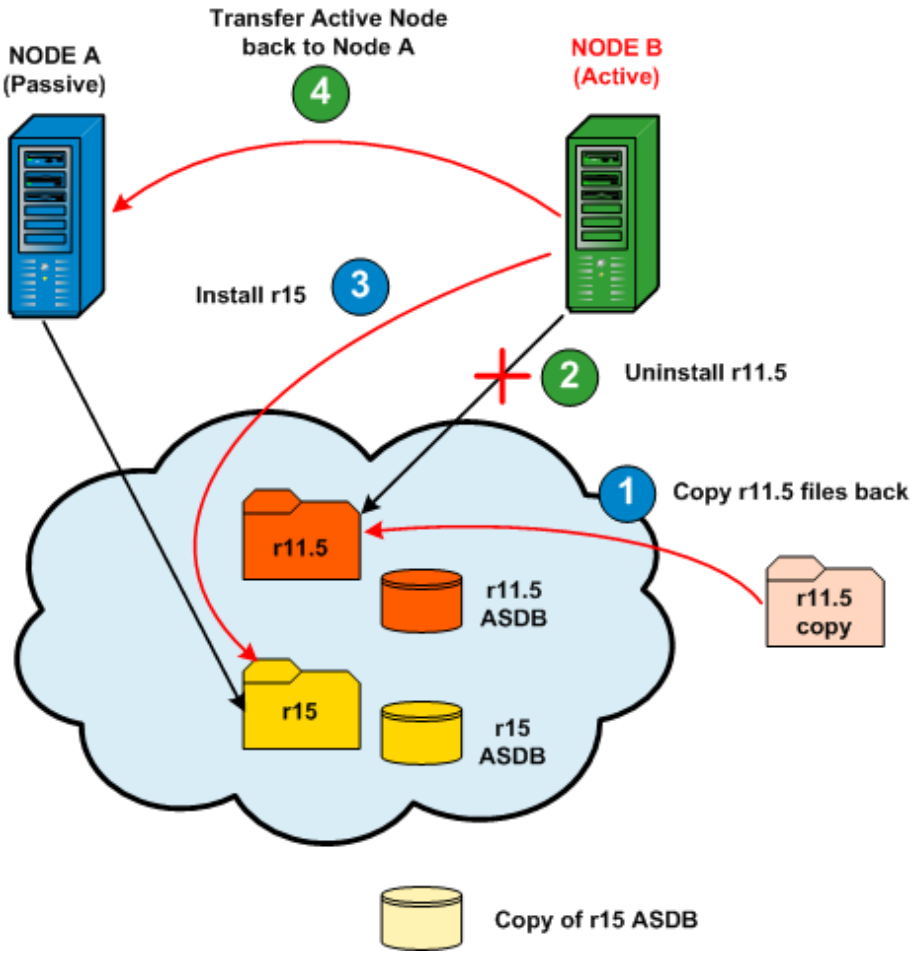
      Note: Cluster Manager is a utility provided by NEC and is installed on servers that have NEC CLUSTERPRO installed. Cluster Manager is accessed from the NEC ExpressCluster Server group of the Start menu. From the Cluster Manager, you perform most of the configuration and management tasks associated with clusters.

   b. 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 Move Group.

      - If there are only two nodes in the cluster, the active node status will automatically be transferred from the initial active node (Node A) to the other node (Node B) and 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 will appear, allowing you to select which node you want to transfer the active status to. When you select the node for transfer, the specified node will become the active node and the previously-selected node will become the passive node. Repeat this procedure for each node in the cluster.

On Node B:

The following diagram provides a graphic overview of the initial tasks being performed for Node B during this upgrade procedure.



1. Copy the CA ARCserve Backup r11.5 installation directory files from the temporary location back into the original location.

   The CA ARCserve Backup r11.5 files are now located back in the original location.

2. Uninstall CA ARCserve Backup r11.5 from Node B.

   CA ARCserve Backup r11.5 is uninstalled.

   Important! During the CA ARCserve Backup r15 new installation on Node B, do not select the "Overwrite DB" option to prevent overwriting the ARCserve database that was migrated during the CA ARCserve Backup r15 upgrade to Node A.

3. Perform CA ARCserve Backup r15 new installation for Node B with the same settings selected for Node A (domain name, server type, install path, installed options …). For example, if r15 was installed on Node A as a primary server, then CA ARCserve Backup r15 must be installed on Node B also as a primary server. For more information, see Install CA ARCserve Backup.

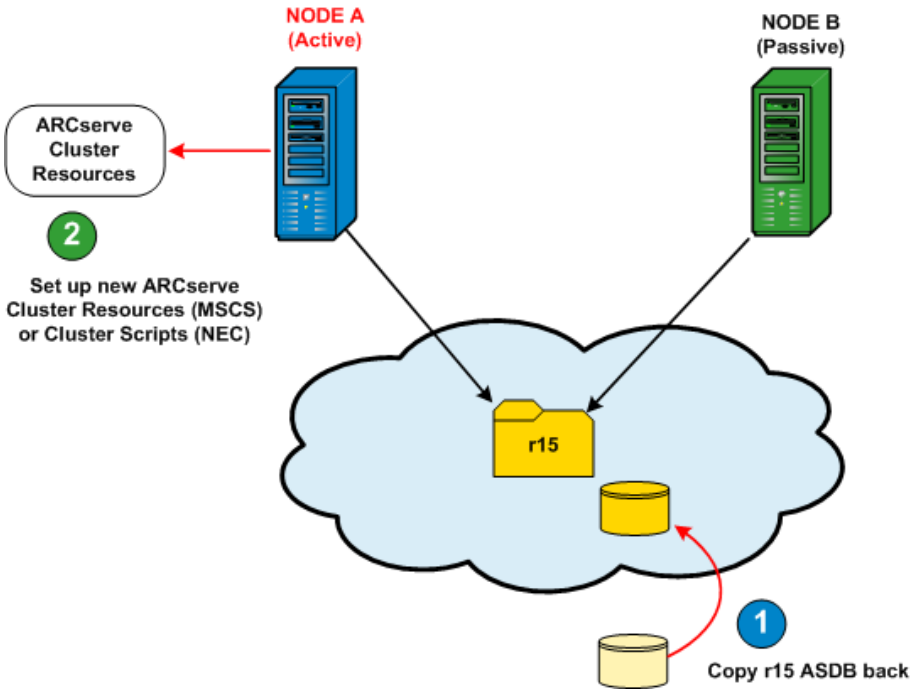
   CA ARCserve Backup r15 is installed on Node B. Do not set up new ARCserve cluster resources at this time.

4. Move the active node from Node B back to Node A as previously described.

   Node B is now the passive node and Node A is the active node.

On Node A:

The following diagram provides a graphic overview of the final tasks being performed for Node A during this upgrade procedure.



1. For SQL Express primary server upgrades only. Copy the SQL ARCserve database directory (SQLASDB) from the temporary location back into the original location.

   The backed-up copy of the SQLASDB directory replaces the SQLASDB directory created during the r15 installation.

2. Rebuild the NEC Cluster Scripts and Registry Sync. For more information, see Enable CA ARCserve Backup in NEC Cluster Scripts (see page 190).

   The new NEC HA scripts are created and the registry is synchronized.

3. To ensure that all CA ARCserve Backup services start properly on the CA ARCserve Backup server, you must execute the cstop and cstart scripts on the CA ARCserve Backup server before you open the CA ARCserve Backup Manager Console. The cstop and cstart batch files are stored in the CA ARCserve Backup installation directory on the CA ARCserve Backup server. For more information about using cstop and cstart, see the *Administration Guide*.

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

More information:

How to Verify a Cluster-aware Installation and Upgrade (see page 198)

Disable CA ARCserve Backup in NEC Cluster Scripts

Cluster scripts and registry keys are inserted during the NEC post-setup process. When upgrading to from BrightStor ARCserve Backup r11.5 to this 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 the NEC Cluster Scripts and Registry Key

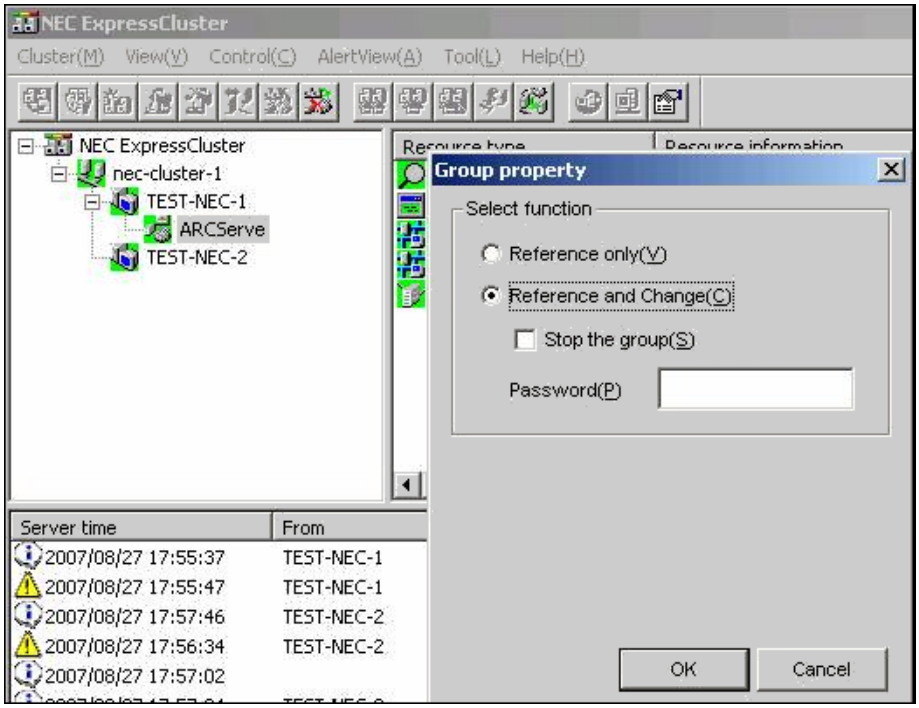
1. Access the Cluster Manager.

   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.

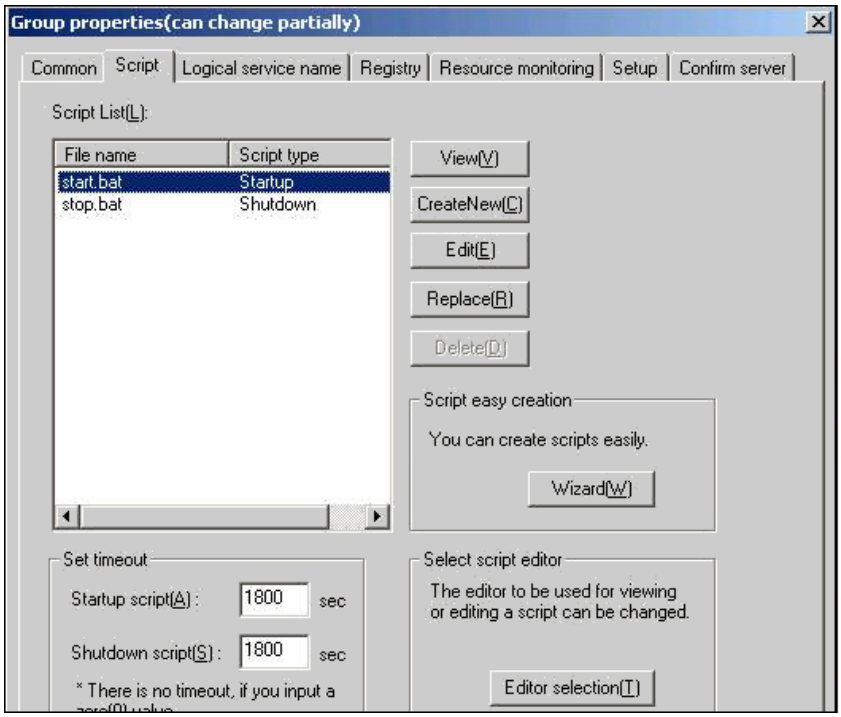
2. Select the NEC Group that the ARCserve server is deployed in, and locate the corresponding ARCserve cluster resources. Right-click on each ARCserve cluster resource and from the pop-up menu, select Property.

   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:

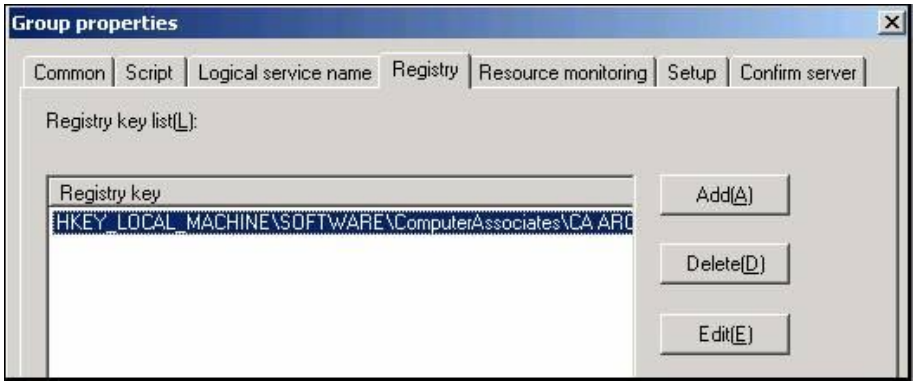
   SET process=0

   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 CA ARCserve Backup in NEC Cluster Scripts

Cluster scripts and registry keys are inserted during the NEC post-setup process. During the upgrade process from BrightStor ARCserve Backup r11.5 to this release, part of 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 the NEC Cluster Scripts and Registry Key

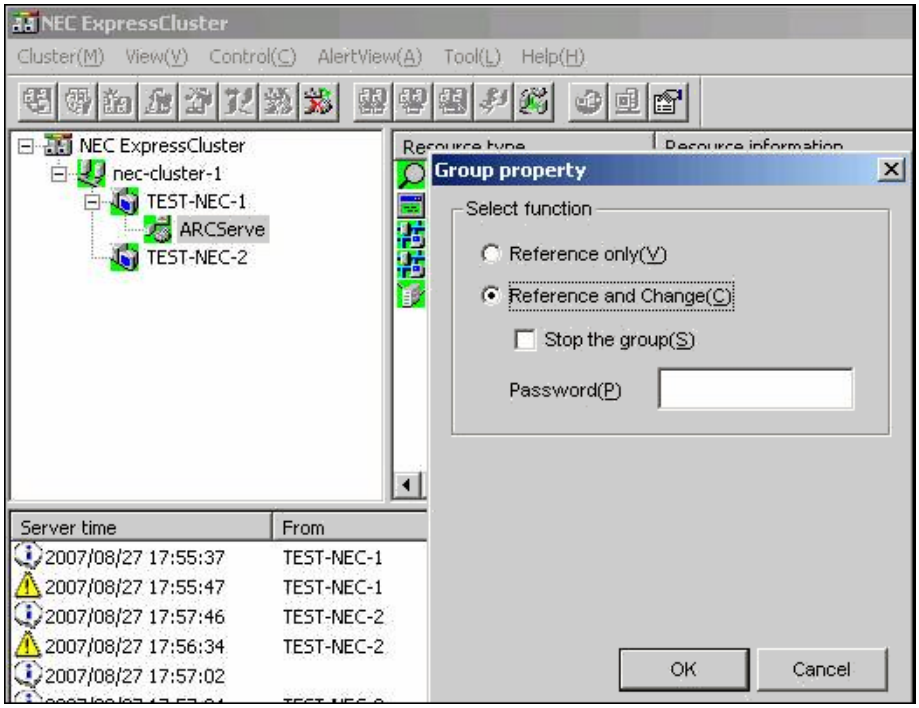
1. Access Cluster Manager.

   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.

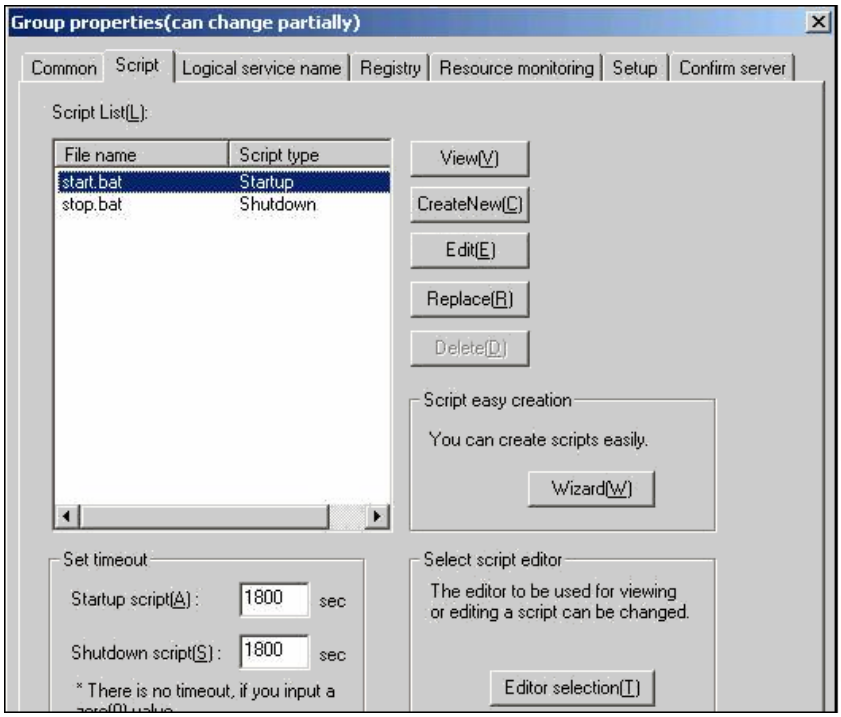
2. Select the NEC Group that the ARCserve server is deployed in, and locate the corresponding ARCserve cluster resources. Right-click on each ARCserve cluster resource and from the pop-up menu, select Property.

   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:

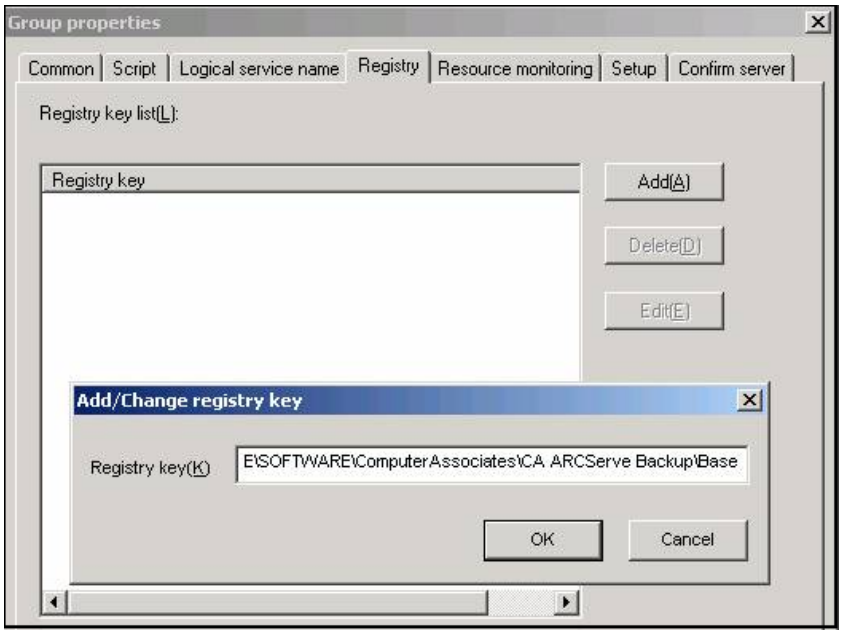
   ```
   SET process=1
   ```

   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 and click OK.

   The Registry key is added to the Registry key list on the Group Properties dialog.

Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an NEC CLUSTERPRO Environment

This section describes the steps you must perform to upgrade from earlier software versions to the current release. Please ensure you are following the appropriate upgrade procedure:

- To upgrade BrightStor ARCserve Backup r11.5, including the latest service packs, in an NEC CLUSTERPRO cluster-aware environment, directly to r12.5, follow the steps in Upgrade CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO Environment (see page 180).
- To upgrade CA ARCserve Backup r12/r12.5, including the latest service packs, to r15 in an NEC CLUSTERPRO environment, follow this procedure.

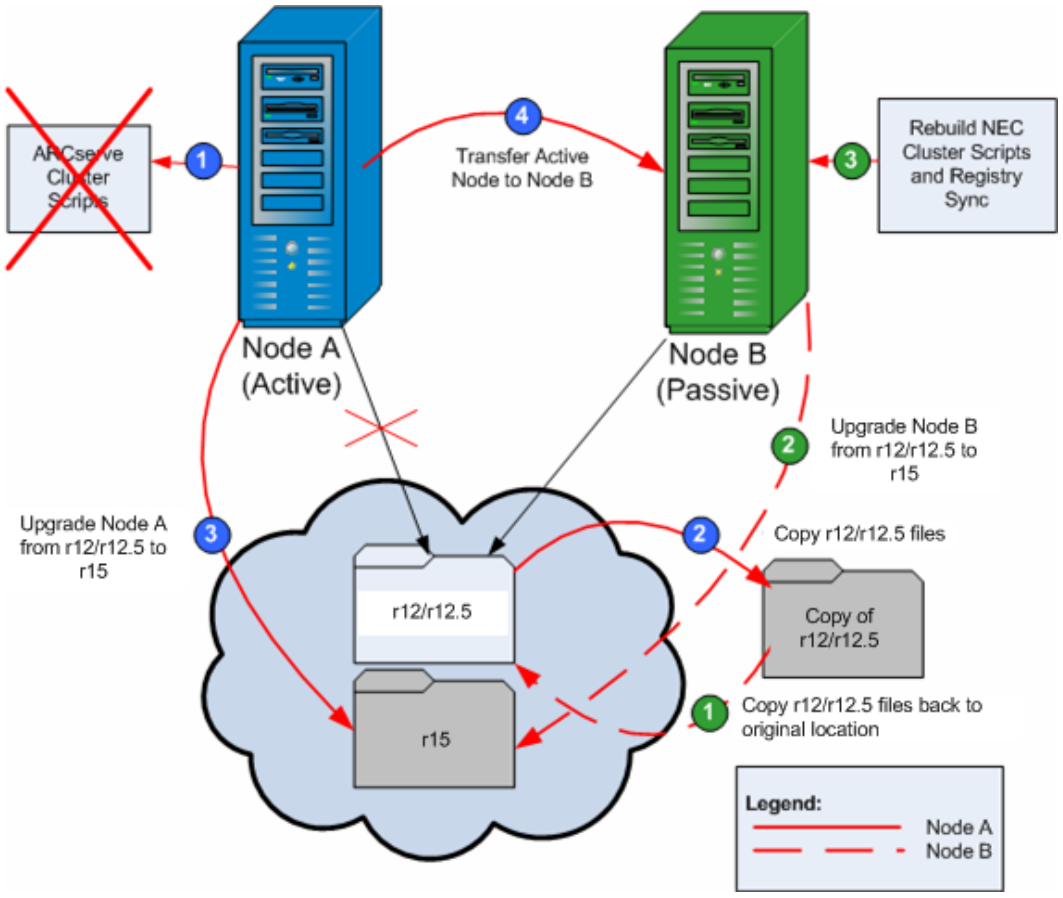
Before you begin, ensure you have read the information in Upgrade CA ARCserve Backup from a Previous Release (see page 97).

When upgrading CA ARCserve Backup from r12/r12.5 to r15 in an NEC CLUSTERPRO environment, the following procedure must be performed to safely protect your clustered backup data. If you are not already using CA ARCserve Backup r12/r12.5 in a cluster environment, you do not need to perform this procedure. The procedure supports the following CA ARCserve Backup r12/r12.5 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 r15 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 CA ARCserve Backup from r12/r12.5 to r15 in an NEC CLUSTERPRO environment

On Node A:

1. Disable the NEC Cluster Scripts and delete the Registry Sync. For more information, see Disable CA ARCserve Backup in NEC Cluster Scripts (see page 187).
2. Copy the CA ARCserve Backup r12/r12.5 installation directory files into a temporary location.

   A backup copy of the CA ARCserve Backup r12/r12.5 files is located in a different location from the original files.
3. Perform CA ARCserve Backup r15 upgrade installation for Node A. For more information, see Upgrade CA ARCserve Backup from a Previous Release (see page 97).

   The installation path location for the CA ARCserve Backup r15 upgrade must be the same location where r12 is currently installed.

   CA ARCserve Backup for Node A is upgraded from r12/r12.5 to r15. 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 CA ARCserve Backup r12/r12.5 installation directory files from the temporary location back into the original location.

   The CA ARCserve Backup r12/r12.5 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 CA 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 CA ARCserve Backup r15 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 CA ARCserve Backup from a Previous Release.

4. Rebuild the NEC Cluster Scripts and Registry Sync. For more information, see Enable CA ARCserve Backup in NEC Cluster Scripts.

   The new NEC HA scripts are created and the registry is synchronized.

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

More information:

How to Verify a Cluster-aware Installation and Upgrade (see page 198)

Uninstall CA ARCserve Backup from a NEC CLUSTERPRO/ExpressCluster

Uninstalling CA 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 CA ARCserve Backup from NEC CLUSTERPRO/ExpressCluster

1. Stop the cluster group. For more information, see Stop NEC Cluster Groups.
2. Remove the registry sync and edit the start.bat and stop.bat scripts to disable CA ARCserve Backup scripts added during installation. For more information, see Disable CA ARCserve Backup in NEC Cluster Scripts (see page 187).
3. 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 share disk so that you do not have to do a network copy later).

   Important! Make sure that the current node for the .dll files being backed up is set as the active node.

   The dynamic link library (.dll) files for CA ARCserve Backup are copied to a different location. This lets you uninstall CA ARCserve Backup from each node in the cluster.
4. From the Windows Control Panel, access the Add or Remove Programs utility, and remove CA ARCserve Backup from the current node.

   CA ARCserve Backup is removed from the current (active) node.
5. Copy the .dll files back into the original location in the ARCserve Backup directory.

   The .dll files for CA ARCserve Backup are copied back into the ARCserve Backup directory.
6. 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 will be changed to offline (passive) and the status of the next node within the cluster will be changed to online (active).
7. Repeat Steps 4 through 7 for all remaining nodes in the cluster.

   CA ARCserve Backup is removed from all nodes in the cluster.

How to Verify a Cluster-aware Installation and Upgrade

This section describes how to verify CA 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 CA ARCserve Backup services start properly, execute the cstop script to stop all CA ARCserve Backup services and then execute the cstart script to restart all CA ARCserve Backup services.

   Note: The cstop and cstart batch files are stored in the CA ARCserve Backup installation directory on the CA ARCserve Backup server. For more information about using cstop and cstart, see the *Administration Guide*.
3. Open the CA 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 CA 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. CA 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 CA ARCserve Backup with Other Products

This section contains the following topics:

CA Antivirus Integration (see page 199)
CA ARCserve Replication Integration (see page 199)
CA ARCserve Backup Patch Manager Integration (see page 200)

CA Antivirus Integration

CA Antivirus is bundled with CA 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: CA 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*.

CA ARCserve Replication Integration

CA ARCserve Replication and CA 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.

CA ARCserve Replication and CA ARCserve High Availability are separately-sold CA products.

For information about integrating CA ARCserve Backup with CA ARCserve Replication, see the *CA ARCserve Replication Integration Guide*.

CA ARCserve Backup Patch Manager Integration

CA ARCserve Backup Patch Manager is packaged with CA ARCserve Backup for Windows on the CA ARCserve Backup for Windows installation media. You can install CA ARCserve Backup Patch Manager directly from the installation media using the CA ARCserve Backup for Windows Installation Browser.

For information about using CA ARCserve Backup Patch Manager, see the documentation provided with CA ARCserve Backup Patch Manager. You can open the CA ARCserve Backup Patch Manager Readme and the CA ARCserve Backup User Guide directly from the CA ARCserve Backup Patch Manager Installation Browser.

Chapter 7: Configuring CA ARCserve Backup

This chapter describes how to configure the CA ARCserve Backup base product. For information about how to configure CA 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 201)
CA ARCserve Backup Home Page (see page 203)
First-Time Home Page and User Tutorial (see page 207)
Service State Icons (see page 208)
Log in to CA ARCserve Backup (see page 208)
Specify CA ARCserve Backup Manager Preferences (see page 210)
Code Pages (see page 212)
CA ARCserve Backup System Account (see page 214)
Configure the Windows Firewall to Optimize Communication (see page 216)
Start the CA ARCserve Backup Database Protection Job (see page 219)
Fine-Tune the CA ARCserve Backup SQL Server Database (see page 220)
Configure Devices Using the Device Wizard (see page 222)
Configure Enterprise Module Components (see page 223)
Configure Global Dashboard (see page 223)
Create File System Devices (see page 232)
How to Define Include and Skip Parameters for CA ARCserve Backup Database Agents (see page 235)
Configuring Your Firewall to Optimize Communication (see page 236)

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 CA ARCserve Backup servers and domains.

This release of CA ARCserve Backup provides you with a redesigned Manager Console. If you are running an older release of CA 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:

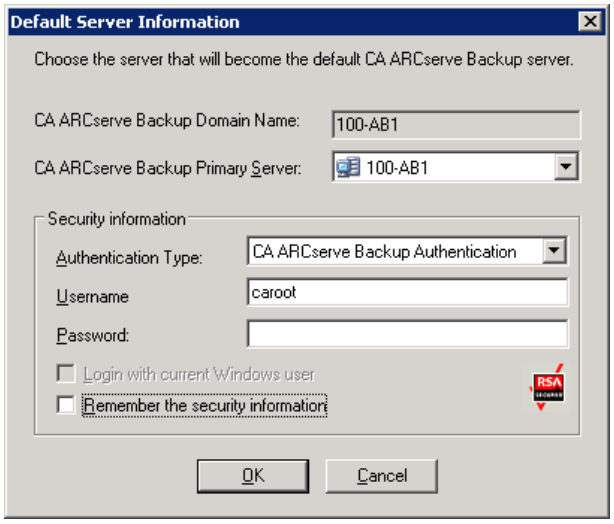
   - To access a server running this release of CA ARCserve Backup, click the Windows Start button, point to Programs, CA, ARCserve Backup, and click Manager.
   - To access an ARCserve server running a previous release, browse to the following file:

     C:\Programs Files\CA\ARCserve Backup\ARCserveMgr.exe

     Double-click ARCserveMgr.exe.
   - If you installed a previous CA ARCserve Backup release in the default installation directory, and used the installation process to upgrade CA 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 CA 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 CA ARCserve Backup Primary Server list.



3. To change the user, select either CA ARCserve Backup Authentication or Windows Authentication and specify a user name and password.

   By default, CA 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, CA ARCserve Backup prompts you to provide CA ARCserve Backup security credentials the first time you open managers, wizards, and so on, and you must provide a CA 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 CA 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.

CA ARCserve Backup Home Page

The Home Page is the central location from which you can log in to other CA ARCserve Backup servers and access all of the CA ARCserve Backup managers, wizards, and utilities.

Default Server and Security

Displays the following information about the CA 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 CA ARCserve Backup primary or stand-alone server, see Log On to CA ARCserve Backup (see page 208).

- View a summary of the user and the user's roles when a Windows user is logged into CA 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 CA 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 CA ARCserve Backup Managers:

- **Job Status Manager--**Lets you monitor jobs and view logs.
- **Backup Manager--**Lets you configure and submit backup jobs.
- **Restore Manager--**Lets you perform complete data recovery.
- **Server Admin--**Lets you manage CA 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 CA 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 CA ARCserve Backup reports.
- **Dashboard**--Lets you access a snapshot overview of your backup infrastructure.

Protection and Recovery

Lets you open the following managers and wizards:

- **Backup Manager--**Lets you configure and submit backup jobs.
- **Restore Manager--**Lets you perform complete data recovery.
- **CA ARCserve Replication--**Lets you start or install CA ARCserve Replication. CA 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 CA ARCserve Replication. For information, see the *CA 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 CA ARCserve Backup engines. For example, the Database Engine, the Job engine, and the Tape engine.
- **Central Agent Admin--**Lets you manage CA ARCserve Backup agents.
- **Device Manager--**Lets you manage the storage devices in your environment.
- **Device Configuration--**Lets you configure your storage devices in your CA ARCserve Backup environment.
- **Device Wizard--**Lets you perform media operations.
- **Device Group Configuration--**Lets you configure the device groups in your CA 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 CA ARCserve Backup environment.
- **Database Manager--**Lets you manage and maintain the CA ARCserve Backup database.
- **Alert Manager--**Lets you create alert notifications about events that occur during a backup.
- **User Profile--**Lets the CA ARCserve Backup administrator manage user profiles and provide access to CA ARCserve Backup.
- **Agent Deployment--**Launches the Agent Deployment tool, which lets you install and upgrade CA ARCserve Backup agents on remote hosts.

Utilities

Lets you open the following wizards and utilities:

- **Job Scheduler Wizard--**Lets you control CA ARCserve Backup command line utilities.
- **Create Boot Kit--**Lets you create disaster recovery boot disk sets. This link is active when you install the CA ARCserve Backup Disaster Recovery Option.

  Note: For more information, see the *Disaster Recovery Option Guide.*
- **Diagnostic Wizard--**Lets you gather information from CA ARCserve Backup system logs. The information gathered can be used for troubleshooting and may help CA Technical Support identify issues.
- **Merge--**Lets you merge session information from media into the CA 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:

- **CA ARCserve Backup on the Web--**Links you to the CA site that provides product information about CA ARCserve Backup.
- **Understanding your Support--**Provides maintenance and support information by product.
- **Registering for Support--**Provides an online form to register for CA Support Online.
- **Accessing Technical Support--**Offers the latest CA 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--**Allows you to take a short survey, provide feedback for new product development, and sign up for your local user community group.

Quick Reference

The Quick Reference section provides access to the following documentation:

- **Readme--**This document contains last minute updates and information that supplement the online help or the documentation.
- **Release Summary--**This document contains a summary of the new features added and enhancements made to CA 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 CA 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 CA 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 three 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 CA ARCserve Backup

When you open the CA ARCserve Backup Manager Console, you must log in to CA ARCserve Backup. The first time you log in to CA 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 CA ARCserve Backup using the Windows account that was provided when you installed CA 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.

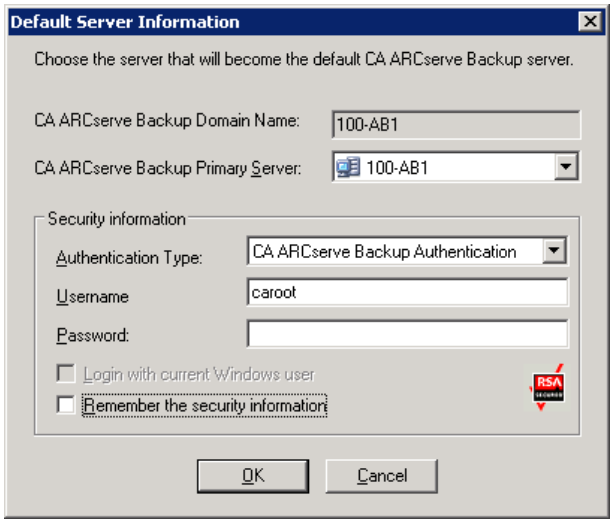
To log in to CA ARCserve Backup

1. Open the CA 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 CA 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 CA ARCserve Backup Primary Server list.



3. To change the user, select either CA ARCserve Backup Authentication or Windows Authentication and specify a user name and password.

   By default, CA 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, CA ARCserve Backup prompts you to provide CA ARCserve Backup security credentials the first time you open managers, wizards, and so on, and you must provide a CA 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 CA 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 CA ARCserve Backup Manager Preferences

CA ARCserve Backup lets you configure how the CA ARCserve Backup Manager windows behave. From the Preferences dialog, you can specify global and library filter options.

To specify CA ARCserve Backup Manager preferences

1. From the Windows Start menu, open the CA ARCserve Backup Manager Console by clicking Start, Programs, CA, ARCserve Backup, and selecting Manager.

   The CA 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 CA 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 CA 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, CA 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 CA 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 CA 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 CA ARCserve Backup supports the use of multiple code pages.

This section contains the following topics:

How CA ARCserve Backup Supports Multiple Code Pages (see page 212)
Specify Code Pages in the Backup Manager Window (see page 213)
Specify Code Pages in the Restore Manager Window (see page 214)

How CA ARCserve Backup Supports Multiple Code Pages

A code page is a map of characters as they relate to a particular language. If the CA 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 CA 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, CA ARCserve Backup applies the characteristics of the code page to all child volumes, directories, and so on. Although code pages do not affect CA ARCserve Backup functionality, CA 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 CA 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.

   CA 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 CA 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.

   CA ARCserve Backup applies the new code page settings immediately.

CA ARCserve Backup System Account

The CA ARCserve Backup System Account is the account CA ARCserve Backup uses to perform various storage-related functions on the local server. Local backup or restore jobs use the CA ARCserve Backup System Account as the security to run the job.

The CA ARCserve Backup System Account is entered into the System Account dialog when CA 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 CA 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 CA ARCserve Backup Manages Authentication

CA 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 CA ARCserve Backup server may be different from the security required when backing up a domain resource.

CA 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 CA ARCserve Backup installation disk or you can download the guides from the CA support website.

How to Use the System Account for Job Security

Typically, when you implement CA ARCserve Backup you give the CA 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 CA 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 CA ARCserve Backup System Account that exceed the local administrator and backup operator.

Configure the Windows Firewall to Optimize Communication

When the CA ARCserve Backup server is running the following operating systems, the Windows Firewall blocks communication to all ports used by CA ARCserve Backup. The operating systems affected are:

- Windows Server 2003 Service Pack 1 with the Windows Firewall enabled.
- Windows Server 2008 with the Windows Firewall enabled.
- Windows Server 2008 systems that were converted to a Domain Controller server after you installed CA ARCserve Backup.

To enable CA ARCserve Backup to communicate properly on these operating systems, you must perform one of the following procedures:

Note: Method 1 is the recommended procedure.

(Method 1) To configure the Windows firewall to optimize communication

1. Open Windows Firewall and ensure Windows Firewall is enabled.

2. Add the following executables, as applicable for your installation, to the Windows Firewall Exceptions list:

   Note: The following executables reside in the CA ARCserve Backup home directory, unless otherwise noted.

   - CA ARCserve Communication Foundation
   - ca_backup.exe
   - ca_restore.exe
   - caauthd.exe
   - cadiscovd.exe
   - carunjob.exe
   - casdscsvc.exe

     Note: This executable resides in the following directory:

     \CA\SharedComponents\ARCserve Backup\CADS
   - caserved.exe
   - CASMgmtSvc
   - catirpc.exe

     Note: This executable resides in the following directory:

     \CA\SharedComponents\ARCserve Backup\ASPortMapper
   - dbeng.exe
   - java.exe
   - jobeng.exe
   - ldbserver.exe
   - lqserver.exe
   - mediasvr.exe
   - msgeng.exe
   - tapeeng.exe
   - univagent.exe (if the Client Agent is installed)

   Note: If you have the Client Agent or any database agent installed, on the Exceptions tab, you must select the File and Printer Sharing option.

   Click OK and close the Windows Firewall dialog.

   Your new settings are saved.

3. Restart the computer and then start the CA ARCserve Backup services.

(Method 2) To configure the Windows firewall to optimize communication

Important! This method disables Windows Firewall.

1. Open Windows Firewall and disable the firewall.

   Click OK and close the Windows Firewall dialog.

   Your new settings are saved.

2. Restart the computer and then start the CA ARCserve Backup services.

Allow Database Agents that Reside on Remote Subnets to Communicate with the ARCserve Server

This scenario applies to CA ARCserve Backup servers running the following operating systems:

- Windows Server 2003 with Service Pack 1 and the firewall is enabled
- Upgrades from Windows XP to Windows XP Service Pack 2 (the upgrade process enables the firewall by default)

When a CA ARCserve Backup database agent is installed on a server that resides in a different subnet than the CA ARCserve Backup server, and the Windows firewall is running on the agent server with the default port settings, the CA ARCserve Backup server cannot communicate with the agent system using ports 445 and 139. As a result, backups for these systems will fail with error message E8602. The affected database agents are as follows:

- Agent for Informix
- Agent for Lotus Domino
- Agent for Oracle
- Agent for Sybase
- Enterprise Option for SAP R/3 for Oracle

The following procedure describes how to modify the default firewall settings which will allow database agents that reside on remote subnets to communicate with the CA ARCserve Backup server.

To allow CA ARCserve Backup database agents the reside on remote subnets to communicate with the ARCserve server

1. From the Windows Start menu select Run.

   The Run dialog opens.

2. In the Open field, specify the following:

   firewall.cpl

   The Windows Firewall dialog opens.

3. Click the Exceptions tab.

   Click File and Printer Sharing and then click the Edit button.

   The Edit a Service dialog opens.

4. Double-click TCP 139.

   The Change Scope dialog opens.

5. Select the Click Any Computer (including those in the Internet) option and click OK.

   Double-click TCP 445.

   The Change Scope dialog opens.

6. Select the Click Any Computer (including those in the Internet) option and click OK.

   Click OK to close the Edit a Service dialog.

   Click OK to close the Windows Firewall dialog.

   The database agents can now communicate with the ARCserve server.

Start the CA ARCserve Backup Database Protection Job

The CA ARCserve Backup database maintains job, media, and device information on your system. After you install CA ARCserve Backup, the Database Protection Job maintains a status of Hold. To use the Database Protection Job to protect the CA ARCserve Backup, you must change the status of the Database Protection Job from Hold to Ready.

To start the CA ARCserve Backup Database Protection Job

1. Open the CA ARCserve Backup Manager Console.

   From the Quick Start menu on the CA 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 CA 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 CA 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 221)
Database Consistency Checks (see page 221)
Specify ODBC Communication for Remote Database Configurations (see page 221)

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 CA ARCserve Backup server running that uses Microsoft SQL as its database, you can redirect the local database to the remote machine. CA 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 CA 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 CA 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 CA 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 CA ARCserve Backup Enterprise Module. With Enterprise Option Configuration you can configure the following devices and applications:

- StorageTek ACSLS libraries
- IBM 3494 libraries
- The CA ARCserve Backup Image Option
- The CA ARCserve Backup Serverless Backup 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 CA 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

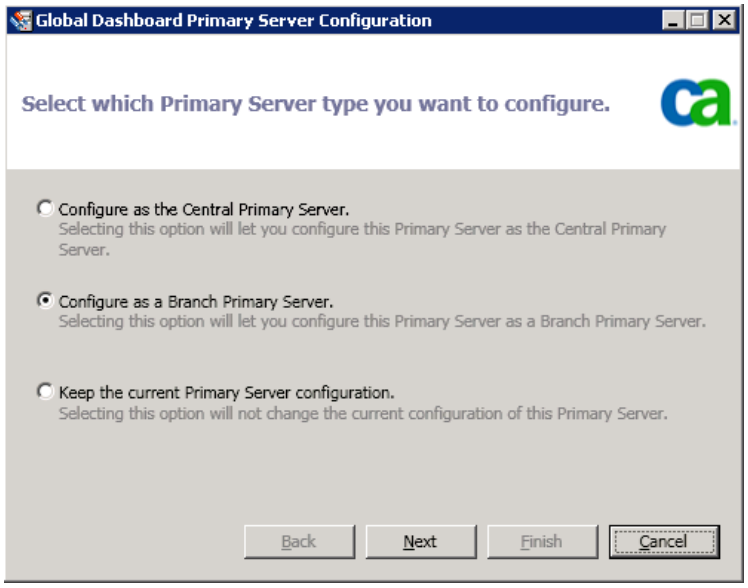
For Global Dashboard to work properly, it is important that the configuration process be performed at the central site and at each associated branch site to enable the necessary communication and synchronization of dashboard-related data from the branch site to the central site. You can configure the 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 CA 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 CA 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 CA 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 and capable of storing dashboard data received from all registered Branch Primary Servers.
- Any primary server (or stand-alone server) within your CA 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 CA 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

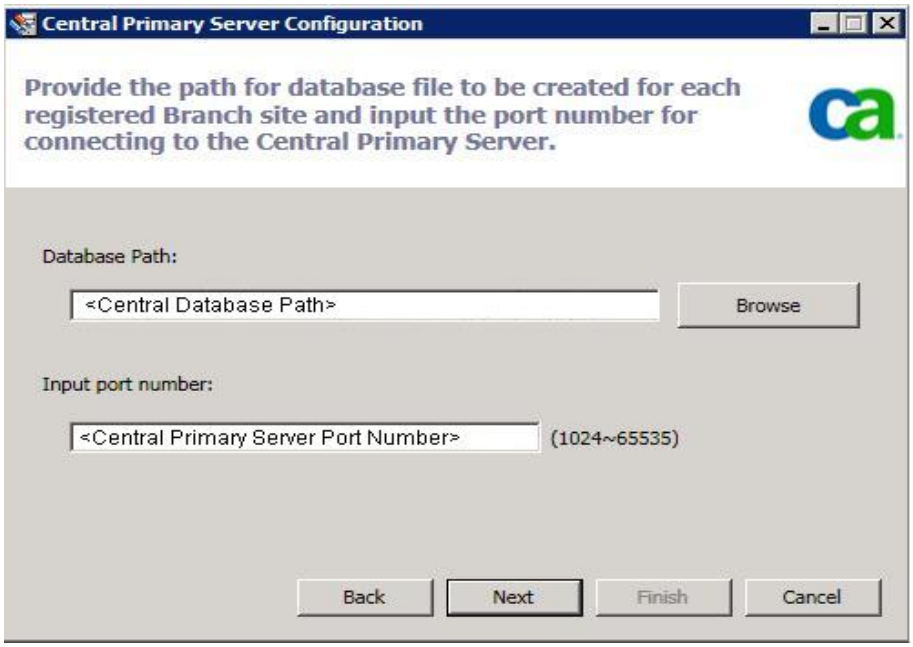
The parameters specified during the configuration of the central site must be used by each registered branch site to enable synchronization of dashboard-related data to the central site.

Note: The local CA 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.



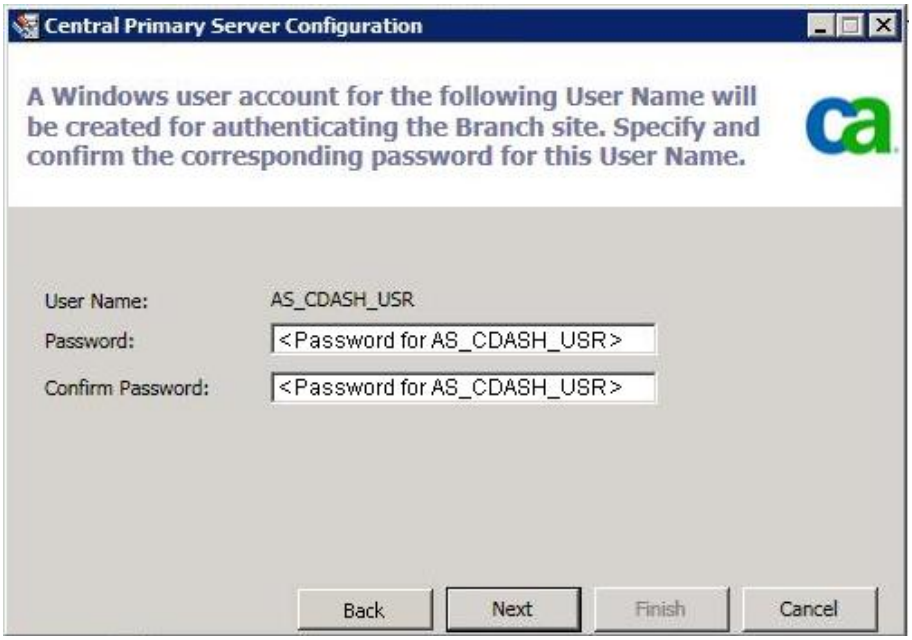
2. Specify the path for the central site database. (This will be the database location where the dashboard-related data from each branch site will be uploaded to and stored).

   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.

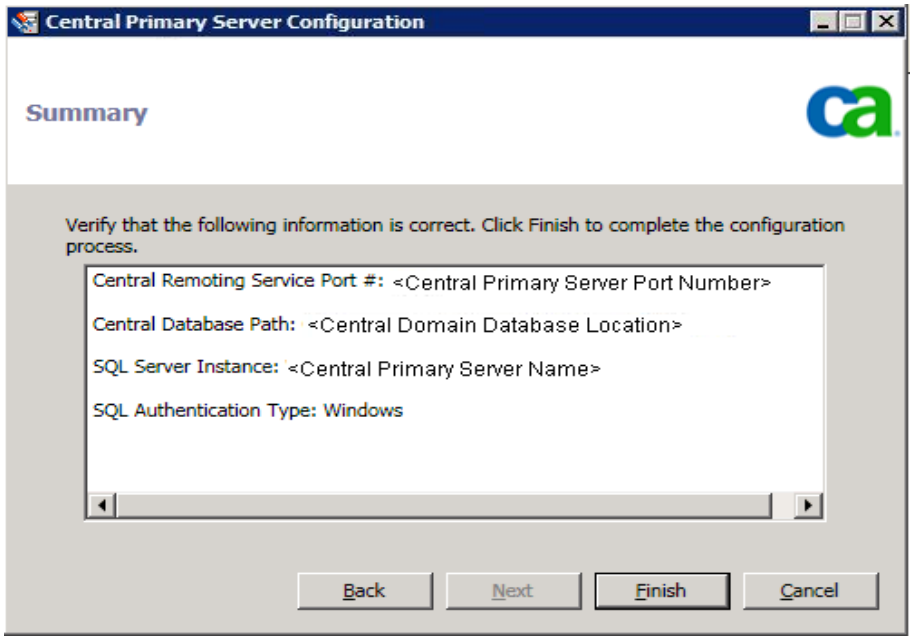
   This password is needed when each branch site wants to register to the Central Primary Server. If necessary, this password can be reset using the Windows User Management. However, if the password is changed, the new information must be manually reset at every branch site that is registered to this Central 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 CA 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 CA 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 CA 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 CA 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

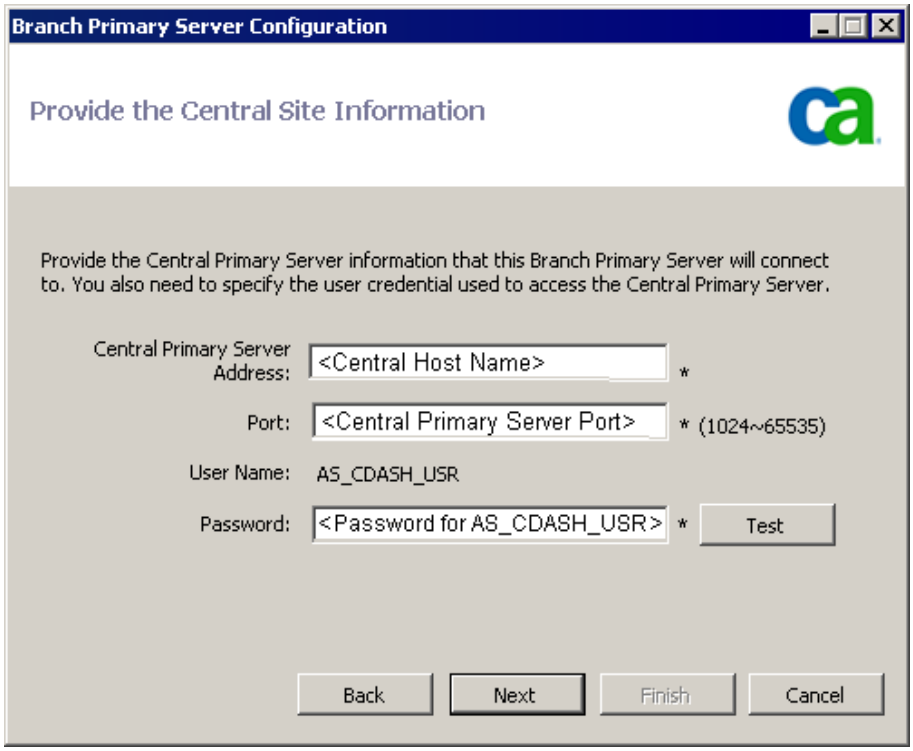
A branch site must be registered to the central site to enable synchronization of dashboard-related data to that central site. A branch site can only report to one Central Primary Server. To register your branch site, you must first configure it to communicate with the central site.

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.



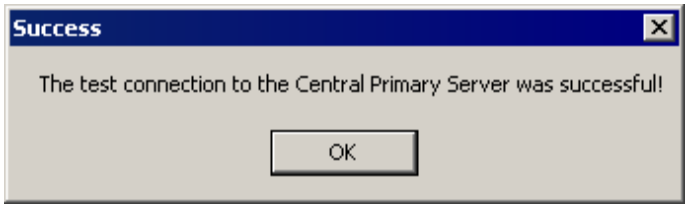
2. Specify the name of the Central Primary Server, the Port number to the Central Primary Server, and the authentication Password.

   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 225).

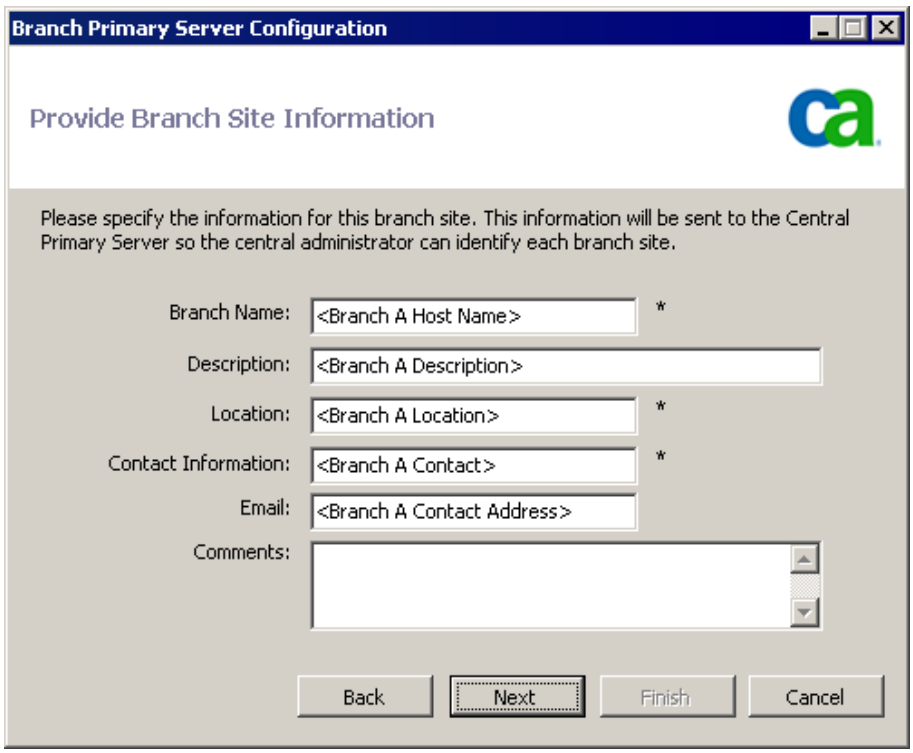
3. Click Test to verify proper connection to the central site.

   A test connection status message will appear.



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.

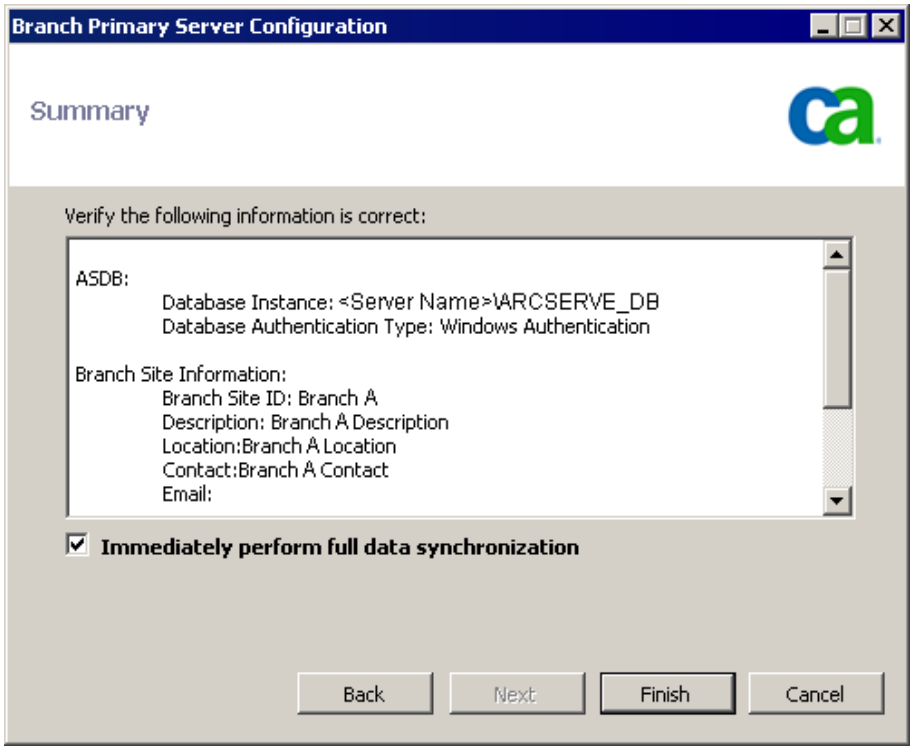
   Click Next to continue.

   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 CA 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 CA 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 CA 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 CA 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. CA 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, CA 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 CA 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. CA 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 CA ARCserve Backup and can also be accessed from the Help menu on the menu bar.

How to Define Include and Skip Parameters for CA ARCserve Backup Database Agents

CA 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 CA 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 CA ARCserve Backup does not support brick level backups on Microsoft Exchange Server databases. In previous releases of CA ARCserve Backup, the SkipDSAFiles registry key was used to define the include and skip value for brick level backups.

Configuring Your Firewall to Optimize Communication

In an environment where you are using multiple CA 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 CA ARCserve Backup servers must match your firewall configuration so that CA ARCserve Backup servers can communicate with each other.

A CA ARCserve Backup server communicates with other CA 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 CA 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

Ports Configuration File Guidelines

The following guidelines apply to modifying the ports configuration file:

- Changing port numbers requires the CA ARCserve Backup ServiceName.

  Note: For more information about service names, see Additional Resources - Firewall Ports Specifications (see page 259).

- 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 CA ARCserve Backup service name (ServiceName). CA 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 CA ARCserve Backup use system-assigned ports for all CA ARCserve Backup RPC-based services.
- Changing the port configuration file on one CA ARCserve Backup server for MSRPC-based services does not ensure that CA ARCserve Backup applies the changes to all remote CA ARCserve Backup servers. You should modify the port configuration file on all remote CA 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 CA 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 CA ARCserve Backup services, you can run cstop and cstart to stop and start the services.

To support backward compatibility, the keys corresponding to CA 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 CA ARCserve Backup database agents send jobs to the CA 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 CA 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 CA ARCserve Backup Components

The following sections provide information about ports used by CA ARCserve Backup components, primarily for Windows configurations.

This section contains the following topics:

External Ports Used for Communication (see page 239)
Ports Used by the CA ARCserve Backup Base Product (see page 240)
Ports Used by CA ARCserve Backup Common Components (see page 248)
Ports Used by CA ARCserve Backup Agents and Options (see page 249)
How to Allow Agents and Database Agents to Communicate through a Firewall (see page 254)
CA ARCserve Backup Dashboard for Windows Firewall Communication Configuration (see page 258)
Additional Resources - Firewall Ports Specifications (see page 259)

External Ports Used for Communication

CA 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 CA ARCserve Backup MSRPC services register their current ports with this service.

All CA ARCserve Backup clients (for example, the Manager) contact this service to enumerate the actual port used by the CA ARCserve Backup service and then contact the service directly.

Port 139/445

This is owned by Microsoft and is not a configurable port. CA 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 CA ARCserve Backup services are installed on Windows NT.
- Port 445 is used only when the CA ARCserve Backup services are installed on Windows 2000, 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. CA 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 CA ARCserve Backup Base Product

For the CA 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 CA ARCserve Backup domain concept. This service is required for GUI communication.

- Default Port: Dynamic Port
- Protocol: TCP

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

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 CA 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 CA 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 CA 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 CA 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 CA 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 CA 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 CA ARCserve Backup Job Queue.

- Default Port: 6503
- Protocol: TCP
- Appears in PortsConfig.cfg as: jobengine

DB Engine (dbeng.exe)

Provides database services for CA 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 CA ARCserve Backup products.

- Default Port: 6502
- Protocol: TCP
- Appears in PortsConfig.cfg as: tapeengine

Discovery Service (casdscsvc.exe)

Lets the CA ARCserve Backup server discover CA 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 CA ARCserve Backup Agents and Options

The CA 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 CA ARCserve Backup Agents and Options (see page 249).

Ports Used by CA ARCserve Backup Common Components

The following sections provide information about the ports used by CA ARCserve Backup common components.

Discovery Service Communication Ports

The Discovery Service discovers CA 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 CA ARCserve Backup receive data and send responses about CA ARCserve Backup products running in your environment.

- Default Port: 41524
- Protocol: UDP

Discovery response

Lets CA ARCserve Backup receive data about CA ARCserve Backup products running in your environment.

- Default Port: 41523
- Protocol: TCP

Discovery broadcast

Lets CA ARCserve Backup broadcast its own CA 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 CA ARCserve Backup Agents and Options

The following sections provide information about the ports used by CA 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 252).

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 CA 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 2000, 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 2000, 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

CA ARCserve Backup Database Agents Communication Ports

For CA 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 2000, 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 CA ARCserve Backup Agents

The CA 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 CA ARCserve Backup Agents and Options (see page 249).

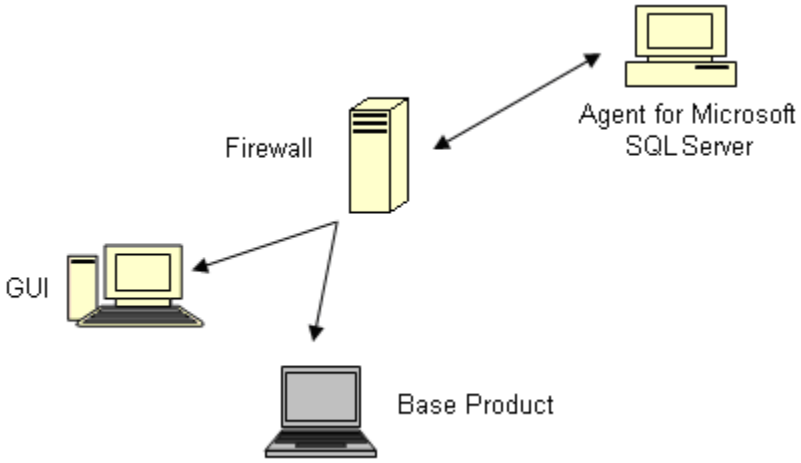
How to Allow Agents and Database Agents to Communicate through a Firewall

The following sections provide examples about allowing CA ARCserve Backup agents and database agents to communicate through a firewall.

Base Product Communicating with the Agent for Microsoft SQL Server

Note: The information contained in this topic applies to BrightStor ARCserve Backup r11.5 Agent for Microsoft SQL Server and older releases of the agent.

In the following scenario, the agent is behind a firewall. The GUI and base product are outside the firewall on different machines:



On the machine with the Agent for Microsoft SQL Server, modify the Portsconfig.cfg file to contain the following entries:

```
ENABLE_CONFIGURABLE_PORTS=1
Dbagentsrpcserver   6071
Sqlagenttcpservice  6070
casdscsvctcp        41523
casdscsvcudp        41524
```

On the firewall, open these four ports and additional port 135. Port 139 or Port 445 must be opened only if the Agent for Microsoft SQL Server is configured to use the Named Pipes transport. They should allow incoming connections to the agent machine.

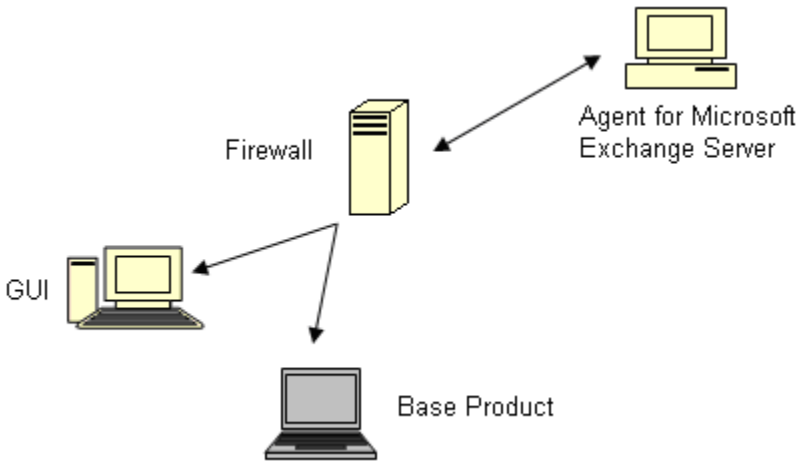
On the machine where the base product is running and the GUI-only machine, add the following entries to the existing Portsconfig.cfg file:

```
ENABLE_CONFIGURABLE_PORTS=1
Dbagentsrpcserver   6071   SQLAgentMachineName
Sqlagenttcpservice  6070   SQLAgentMachineName
casdscsvctcp        41523
casdscsvcudp        41524
```

GUI Managing the Agent for Microsoft Exchange Server Using Named Pipes

Note: The information contained in this topic applies to BrightStor ARCserve Backup r11.5 Agent for Microsoft Exchange Server and older releases of the agent.

In the following scenario, the agent is behind a firewall, and the GUI and base product are outside the firewall on different machines:



On the machine with the Agent for Microsoft Exchange Server, modify the Portsconfig.cfg file to contain the following entries:

```
ENABLE_CONFIGURABLE_PORTS=1
Dbagentsrpcserver        6071
casdscsvctcp            41523
casdscsvcudp             41524
```

On the firewall, open these four ports and additional port 135. Port 139 or Port 445 must be opened. They should allow incoming connections to the agent machine.

On the GUI machine, modify the Portsconfig.cfg file to contain the following entries:

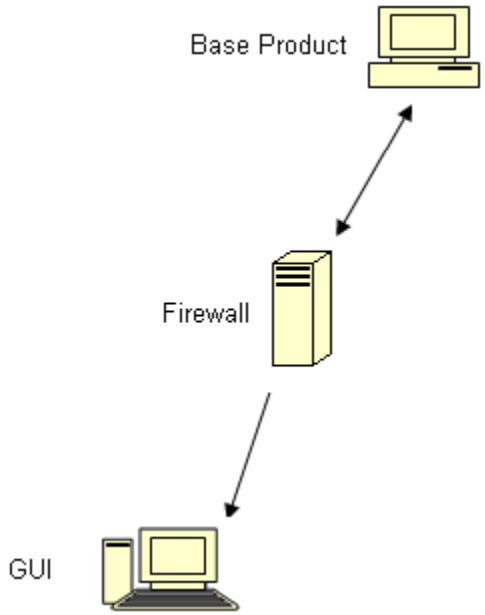
```
ENABLE_CONFIGURABLE_PORTS=1
Dbagentsrpcserver        6071    ExchangeAgentMachineName
```

On the machine where the base product is running, add the following entries to the existing Portsconfig.cfg file:

```
ENABLE_CONFIGURABLE_PORTS=1
exchangeagenttcpserverlevel 6074    ExchangeAgentMachineName
casdscsvctcp            41523
casdscsvcudp             41524
```

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
```

CA ARCserve Backup Dashboard for Windows Firewall Communication Configuration

The installation wizard configures the firewall communication ports between CA ARCserve Backup server and the client system when you install CA ARCserve Backup and CA 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 CA 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>
    CA Portal6052</port>
    </service>
```

CA ARCserve Backup Server System

The CA 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 CA 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 CA ARCserve Backup services that you can configure using the ports configuration file:

CA 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

Service Display Name	Process Name	Key	Default Port	Service Type
Job Engine	jobeng.exe	jobengine	6503	MSRPC
Database Engine	dbeng.exe	databaseengine	6504	MSRPC
Message Engine	msgeng.exe	rtcports	System port	MSRPC

CA 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

CA ARCserve Backup ONCRPC Services

Service Display Name	Process Name	Key	Default Port	Service Type
Remote Procedure Call Server	CASportmap.exe	CASportmap	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

CA 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
  ```

- Machine A and D are CA ARCserve Backup servers. Machine B and C are Client Agent machines. If you want to change the communication port between machine A and B to 7000, you can set the communication port between A and C to the default, 6050. Also, on machine A, there is a client agent installed for the CA 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, add the following lines to the PortsConfig.cfg file:

  ```
  fsbackupservice      7000   MachineB

  fsbackupserviceudp          7000    MachineB
  ```

  Be aware of the following:

  - You can perform this change using the Admin.exe application installed by the client agent.
  - You must restart the Universal Agent service.

- Machine A and D are CA ARCserve Backup servers. Machine B and C are client agent machines. If you want machine A to browse and back up files on machine B, add the following to PortsConfig.cfg file:

  fsbackupservice 7000 MachineB

  fsbackupserviceudp 7000 MachineB

  To allow the client agent from machine A to communicate with the CA ARCserve Backup machine D, add the following lines to the PortsConfig.cfg file on machine A:

  fsbackupservice 8000 MachineA

  fsbackupserviceudp 8000 MachineA

  You must restart the Universal Agent on machine A.

  Note: You can apply this logic to the CA ARCserve Backup Agent for Microsoft SQL Server (sqlagenttcpservice) for TCP-based services (fsbackupservice, sqlagenttcpservice).

- For CA 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 CA ARCserve Backup Agent RPC Server will try to use port 9000.

  dbagentsrpcserver 9000;9001

  This setting means that the CA 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 CA ARCserve Backup will write a message in the Windows Application Activity Log.

  dbagentsrpcserver 9000-9500

  This setting means that the CA ARCserve Backup Agent RPC Server tries to communicate using port 9000. If it does not succeed CA 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:

Note: The PortsConfig.cfg file is stored in the following directory:

\Program Files\CA\SharedComponents\ARCserve Backup

- If you want to change the Network Attached Storage (NAS) port on the CA ARCserve Backup server, after installing the CA ARCserve Backup NDMP NAS Option, you must change the port assignment on the NAS filer as well.
- 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 CA 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, CA 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, CA 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 CA ARCserve Backup Client Agent, the CA ARCserve Backup Agent for Microsoft Exchange Server, and the CA ARCserve Backup NDMP NAS Option). If you add a machine with a Windows NT, Windows 2000, Windows XP, or Windows Server 2003 operating system, browsing functionality is performed through the Universal Agent.
- Changing the ports for the CA ARCserve Backup Agent for Microsoft Exchange Server and the CA ARCserve Backup Agent for Microsoft SQL Server is for TCP backups for these agents. The RPC server lets you browse all CA ARCserve Backup for Windows database agents.

- If you are upgrading from an older version of CA ARCserve Backup and your current installation uses a configuration file labeled CAPortConfig.cfg for CA ARCserve Backup Client Agents configurations, the installation process migrates CAPortConfig.cfg settings to the PortsConfig.cfg file.

  For previous CA 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 CA ARCserve Backup

This section contains the following topics:

Uninstall CA ARCserve Backup (see page 265)
Uninstall CA ARCserve Backup Components Using the Command Line (see page 268)
Uninstall Agent Deployment Setup Files (see page 271)

Uninstall CA ARCserve Backup

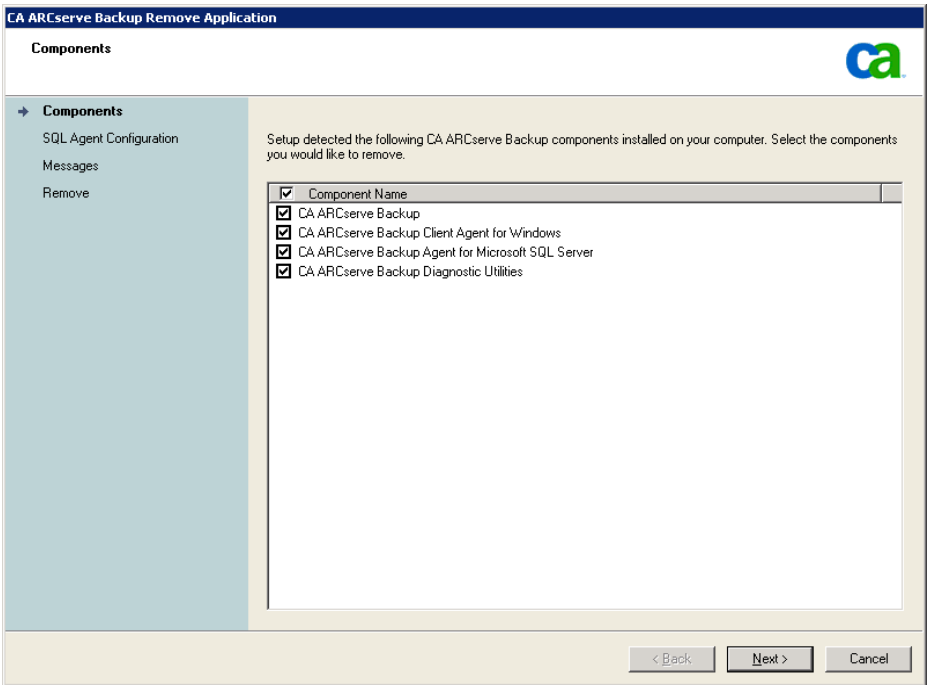
You can uninstall CA ARCserve Backup using the Add and Remove Programs application located in the Windows Control Panel.

To ensure that CA ARCserve Backup is completely uninstalled from your system, you should uninstall all CA ARCserve Backup components that appear in the Uninstall Components dialog. For example, you should uninstall CA ARCserve Backup Client Agent for Windows, CA ARCserve Backup Agent for Microsoft SQL Server, CA ARCserve Backup Diagnostic Utilities, and so on.

You can uninstall the following CA ARCserve Backup components from Windows Add or Remove Programs:

- CA ARCserve Backup (base product)
- CA ARCserve Backup Agent for Informix
- CA ARCserve Backup Agent for Lotus Domino
- CA ARCserve Backup Agent for Microsoft Exchange Server
- CA ARCserve Backup Agent for Microsoft SharePoint Server
- CA ARCserve Backup Agent for Microsoft SQL Server
- CA ARCserve Backup Agent for Open Files for Windows
- CA ARCserve Backup Agent for Oracle
- CA ARCserve Backup Agent for Sybase
- CA ARCserve Backup Agent for Virtual Machines
- CA ARCserve Backup Client Agent for Windows
- CA ARCserve Backup Diagnostic Utility

- CA ARCserve Backup Disaster Recovery Option
- CA ARCserve Backup Enterprise Module
- CA ARCserve Backup Enterprise Option for SAP R/3 for Oracle
- CA ARCserve Backup Global Dashboard
- CA ARCserve Backup Image Option
- CA ARCserve Backup NDMP NAS Option
- CA ARCserve Backup Serverless Backup Option



Use the Server Admin Manager to uninstall the following CA ARCserve Backup components:

- CA ARCserve Backup Central Management Option
- CA ARCserve Backup Tape Library Option
- CA ARCserve Backup Storage Area Network (SAN) Option

The uninstallation routine removes all CA 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-1.6.0

  If you upgraded from a previous CA 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 1.6.0 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 CA 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 CA ARCserve Backup in a cluster, you can safely delete this directory after CA ARCserve Backup is uninstalled from the last cluster node.

To uninstall CA ARCserve Backup

1. Close the CA 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 CA ARCserve Backup.

   Click Remove.

   The Components dialog opens.

4. Select the CA ARCserve Backup components that you want to uninstall and click Remove.

   The CA ARCserve Backup components specified are uninstalled from your computer.

Important! The uninstallation routine does not uninstall the CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

Uninstall CA 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 CA ARCserve Backup components, agents, and options using the Windows command line. For example, you need to uninstall the CA 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.

- CA ARCserve Backup Member server and supported options
- CA ARCserve Backup Agent for Open Files
- CA ARCserve Backup Agent for Virtual Machines
- CA ARCserve Backup Client Agent for Windows
- CA ARCserve Backup for Windows Disaster Recovery Option

Important! The procedure that follows describes the steps to uninstall all CA ARCserve Backup components from all Windows operating systems using the command line.

To uninstall CA ARCserve Backup components using the command line

1. Log in to the computer where you want to uninstall CA 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\r15\uninstall.exe /p <ProductCode>

   - **x64 operating systems:**

     %ProgramFiles%(x86)\CA\SharedComponents\ARCserve Backup\Setup\r15\uninstall.exe /p <ProductCode>

   <ProductCode>

   The table listed below defines the product code that you must specify for the CA ARCserve Backup component that you want to uninstall.

   Example:

   Use the following syntax to uninstall the CA ARCserve Backup base product from a Windows x86 operating system using the command line:

   %ProgramFiles%\CA\SharedComponents\ARCserve Backup\Setup\r15\uninstall.exe /p {CAABDF1F-E6BC-483F-B7E5-CEEF32EBE841}

Component	<ProductCode>
CA ARCserve Backup (x86 platforms)	{CAABDF1F-E6BC-483F-B7E5-CEEF32EBE841}
CA ARCserve Backup Agent for Informix (x86 platforms)	{CAABD973-463D-456C-84D3-9CBEA3118916}
CA ARCserve Backup Agent for Lotus Domino (x86 platforms)	{CAABD7B3-9037-44D6-BE1D-8F61DBDAFEF2}
CA ARCserve Backup Agent for Microsoft Exchange Server (x86 platforms)	{CAABD512-714D-4DA3-A5A7-7FEB2A9605F5}
CA ARCserve Backup Agent for Microsoft Exchange Server (x64 platforms)	{CAABD2C7-22CA-42B6-A1E7-987697879480}
CA ARCserve Backup Agent for Microsoft SharePoint Server (x86 platforms)	{CAABD6D4-2659-4371-83C0-00DB8526A2FE}

Component	<ProductCode>
CA ARCserve Backup Agent for Microsoft SharePoint Server (x64 platforms)	{CAABD3DF-7AB2-4631-A6C2-AE6153B56E34}
CA ARCserve Backup Agent for Microsoft SQL Server (x86 platforms)	{CAABD63E-96AC-4750-9B65-D7BDB499441E}
CA ARCserve Backup Agent for Microsoft SQL Server (x64 platforms)	{CAABD412-EFC0-45AD-AE7F-6A09675E94A7}
CA ARCserve Backup Agent for Microsoft SQL Server (Intel Itanium platforms)	{CAABD793-6202-4D9A-99E9-99A629CB6054}
CA ARCserve Backup Agent for Open Files for Windows (x86 platforms)	{CAABD6E7-6373-406C-9046-00EB1A6B8578}
CA ARCserve Backup Agent for Open Files for Windows (x64 platforms)	{CAABD5EB-4BC4-44D2-BE88-54C56F393DBF}
CA ARCserve Backup Agent for Open Files for Windows (Intel Itanium platforms)	{CAABD895-E93A-4244-96AE-5963009F6021}
CA ARCserve Backup Agent for Oracle (x86 platforms)	{CAABD5F5-1E0D-4818-8EFC-57873293516E}
CA ARCserve Backup Agent for Oracle (x64 platforms)	{CAABD26F-DAFE-494A-873F-0DB774782430}
CA ARCserve Backup Agent for Oracle (Intel Itanium platforms)	{CAABD98E-4890-4572-96BF-5B70AA7248C1}
CA ARCserve Backup Agent for Sybase (x86 platforms)	{CAABD17A-0D49-4EC3-A53B-8163432A3B56}
CA ARCserve Backup Agent for Virtual Machines (x86 platforms)	{CAABD355-F0C1-4605-AF1E-B7A6666C7D49}
CA ARCserve Backup Agent for Virtual Machines (x64 platforms)	{CAABD127-3C7B-4D96-A9BB-FC4A566D6136}
CA ARCserve Backup Client Agent for Windows (x86 platforms)	{CAABDBA1-02D7-49A4-9C2A-1B5BE1184517}
CA ARCserve Backup Client Agent for Windows (x64 platforms)	{CAABDB75-E0F2-44BB-AAE1-4D03EBF7F17B}
CA ARCserve Backup Client Agent for Windows (Intel Itanium platforms)	{CAABD4D6-641C-41EF-B76B-7BED859E86F5}
CA ARCserve Backup Diagnostic Utilities (x86 platforms)	{CAABD7EE-D20D-40B6-B7DB-C00A108A2441}
CA ARCserve Backup Disaster Recovery Option (x86 platforms)	{CAABD5C6-6B02-4966-A014-564265A15259}
CA ARCserve Backup Enterprise Module (x86	{CAABD24F-8E1F-401A-B034-024E8FDE28EB}

Component	<ProductCode>
platforms)	
CA ARCserve Backup Enterprise Option for SAP R3 for Oracle (x86 platforms)	{CAABDE6D-F471-4E47-A694-2D0B3B417694}
CA ARCserve Backup Enterprise Option for SAP R3 for Oracle (x64 platforms)	{CAABDD15-6242-436F-B577-9015CD250172}
CA ARCserve Backup Enterprise Option for SAP R3 for Oracle (Intel Itanium platforms)	{CAABD3F8-B8DC-43DC-B9E8-730801DB1466}
CA ARCserve Backup Global Dashboard	{A4D0BC77-BBE1-4708-A878-30D9BE778B2C}
CA ARCserve Backup Image Option (x86 platforms)	{CAABD962-195A-4B0F-8134-83247DF8AE0A}
CA ARCserve Backup Microsoft Windows EBS Option (x86 platforms)	{CAABD3CE-2BF1-4B56-8A64-887B848AF1CF}
CA ARCserve Backup NDMP NAS Option (x86 platforms)	{CAABDAB4-671F-406A-A779-5D431DDC471C}
CA ARCserve Backup Serverless Backup Option (x86 platforms)	{CAABD32D-AF04-406D-B0CB-732961EF02FA}

After the command executes, the CA ARCserve Backup component is uninstalled.

Uninstall Agent Deployment Setup Files

CA ARCserve Backup does not contain a routine that lets you uninstall Agent Deployment Setup Files. If you need to free disk space on the CA ARCserve Backup server, you can safely delete Agent Deployment Setup Files from the CA ARCserve Backup server without adversely affecting your CA 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 CA ARCserve Backup server.

   Note: The CA 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\r15\Uninstall.exe" /q /p {CAABD375-B0AA-4511-A384-439D5CBC6D94}

   - **x64 Platforms:**

     C:\Program Files (x86)\CA\SharedComponents\ARCserve Backup\Setup\r15\Uninstall.exe" /q /p {CAABD375-B0AA-4511-A384-439D5CBC6D94}

   Agent Deployment Setup Files are deleted from the CA ARCserve Backup server.

Note: To run Agent Deployment after the setup files are deleted from the CA ARCserve Backup server, do one of the following:

- Re-install Agent Deployment Setup Files using the CA ARCserve Backup installation media.
- Execute Agent Deployment and provide the CA ARCserve Backup installation media when prompted.

Appendix A: Troubleshooting Your Installation

This appendix contains information about troubleshooting your CA ARCserve Backup installation.

This section contains the following topics:

Setup Cannot Communicate with Remote Microsoft SQL Server Databases (see page 273)
Unable to Log In to CA ARCserve Backup After Installing This Release (see page 275)
CA ARCserve Backup Services Fail to Initialize (see page 276)
The Tape Engine Does Not Start on Member Server Upgrades (see page 277)
Unable to Log in to CA ARCserve Backup After Upgrading to This Release (see page 278)
Unable to Determine What Devices Are Supported by CA ARCserve Backup (see page 279)
Cluster HA Resources Not Created (see page 280)

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\system322

     - **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 CA ARCserve Backup After Installing This Release

Valid on Windows platforms.

Symptom:

After you perform a new installation of CA ARCserve Backup, you cannot log in to CA 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:

- CA ARCserve Backup Domain Server
- CA 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 CA ARCserve Backup Domain Server, and try to log in to the CA ARCserve Backup Manager Console again. If you still cannot log in, open the command window, change the directory to the CA 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 CA 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 CA 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 CA ARCserve Backup home directory under \log.

CA ARCserve Backup Services Fail to Initialize

Valid on Windows platforms.

Symptom:

Why are my CA ARCserve Backup services failing to initialize?

Solution:

CA 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 CA 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, CA 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

CA 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, CA ARCserve Backup services may try to initialize before the external portmapper has fully initialized. Under these circumstances, CA 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 CA ARCserve Backup services wait before initializing portmapper registration. For example, DelayedRegistration=1 causes all CA 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 CA ARCserve Backup engines, see the online help or the *Administration Guide*.

Unable to Log in to CA ARCserve Backup After Upgrading to This Release

Valid on Windows platforms.

Symptom:

User profiles do not migrate when you upgrade to this release of CA ARCserve Backup. As a result, the users cannot log in to the CA ARCserve Backup managers and domain.

Solution:

This problem only affects upgrades from previous releases of CA ARCserve Backup, such as CA ARCserve Backup r12 SP1 and CA 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 CA 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 CA 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 CA ARCserve Backup installation directory. For example:

C:\Program Files\CA\ARCserve Backup\caauthd.exe

Unable to Determine What Devices Are Supported by CA ARCserve Backup

Valid on Windows platforms.

Symptom:

What devices does CA ARCserve Backup support?

Solution:

Refer to the CA web site for a certified device list to confirm the firmware and model of the supported device. To access this information, open the CA ARCserve Backup Home Page and click the Accessing Technical Support link under Technical Support, as shown in the following illustration:

More information:

CA ARCserve Backup Home Page (see page 203)

Cluster HA Resources Not Created

Valid on Windows platforms running Microsoft Cluster Server (MSCS).

Symptom:

CA ARCserve Backup cannot create cluster HA resources.

Solution:

This problem presents itself after you install CA 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 CA 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 CA ARCserve Backup virtual name.
3. Specify the following:
   - **Share name:** ARCSERVE$
   - **Path:** The CA ARCserve Backup home directory.
4. Execute the babha –postsetup command.

Appendix B: Using Best Practices to Install and Upgrade CA ARCserve Backup

The objective of this appendix is to provide you with a set of best practices that you can use to install CA ARCserve Backup and upgrade CA ARCserve Backup from a previous release.

This section contains the following topics:

Best Practices for Installing CA ARCserve Backup (see page 281)
Best Practices for Upgrading CA ARCserve Backup from a Previous Release (see page 323)
General Best Practices (see page 380)

Best Practices for Installing CA ARCserve Backup

Consider the following best practices when you are installing CA ARCserve Backup.

This section contains the following topics:

How to Complete Prerequisite Tasks for Installing CA ARCserve Backup (see page 282)
Installing CA ARCserve Backup into a Single-server Environment (see page 283)
Installing a Primary Server with Member Servers (see page 287)
Installing a Primary Server with Member Servers and Devices (see page 294)
Installing a Primary Server with Member Servers and Shared Devices in a SAN (see page 301)
Installing Multiple Primary Servers with Member Servers in a SAN (see page 309)
Installing CA ARCserve Backup into a Cluster-aware Environment (see page 317)

How to Complete Prerequisite Tasks for Installing CA ARCserve Backup

Before you install CA ARCserve Backup, complete the following prerequisite tasks:

Licensing

Ensure that you have the licenses that you require to install CA ARCserve Backup.

System requirements

Review the readme file for a description of the system requirements for the computers where you will install CA ARCserve Backup.

CA ARCserve Backup database

Determine the application that you will use for the CA 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 is not supported on IA-64 (Intel Itanium) operating systems.

  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 CA ARCserve Backup database.

Note: For more information, see Database Requirements (see page 67).

CA ARCserve Backup server type

Determine the type of CA ARCserve Backup server that you require. The installation wizard detects and analyzes your current configuration. The installation wizard then determines the type of CA 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 CA 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 CA 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 CA 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, CA ARCserve Backup automatically detects and configures attached devices; manual configuration is not required.

Installing CA ARCserve Backup into a Single-server Environment

The following sections describe best practices that you can use to install CA ARCserve Backup into a single-server environment.

This section contains the following topics:

Recommended Configuration - Stand-alone Server (see page 283)
Components You Must Install (see page 285)
How to Install a Stand-alone Server or Primary Server (see page 286)
How to Verify a Stand-alone Server Installation (see page 286)

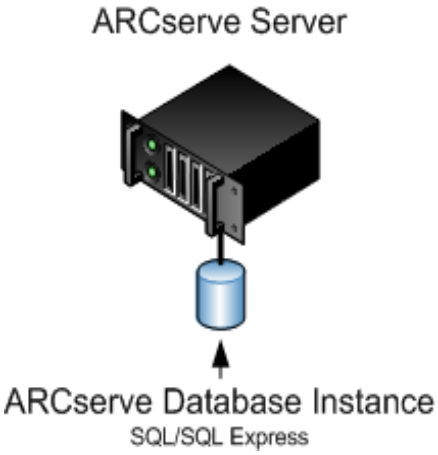
Recommended Configuration - Stand-alone Server

When you require a single backup server to protect your environment, the best practice is to install CA 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 CA 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 CA ARCserve Backup Stand-alone Server or a CA ARCserve Backup Primary Server.

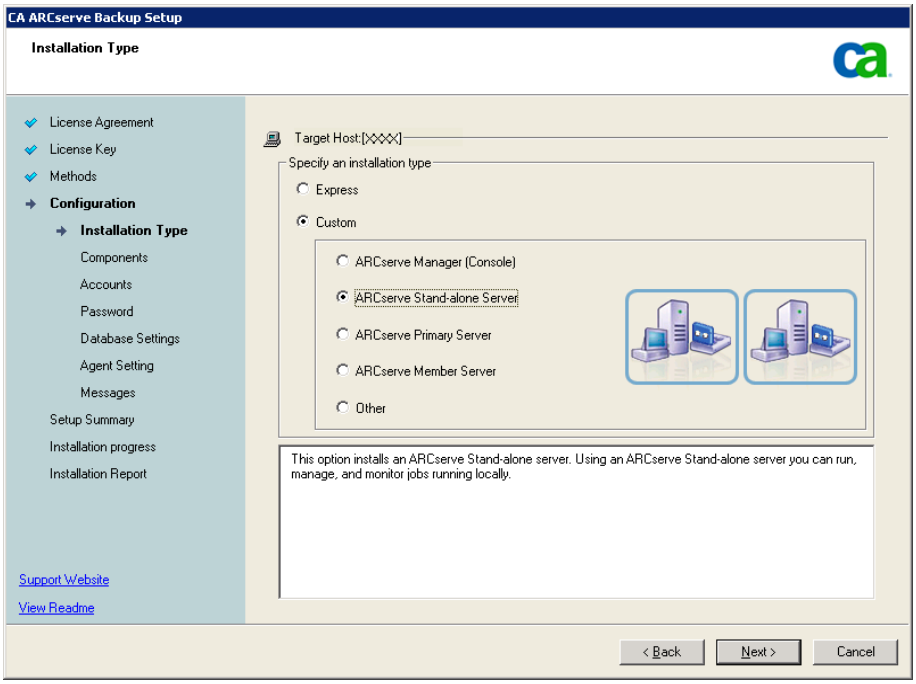


Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Stand-alone Server

Lets you install CA ARCserve Backup on a stand-alone backup server.



CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

How to Install a Stand-alone Server or Primary Server

Complete the following tasks to install CA ARCserve Backup into a single-server environment:

1. Install the CA 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 CA ARCserve Backup installation functions properly, complete the following tasks:

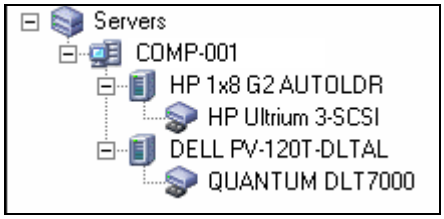
1. Open the CA ARCserve Backup Manager Console.
2. Open the Database Manager and the Job Status Manager.

   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 CA 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 online help or 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 CA ARCserve Backup with a primary server and one or more member servers.

This section contains the following topics:

Recommended Configuration (see page 288)
Components You Must Install (see page 290)
How to Install a Primary Server with Member Servers (see page 292)
How to Verify a Primary Server with Member Servers Installation (see page 292)

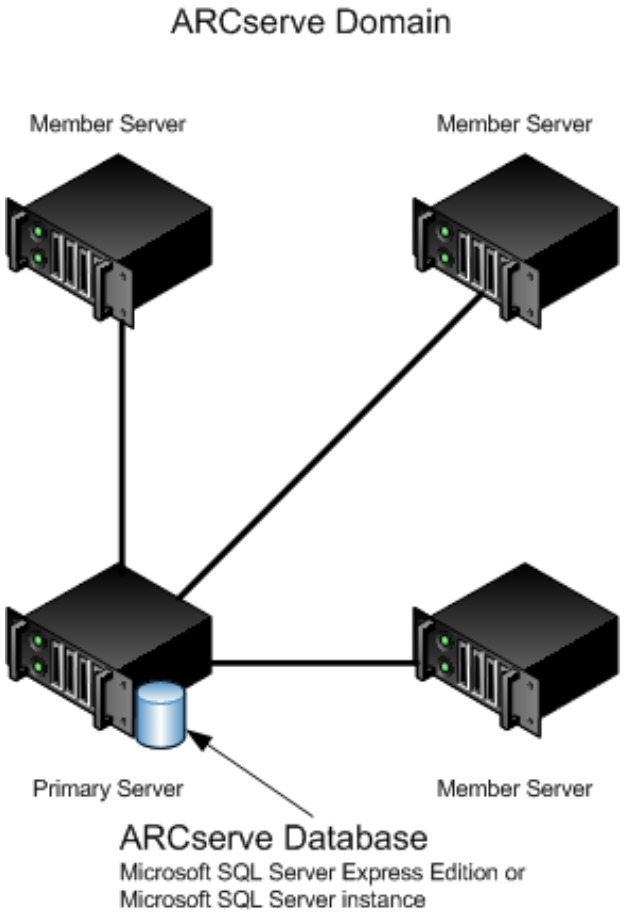
Recommended Configuration

When you require multiple backup servers that reside in the same domain to protect your environment, the best practice is to install CA 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 CA 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 CA 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 CA ARCserve Backup database is hosted by Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.

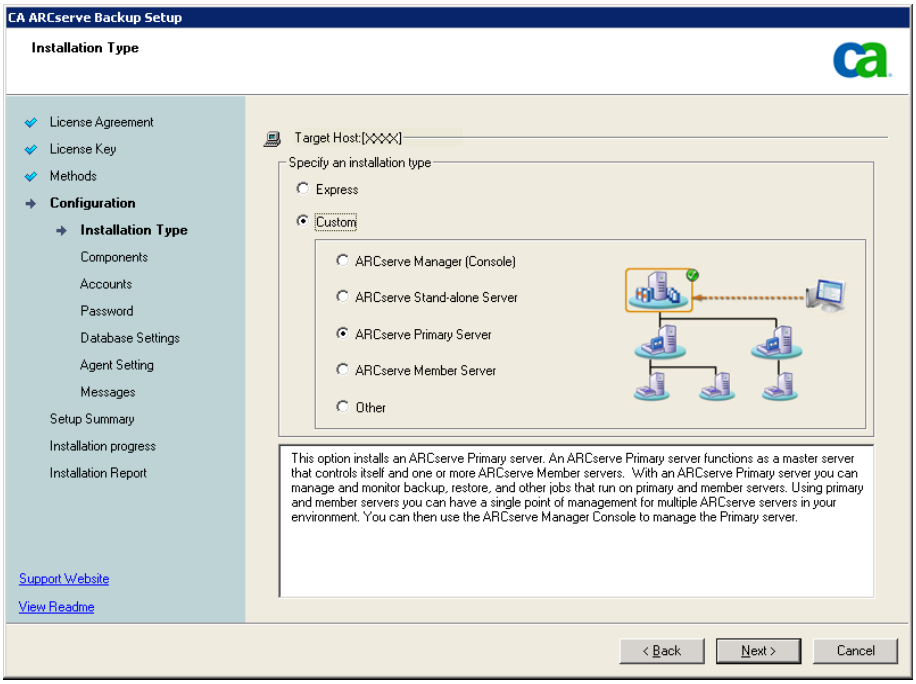


Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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.

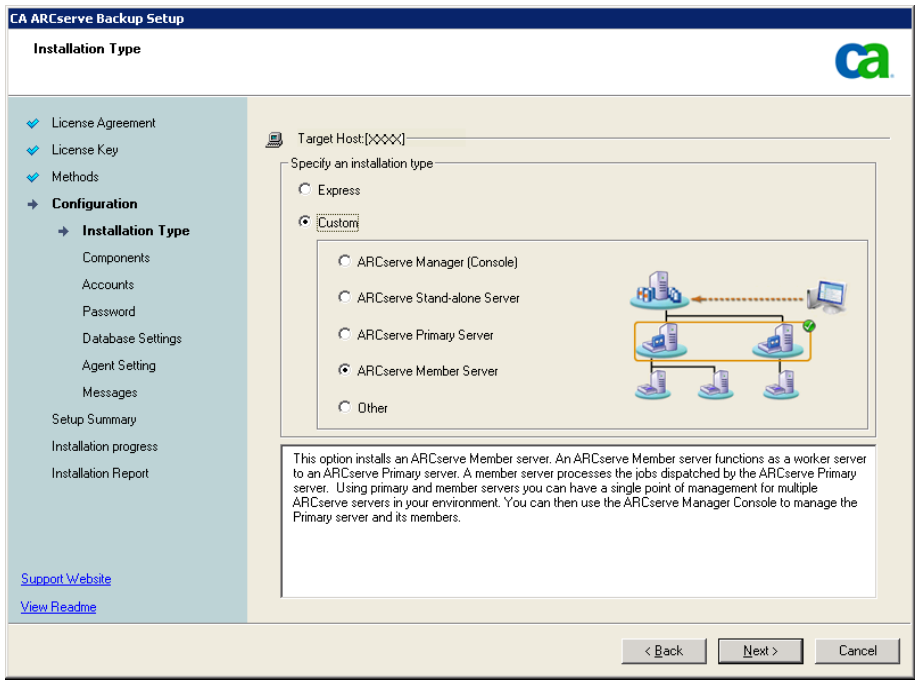
Important! The uninstallation routine does not uninstall the CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Member Server

Lets servers in a CA 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 CA 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 CA ARCserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the CA ARCserve Backup database.

2. Install the CA ARCserve Backup Member Server on all servers that will function as members of the new CA ARCserve Backup domain.

3. Verify the installation.

How to Verify a Primary Server with Member Servers Installation

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

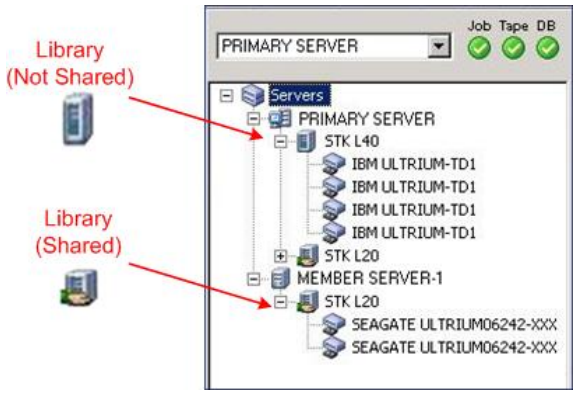
3. Open the Database Manager and the Job Status Manager.

   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 CA 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 online help or 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 CA 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 295)
Components You Must Install (see page 297)
How to Install a Primary Server with Member Servers and Devices (see page 299)
How to Verify a Primary Server with Member Servers and Devices Installation (see page 299)

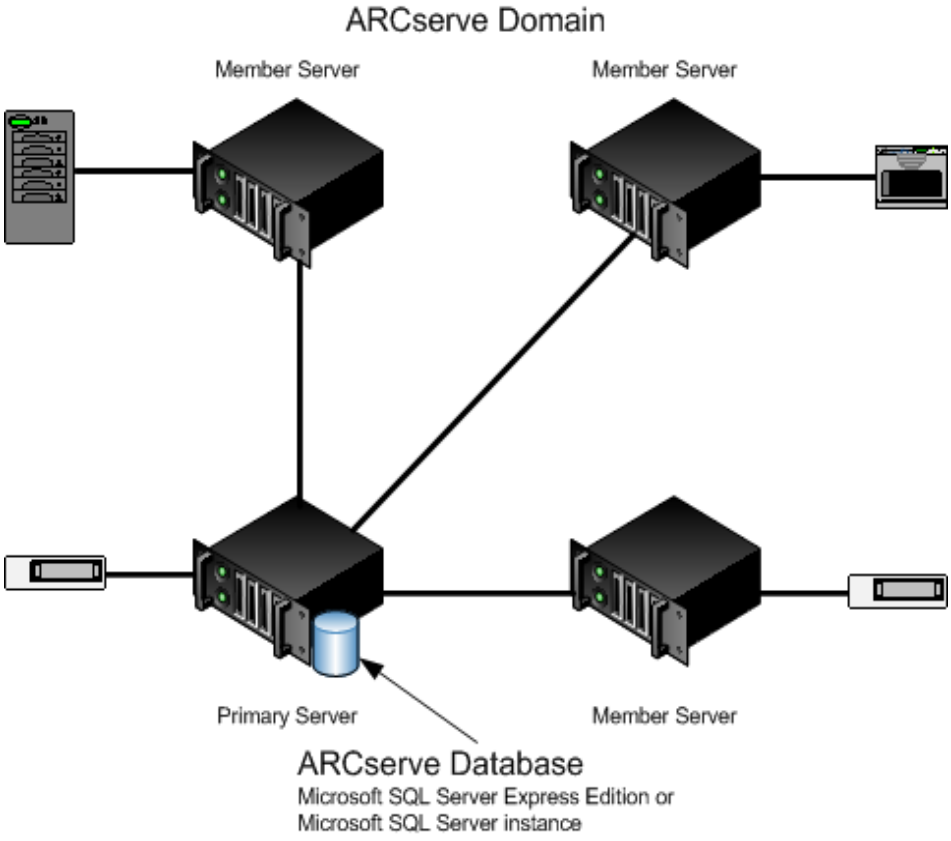
Recommended Configuration

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 CA 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 CA 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 CA 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 CA ARCserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.

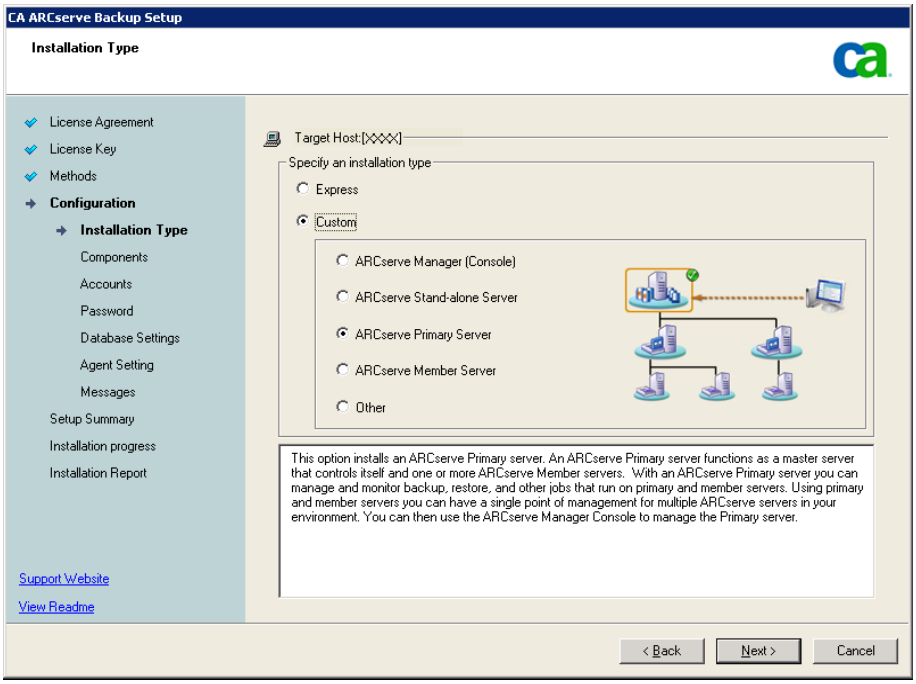


Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

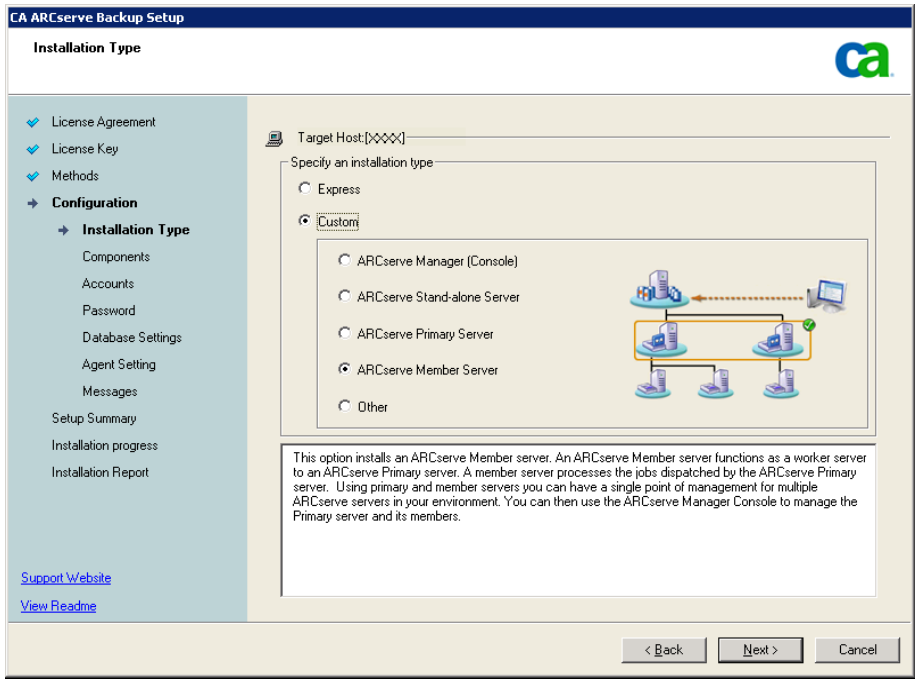
Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Tape Library Option

Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.

CA ARCserve Backup Member Server

Lets servers in a CA 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 CA 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 CA ARCserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the CA 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 CA ARCserve Backup Member Server on all servers that will function as members of the new CA 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 CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

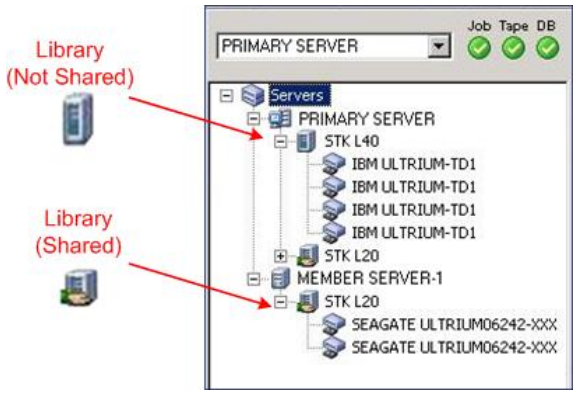
3. Open the Database Manager and the Job Status Manager.

   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 CA 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 online help or 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 CA 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 302)
Components You Must Install (see page 304)
How to Install a Primary Server with Member Servers and Shared Devices in a SAN (see page 306)
How to Verify a Primary Server with Member Servers and Shared Devices in a SAN Installation (see page 307)

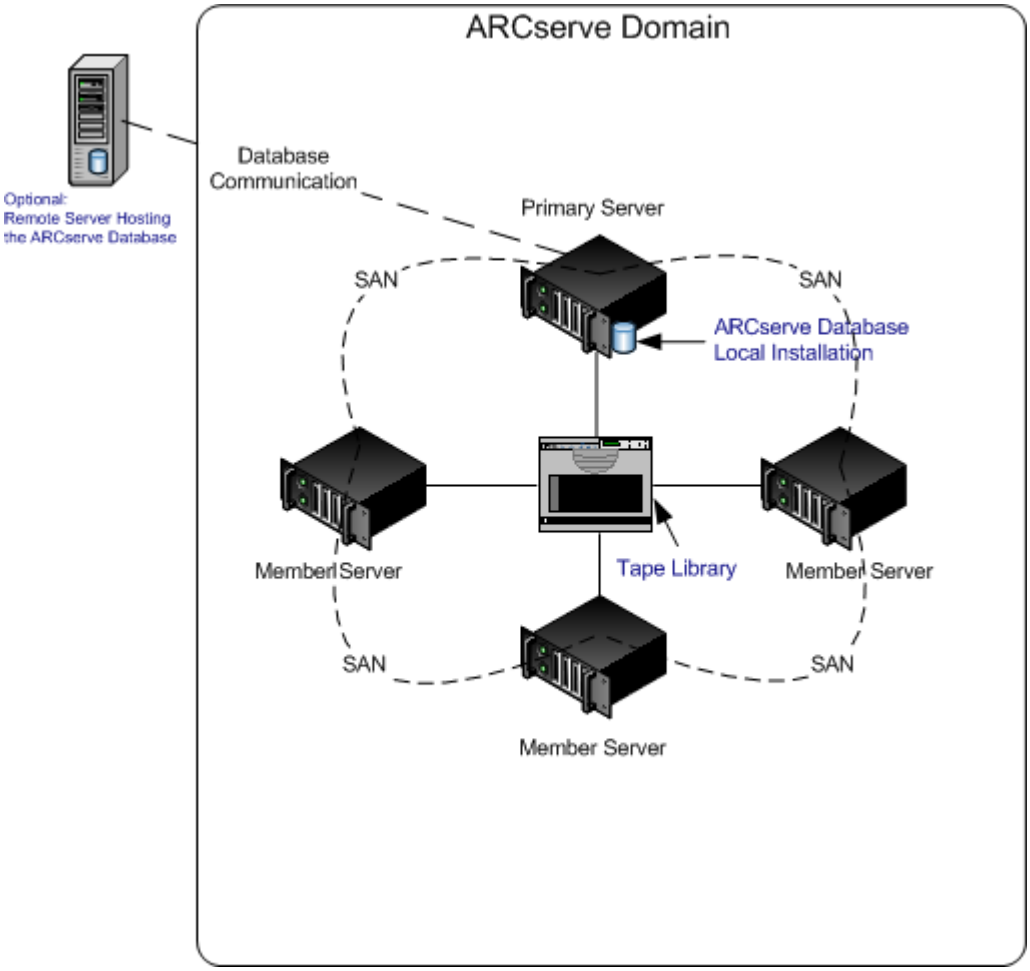
Recommended Configuration

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 CA 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 CA 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 CA 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 CA ARCserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.

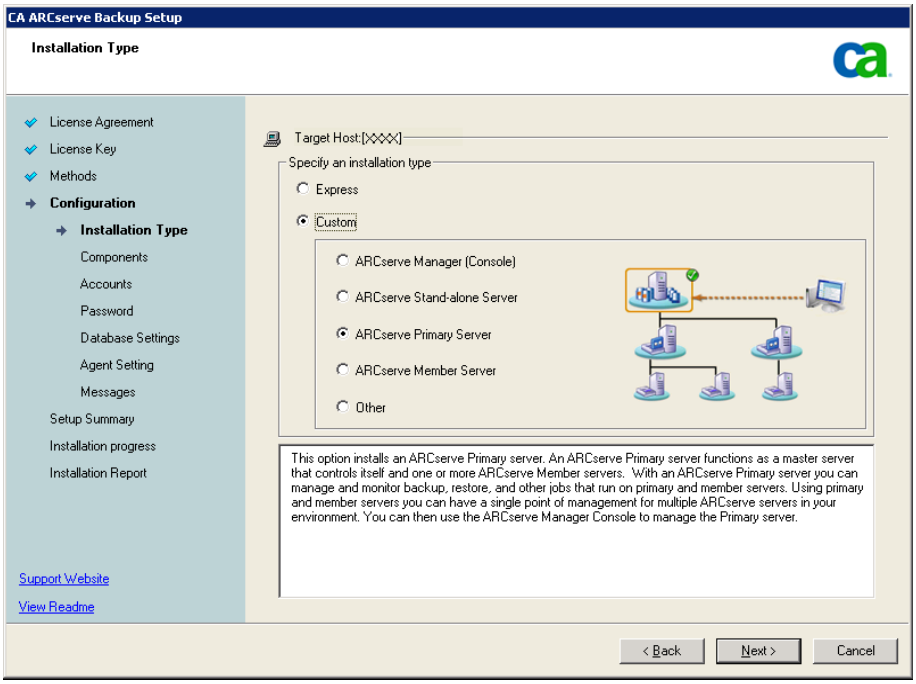


Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Tape Library Option

Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.

CA ARCserve Backup Storage Area Network (SAN) Option

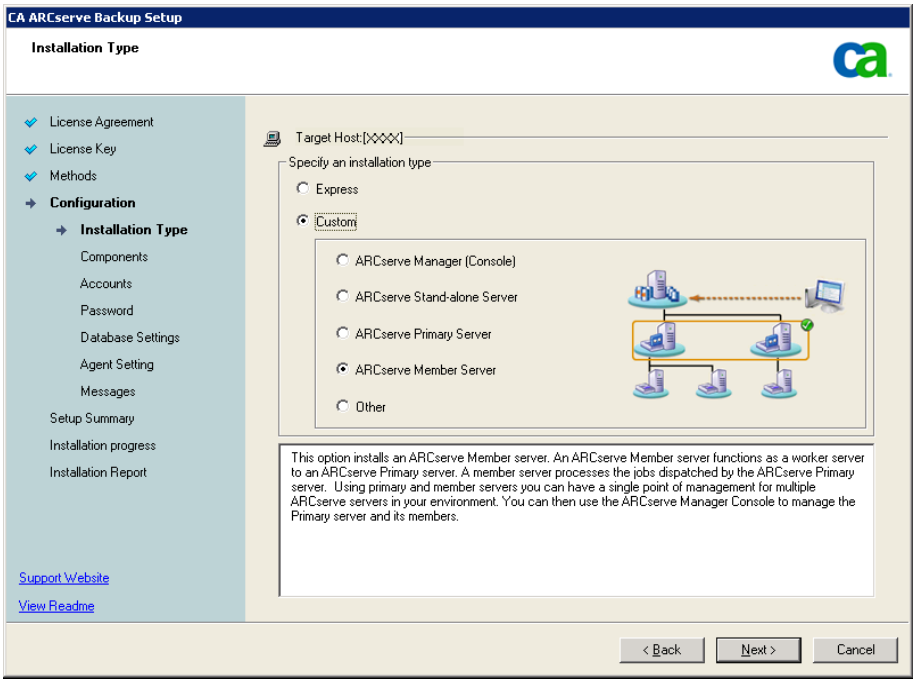
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the CA ARCserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

CA ARCserve Backup Member Server

Lets servers in a CA 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 CA 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 CA ARCserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the CA 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 CA ARCserve Backup Member Server on all servers that will function as members of the new CA 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 CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

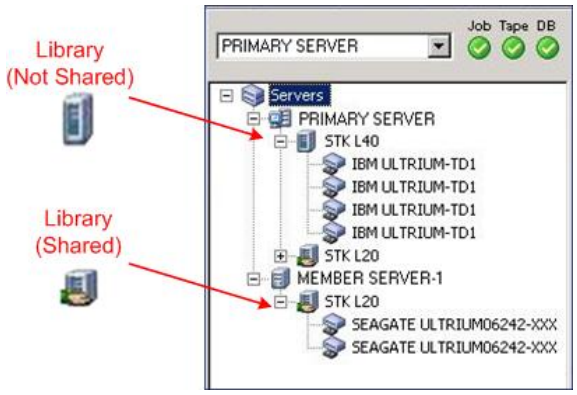
3. Open the Database Manager and the Job Status Manager.

   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 CA 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 online help or 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 CA 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 310)
Components You Must Install (see page 312)
How to Install Multiple Primary Servers with Member Servers in a SAN (see page 314)
How to Verify a Multiple Primary Servers with Member Servers in a SAN Installation (see page 315)

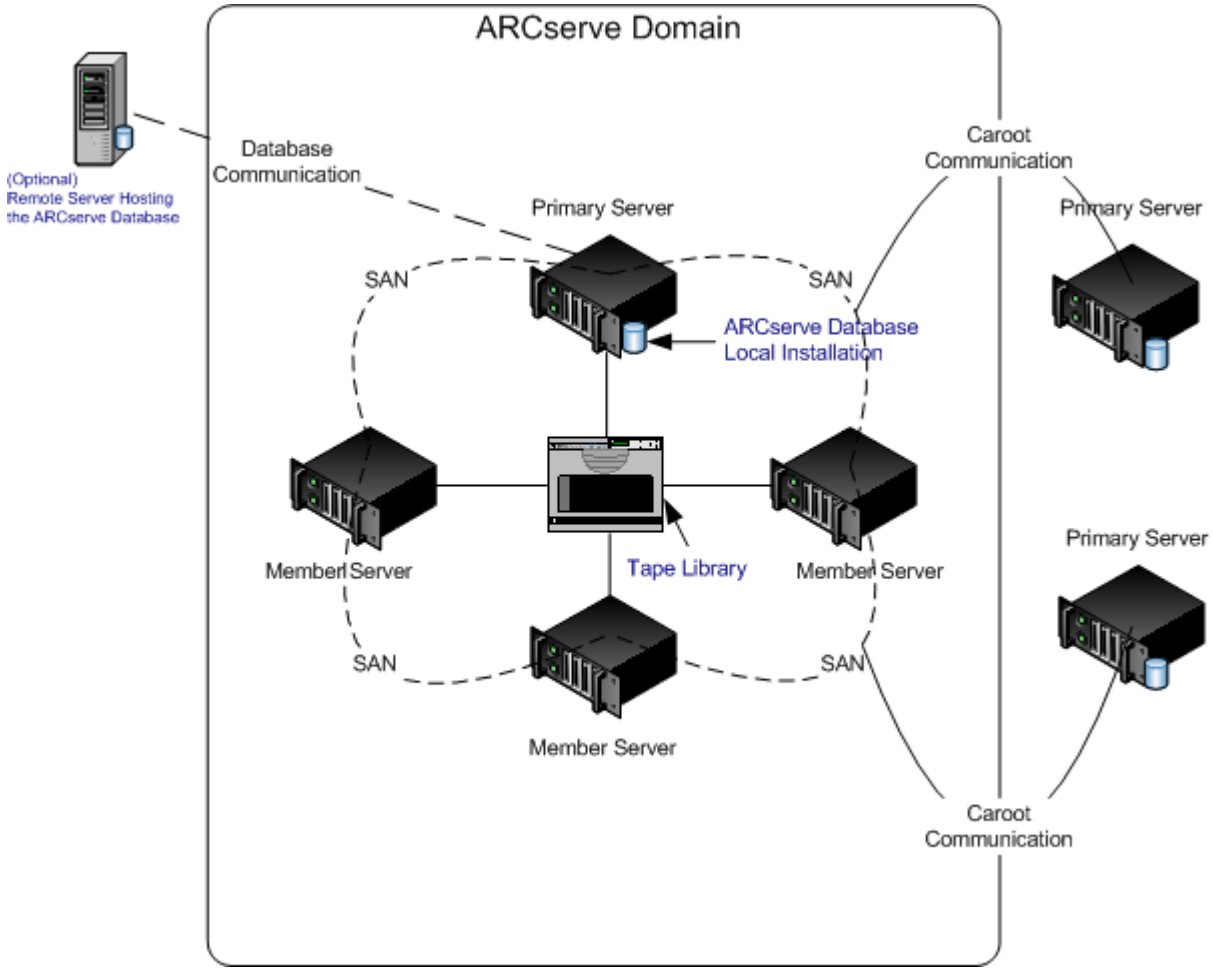
Recommended Configuration

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 CA 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 CA 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 CA 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 CA ARCserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the database instance resides on the primary server.

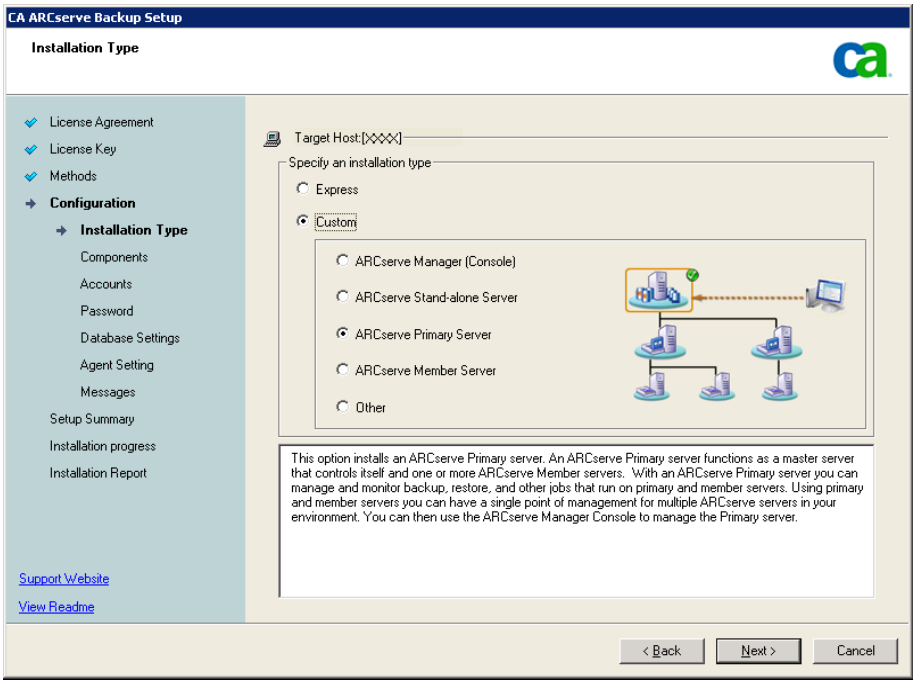


Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Tape Library Option

Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.

CA ARCserve Backup Storage Area Network (SAN) Option

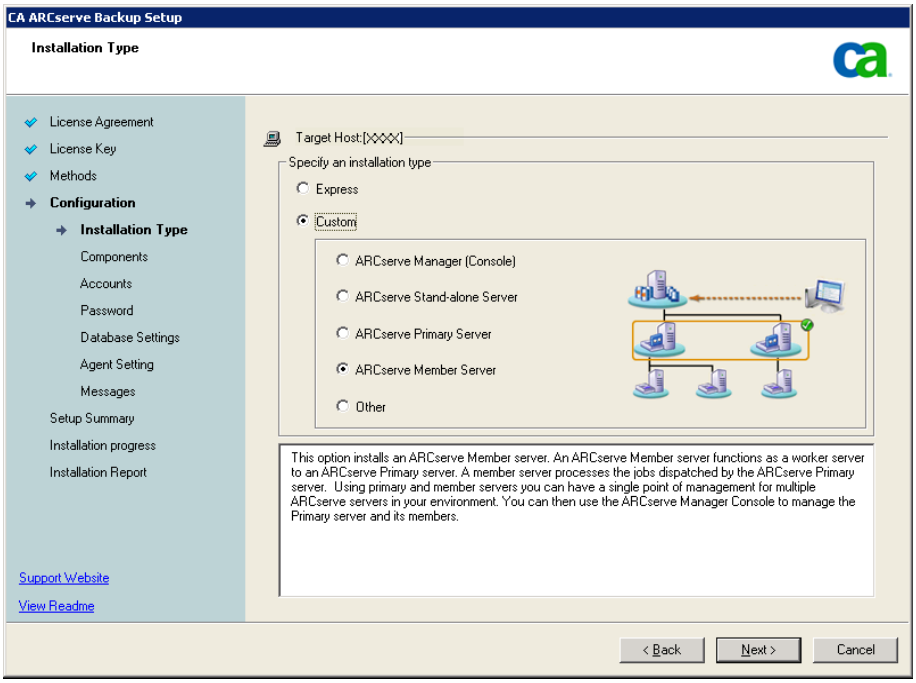
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the CA ARCserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

CA ARCserve Backup Member Server

Lets servers in a CA 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 CA 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 CA ARCserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the CA 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 CA ARCserve Backup Member Server on all servers that will function as members of the new ARCserve domain.
5. Install the CA 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 CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA ARCserve Backup Manager Console on the primary server.
2. Open the Server Admin.

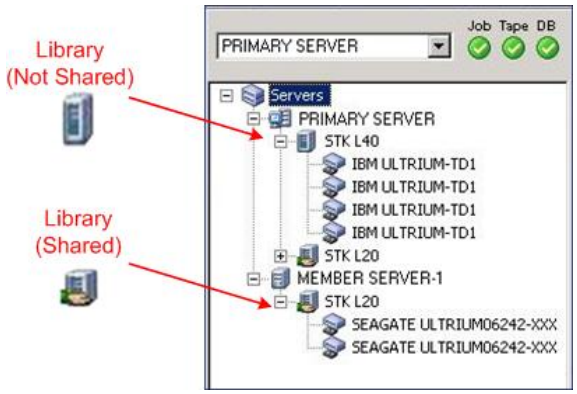
   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.
3. Open the Database Manager and the Job Status Manager.

   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 CA 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 online help or 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 CA ARCserve Backup into a Cluster-aware Environment

The following sections describe best practices that you can use to install CA ARCserve Backup into a cluster-aware environment.

This section contains the following topics:

Recommended Configuration (see page 318)
Components You Must Install (see page 319)
How to Install CA ARCserve Backup into a Cluster-aware Environment (see page 321)
How to Verify a Cluster-aware Installation (see page 321)

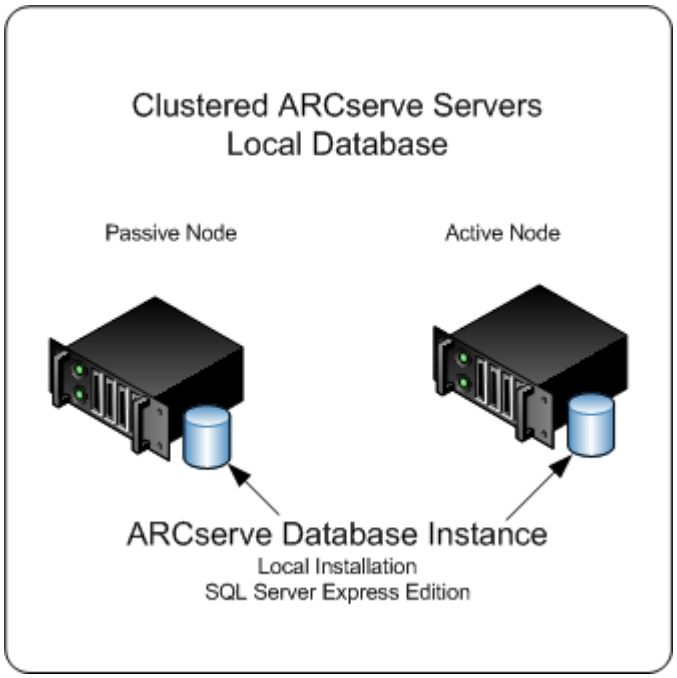
Recommended Configuration

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 CA ARCserve Backup using the Primary Server and Member Server installation options into your cluster aware environment. This architecture lets you centrally manage your CA 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 CA 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 CA 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.

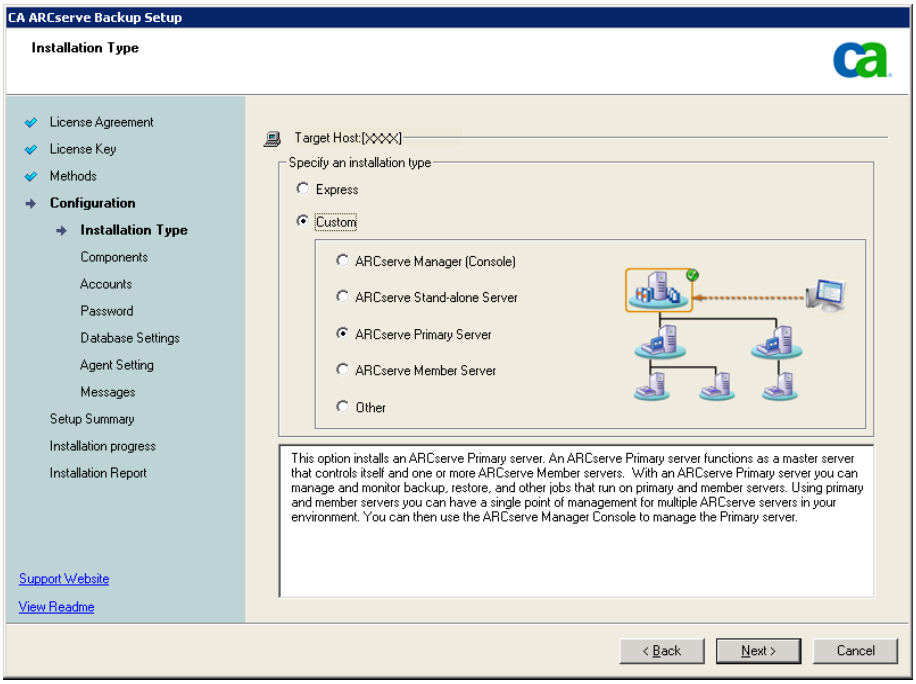


Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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.

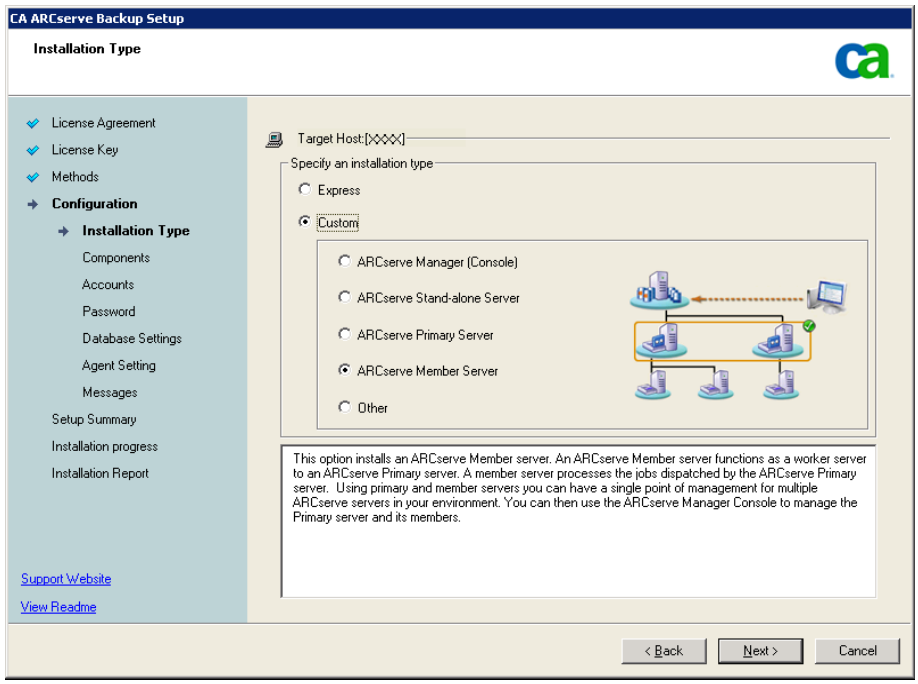
Important! The uninstallation routine does not uninstall the CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Member Server

Lets servers in a CA ARCserve Backup domain receive instructions about jobs and devices from a primary server.



How to Install CA ARCserve Backup into a Cluster-aware Environment

You can install CA ARCserve Backup to a cluster environment with job failover capability on the following cluster platforms:

- Microsoft Cluster Server (MSCS) in x86/AMD64/IA64 Windows Server
- NEC CLUSTERPRO/ExpressCluster for Windows 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, and CLUSTERPRO/ExpressCluster X 2.0 for Windows.

To install CA ARCserve Backup into a cluster aware environment

1. Refer to one of the following sections for information about how to install CA ARCserve Backup into a cluster-aware environment:
   - For MSCS, see Deploy CA ARCserve Backup Server on MSCS (see page 138).
   - For NEC CLUSTERPRO, see Deploy CA ARCserve Backup Server on NEC Cluster (see page 163).
2. Verify the installation.

How to Verify a Cluster-aware Installation

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA ARCserve Backup Manager Console on the primary server.

   Ensure that you can view database information and Activity Log data in the Job Status Manager.

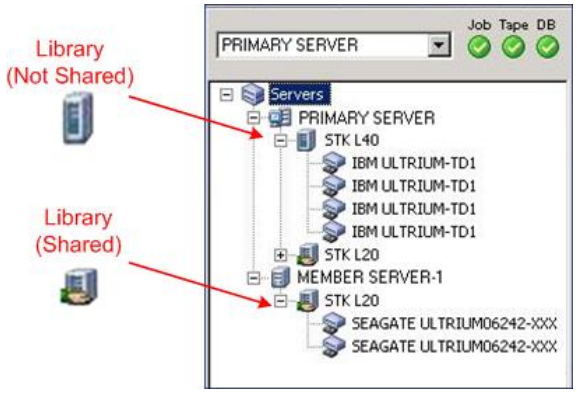
2. Open the Database Manager and the Job Status Manager.

   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 CA 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 online help or 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 CA ARCserve Backup from a Previous Release

Consider the following best practices when upgrading CA ARCserve Backup from a previous release.

This section contains the following topics:

How to Complete Prerequisite Tasks for Upgrading CA ARCserve Backup (see page 324)
Upgrading a Stand-alone Server or Primary Server (see page 326)
Upgrading Multiple Stand-alone Servers in a Domain (see page 332)
Upgrading Multiple Stand-alone Servers Sharing a Remote Database (see page 340)
Upgrading Servers in a SAN Using a Local or Remote Database (see page 347)
Upgrading Multiple Servers in a SAN and Non-SAN Environment to this Release (see page 356)
Upgrading Multiple Servers Using a Central Database (see page 364)
Upgrading Multiple Servers in a Cluster-aware Environment (see page 372)

How to Complete Prerequisite Tasks for Upgrading CA ARCserve Backup

Before you upgrade CA ARCserve Backup, complete the following prerequisite tasks:

Licensing

Ensure that you have the licenses that you require to upgrade CA ARCserve Backup.

System requirements

Review the readme file for a description of the system requirements for the computers where you will upgrade CA 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 77) and Backward Compatibility (see page 78).

Note: For a description of supported platforms for all CA ARCserve Backup agents, see the readme file.

CA ARCserve Backup database

Determine which application that you will to host the CA 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.

  CA 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 CA ARCserve Backup database.
- Microsoft SQL Server 2008 Express Edition is not supported on IA-64 (Intel Itanium) operating systems.
- 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 67).

CA ARCserve Backup server type

Determine the type of CA 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 CA ARCserve Backup server that you should upgrade to and the agents and options that you need to install.

If you plan to add CA 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 CA ARCserve Backup servers.

  To enable central management capabilities, you must install and license CA ARCserve Backup and the Central Management Option.

  Note: For more information about the different types of ARCserve server installations, see Types of CA ARCserve Backup Server Installations (see page 62).

Attached devices

Ensure that all devices, such as libraries, are attached to the CA ARCserve Backup servers before you start the upgrade process. The first time the Tape Engine starts after the upgrade is complete, CA 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. CA ARCserve Backup detects all jobs with a Ready Status and places them in a Hold status for you. If there are jobs in progress, CA 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

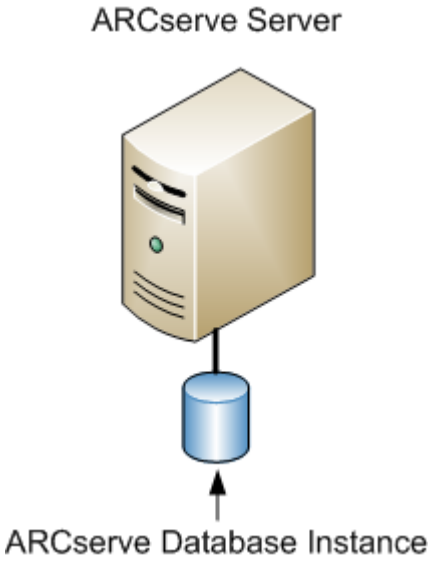
The following sections describe best practices that you can use to upgrade an ARCserve stand-alone server to this release.

This section contains the following topics:

Current Configuration - ARCserve Stand-alone Server (see page 326)
Recommended Configuration - CA ARCserve Backup Stand-alone Server or Primary Server (see page 327)
New Components You Must Install (see page 328)
Components You Must Upgrade (see page 330)
How to Upgrade to an ARCserve Stand-alone Server (see page 330)
How to Verify a Stand-alone Server or Primary Server Upgrade (see page 330)

Current Configuration - ARCserve Stand-alone Server

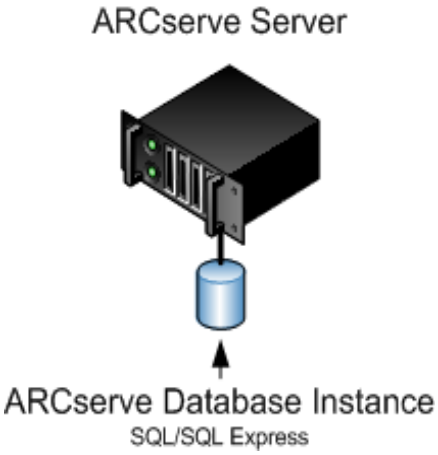
The following diagram illustrates the architecture of a CA ARCserve Backup stand-alone server configuration in previous releases:



Recommended Configuration - CA 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 CA ARCserve Backup Stand-alone Server or a CA ARCserve Backup Primary Server.

The following diagram illustrates the architecture of a CA ARCserve Backup Primary Server or a CA ARCserve Backup Stand-alone Server.

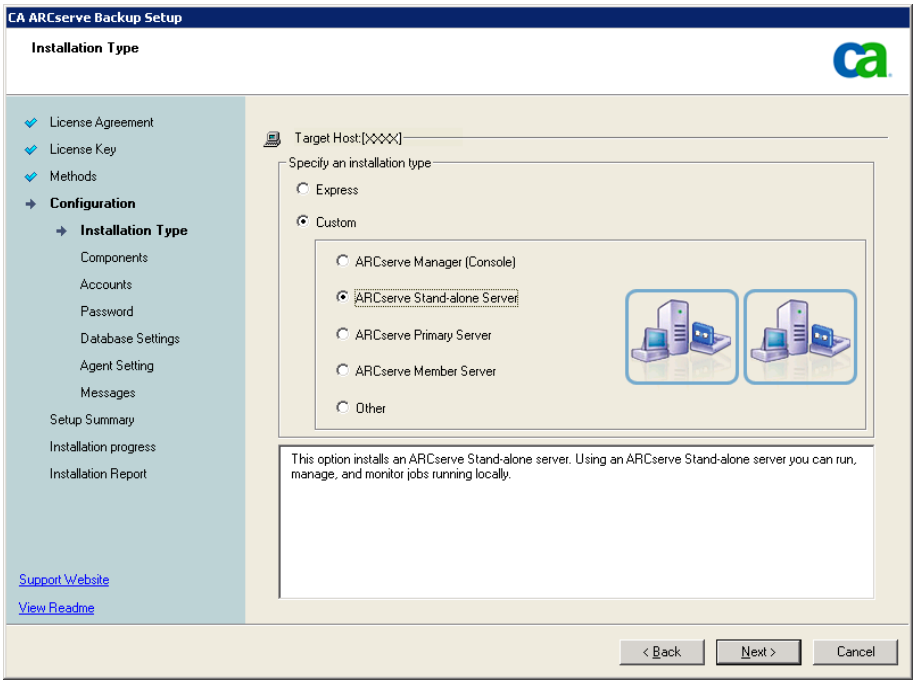


New Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Stand-alone Server

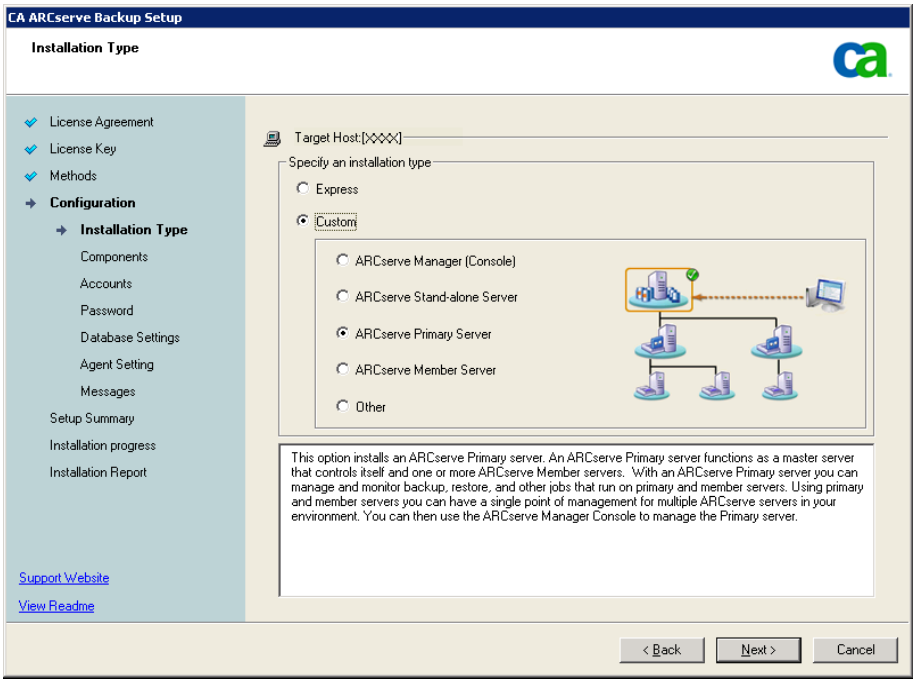
Lets you install CA ARCserve Backup on a stand-alone backup server.



(Optional) CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 1: Setup: Installation Type dialog. ARCserve Primary Server is specified.



CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following CA ARCserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade to an ARCserve Stand-alone Server

Complete the following tasks to upgrade an ARCserve stand-alone server environment to a CA ARCserve Backup Stand-alone or Primary Server environment.

1. Install the CA ARCserve Backup Primary Server or the CA 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 CA ARCserve Backup, Setup launches a migration wizard that lets you migrate data from your previous installation to the new CA 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) CA ARCserve Backup does not support recovering the CA ARCserve Backup database when the last backup of the CA ARCserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the CA ARCserve Backup database as soon as possible after the upgrade is complete. For information about backing up the CA ARCserve Backup database, see the *Administration Guide*.

More information:

Upgrade Considerations (see page 76)
Upgrade CA ARCserve Backup from a Previous Release (see page 97)

How to Verify a Stand-alone Server or Primary Server Upgrade

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

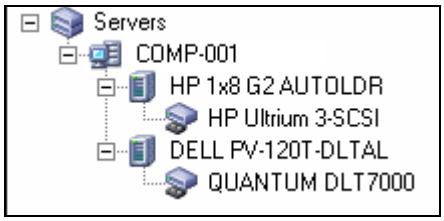
   Ensure that all previous backup data migrated successfully.

   Note: CA 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 CA 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 online help or 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

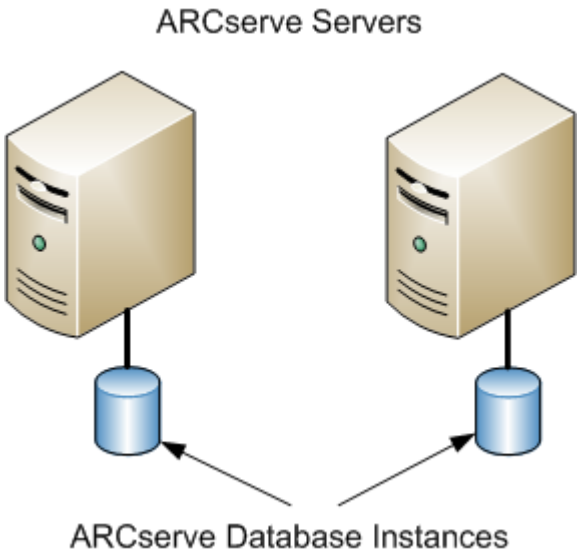
The following sections describe best practices that you can use to upgrade multiple ARCserve servers that do not share a database in a domain to a CA ARCserve Backup domain that consists of a primary server and multiple member servers.

This section contains the following topics:

Current Configuration - Multiple ARCserve Servers in a Domain (see page 333)
Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers (see page 333)
New Components You Must Install (see page 335)
Components You Must Upgrade (see page 336)
How to Upgrade Multiple ARCserve Servers to a Centralized Management Environment (see page 337)
How to Verify a Domain with a Primary Server and Member Servers Upgrade (see page 337)

Current Configuration - Multiple ARCserve Servers in a Domain

The following diagram illustrates the architecture of multiple CA ARCserve Backup servers in a domain in previous releases:



Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers

If your current configuration consists of multiple CA 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.

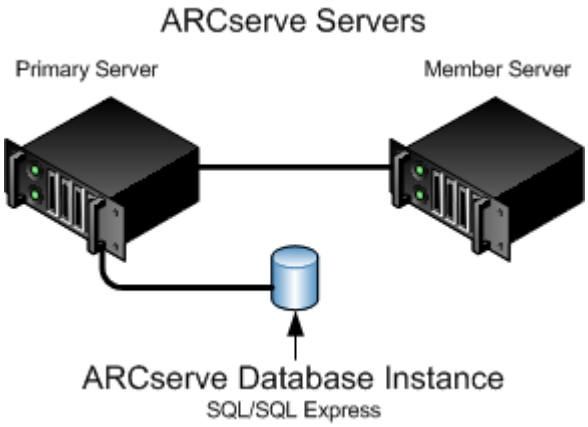
To upgrade to a centralized management environment, you must upgrade one of your existing CA ARCserve Backup servers to a CA ARCserve Backup Primary Server and then upgrade all other servers in the domain to CA ARCserve Backup Member Servers.

Note: The domain primary from your previous installation must assume the role of the CA ARCserve Backup Primary Server.

To install member servers, the installation wizard must be able to detect the CA ARCserve Backup domain name and primary server name in your network. You should therefore install CA 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 CA 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 CA ARCserve Backup to communicate with a remote database, you must use Microsoft SQL Server to host the ARCserve database.

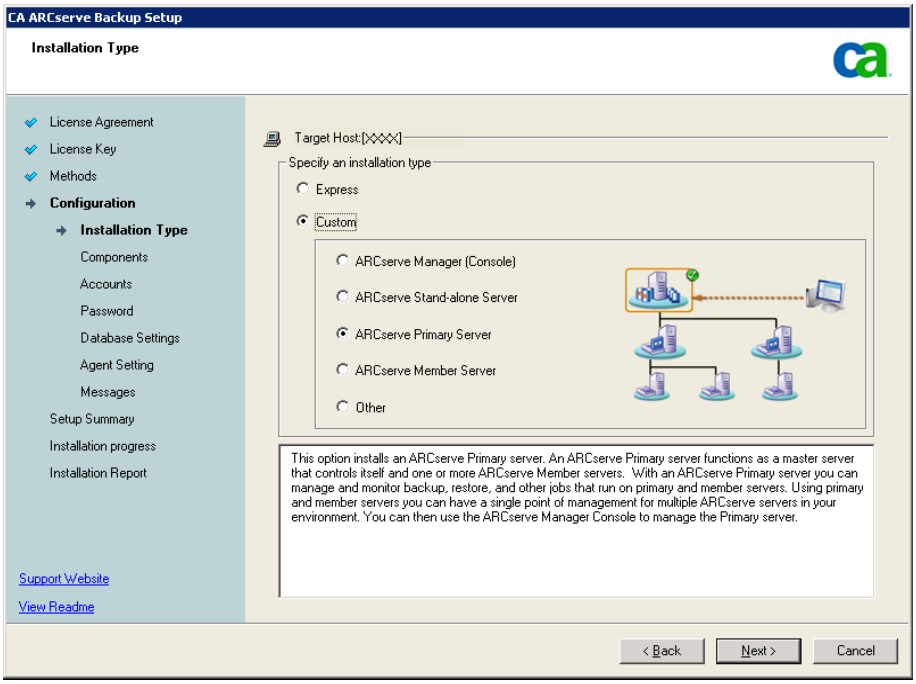
New Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 2: Setup: Installation Type dialog. ARCserve Primary Server is specified.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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.

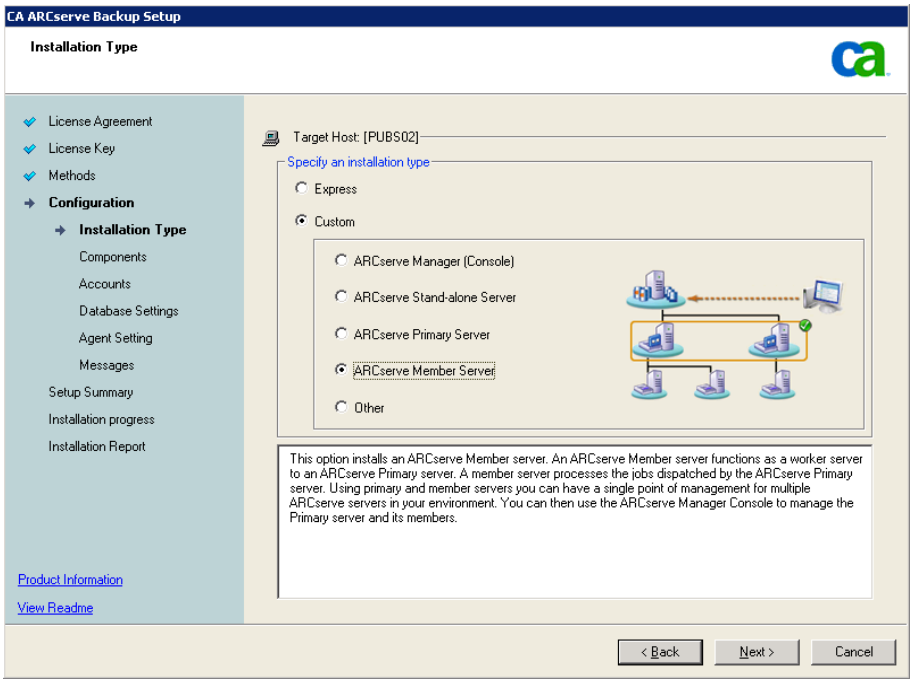
Important! The uninstallation routine does not uninstall the CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA 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 CA ARCserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade Multiple ARCserve Servers to a Centralized Management Environment

Complete the following tasks to upgrade multiple ARCserve servers to a centralized management environment that consist of a CA ARCserve Backup Primary Server and one or more CA ARCserve Backup Member Servers.

1. Install the CA 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 CA ARCserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the CA ARCserve Backup database.

   When you are prompted, migrate the data from the previous release to the new database.

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

More information:

Upgrade Considerations (see page 76)
Upgrade CA ARCserve Backup from a Previous Release (see page 97)

How to Verify a Domain with a Primary Server and Member Servers Upgrade

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

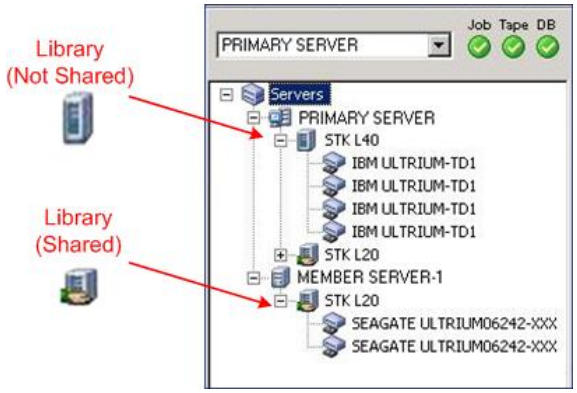
   Ensure that all previous backup data migrated successfully.

   Note: CA 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 CA 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 online help or 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

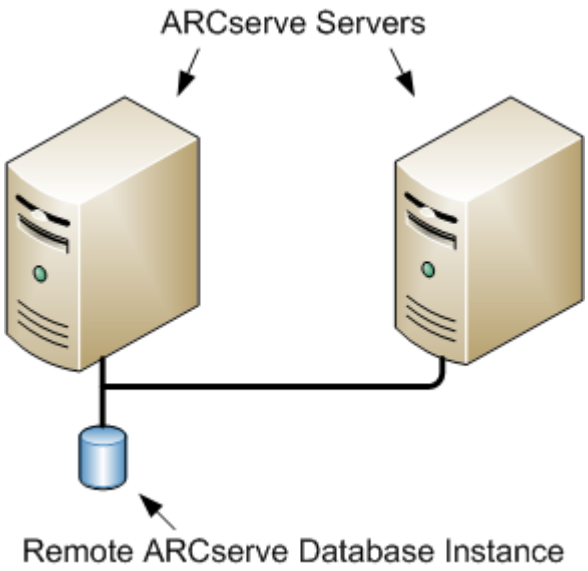
The following sections describe best practices that you can use to upgrade multiple ARCserve stand-alone servers, sharing a remote ARCserve database, to a CA ARCserve Backup Primary server and multiple CA ARCserve Backup Member servers.

This section contains the following topics:

Current Configuration - Multiple ARCserve Servers Sharing a Remote Database (see page 340)
Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers (see page 341)
New Components You Must Install (see page 342)
Components You Must Upgrade (see page 343)
How to Upgrade Multiple ARCserve Servers Sharing a Database to a Centralized Management Environment (see page 344)
How to Verify a Centralized Management Environment Upgrade (see page 344)

Current Configuration - Multiple ARCserve Servers Sharing a Remote Database

The following diagram illustrates the architecture of multiple CA ARCserve Backup stand-alone servers in a domain, sharing a remote database, in previous releases:



Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers

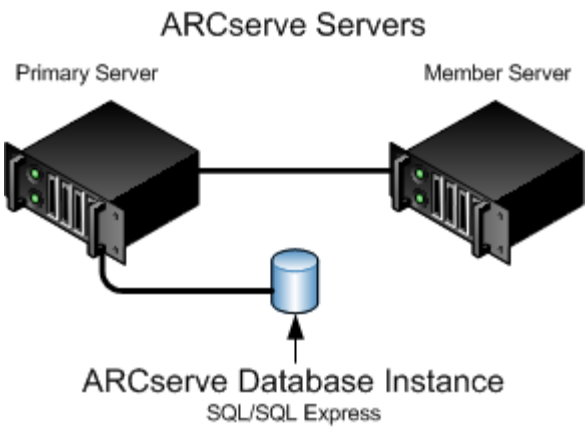
If your current configuration consists of multiple CA ARCserve Backup servers in a domain, the best practice is to upgrade to a centralized management environment that consists of a primary server and one or more member servers. A centralized management environment lets you share a local or remote database in a CA ARCserve Backup domain.

To upgrade to a centralized management environment, you must upgrade one of your existing ARCserve servers to a CA ARCserve Backup Primary Server and then upgrade all other servers in the domain to CA ARCserve Backup Member Servers.

Note: The system from your previous installation that is hosting the ARCserve database must assume the role of the CA ARCserve Backup Primary Server.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install CA 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 CA ARCserve Backup to communicate with a remote database, you must use Microsoft SQL Server to host the CA ARCserve Backup database instance.

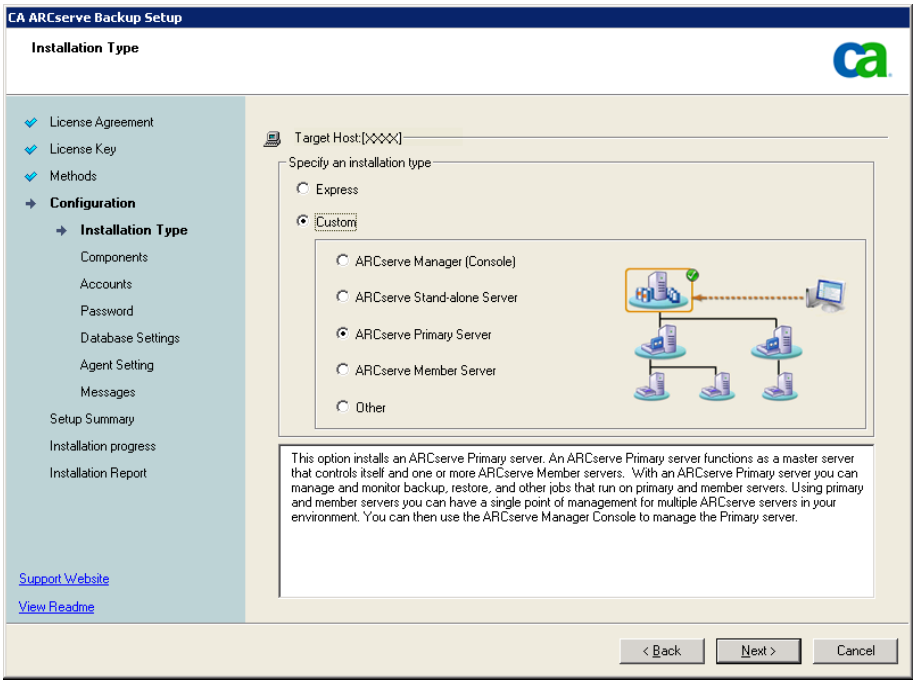
New Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 3: Setup: Installation Type dialog. ARCserve Primary Server is specified.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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.

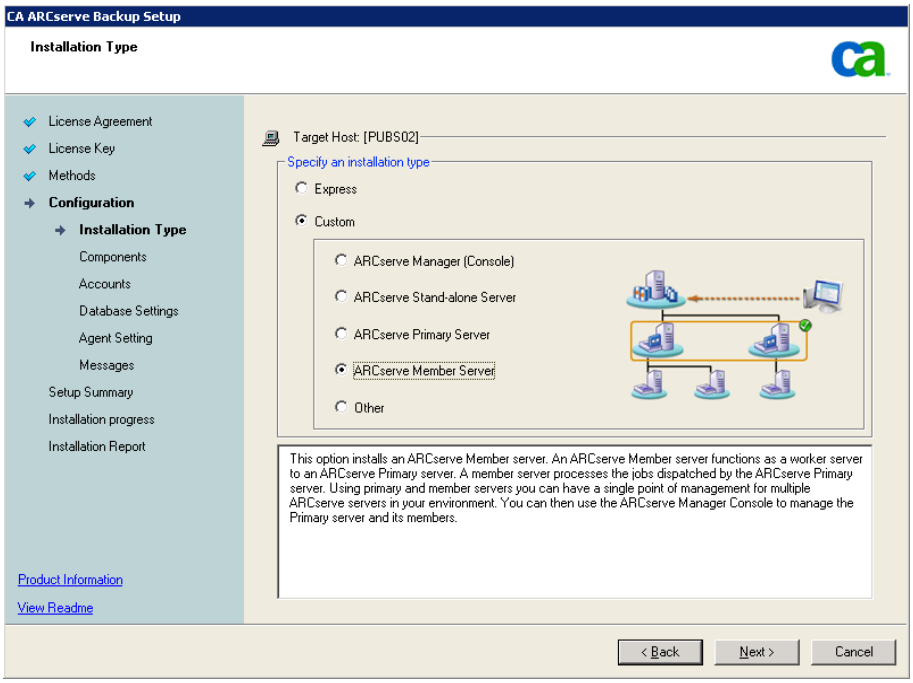
Important! The uninstallation routine does not uninstall the CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA 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 CA 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

Complete the following tasks to upgrade multiple ARCserve servers sharing a database to a centrally managed ARCserve domain.

1. Install the CA 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 CA ARCserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the CA ARCserve Backup database.

   When you are prompted, migrate the data from the previous release to the new database.

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

More information:

Upgrade Considerations (see page 76)
Upgrade CA ARCserve Backup from a Previous Release (see page 97)

How to Verify a Centralized Management Environment Upgrade

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

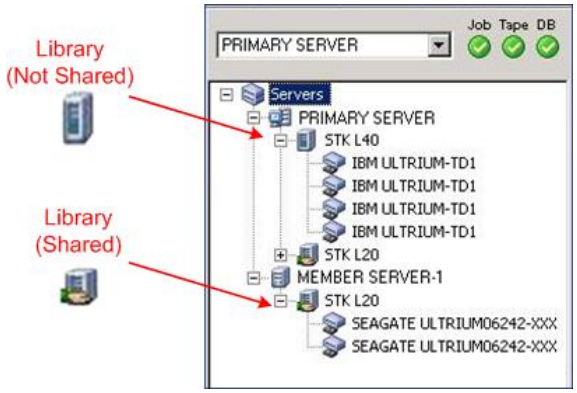
   Ensure that all previous backup data migrated successfully.

   Note: CA 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 CA 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 online help or 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

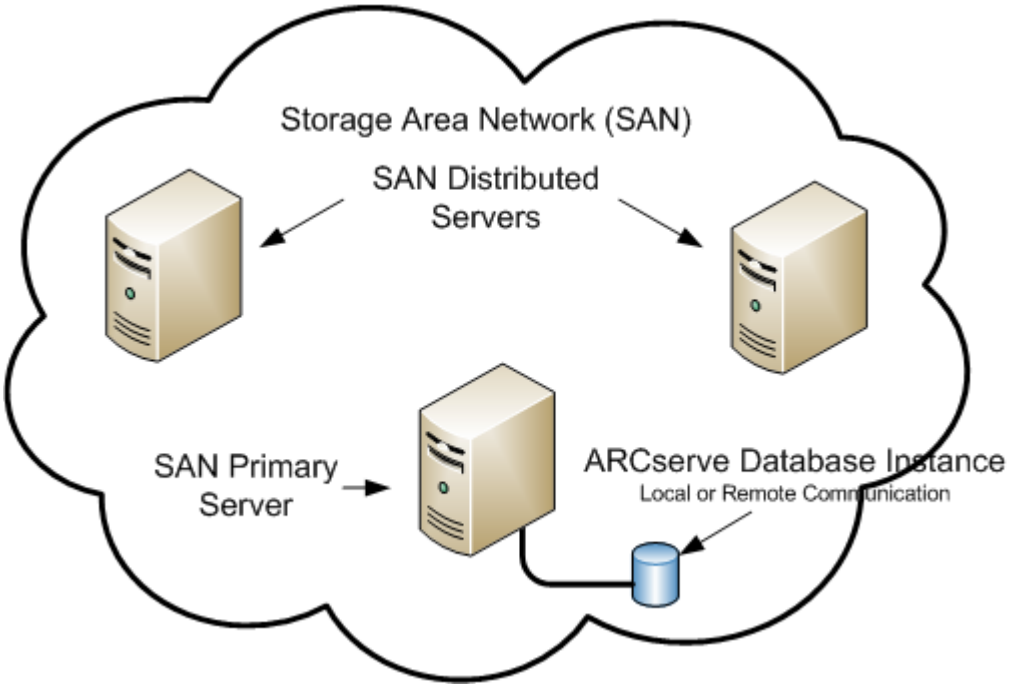
The following sections describe best practices that you can use to upgrade multiple ARCserve servers that reside on a SAN and share a local or remote ARCserve database.

This section contains the following topics:

Current Configuration - Multiple ARCserve Servers in a SAN Using a Local or Remote Database (see page 347)
Recommended Configuration - CA ARCserve Backup Domain with a SAN Primary Server and SAN Distributed Servers (see page 348)
New Components You Must Install (see page 350)
Components You Must Upgrade (see page 352)
How to Upgrade Multiple ARCserve Servers in a SAN to This Release (see page 353)
How to Verify a Centralized Management Environment Upgrade+ (see page 353)

Current Configuration - Multiple ARCserve Servers in a SAN Using a Local or Remote Database

The following diagram illustrates the architecture of multiple CA ARCserve Backup servers in a SAN environment, using a local or remote database, in previous releases:



Recommended Configuration - CA ARCserve Backup Domain with a SAN Primary Server and SAN Distributed Servers

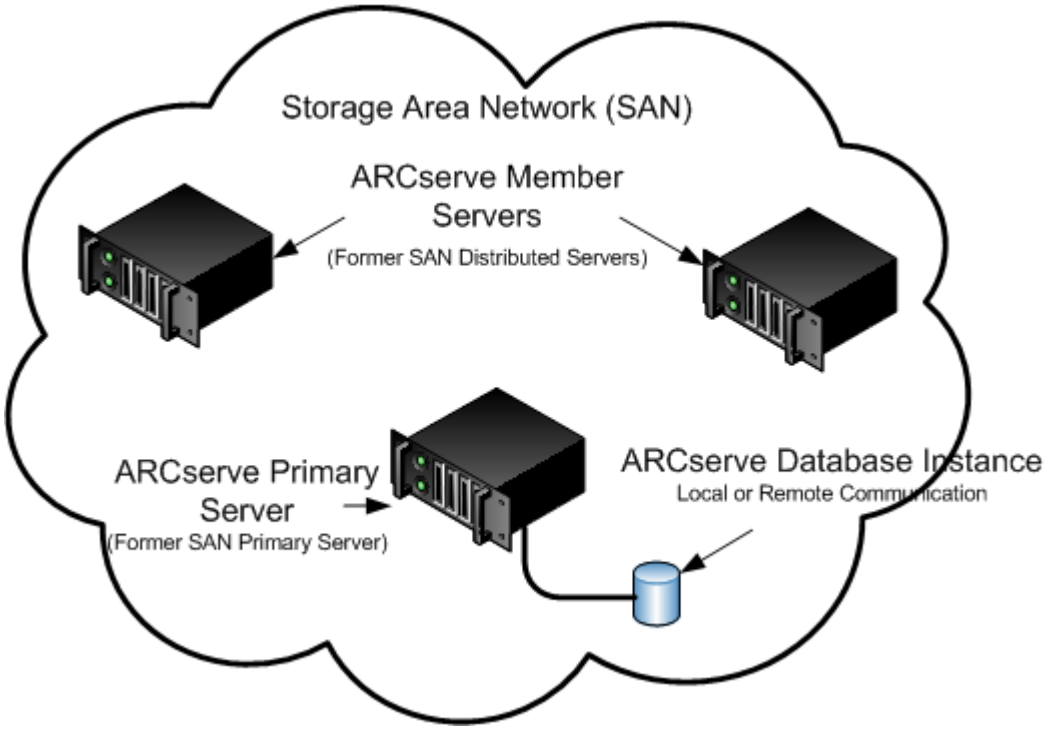
If your current configuration consists of multiple CA ARCserve Backup servers that reside on a SAN and share a local or remote CA ARCserve Backup database, the best practice is to upgrade to a centralized management environment. With a centralized management environment, you can share libraries and a 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 CA ARCserve Backup Primary Server, and then upgrade your SAN distributed servers to CA ARCserve Backup Member Servers of that particular primary server.

To install member servers, the installation wizard must be able to detect the CA ARCserve Backup domain name and the primary server name in your environment. You should therefore install CA 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 CA 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.



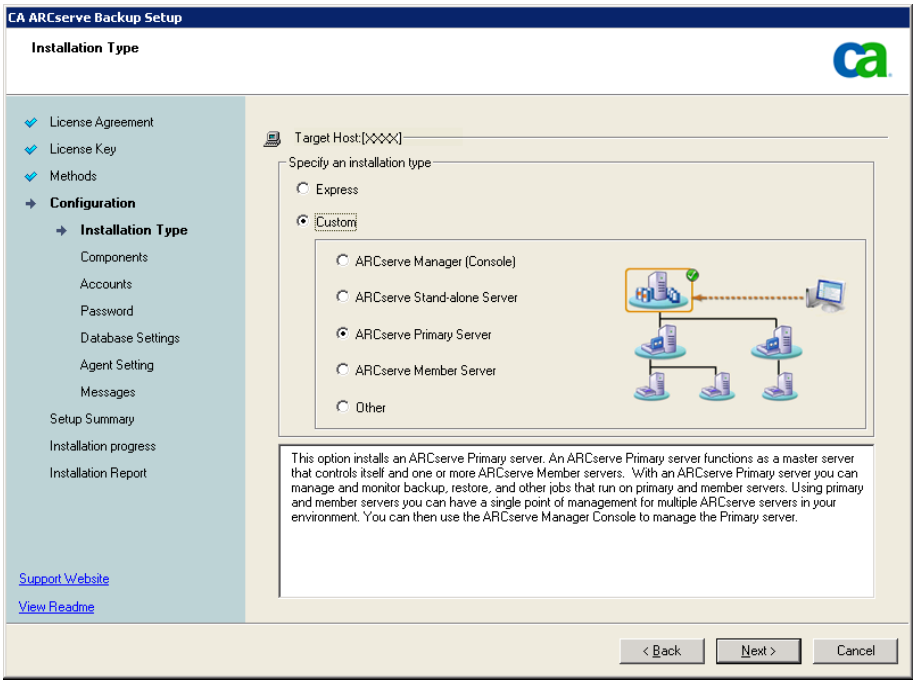
New Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 4: Setup: Installation Type dialog. ARCserve Primary Server is specified.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Tape Library Option

Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.

CA ARCserve Backup Storage Area Network (SAN) Option

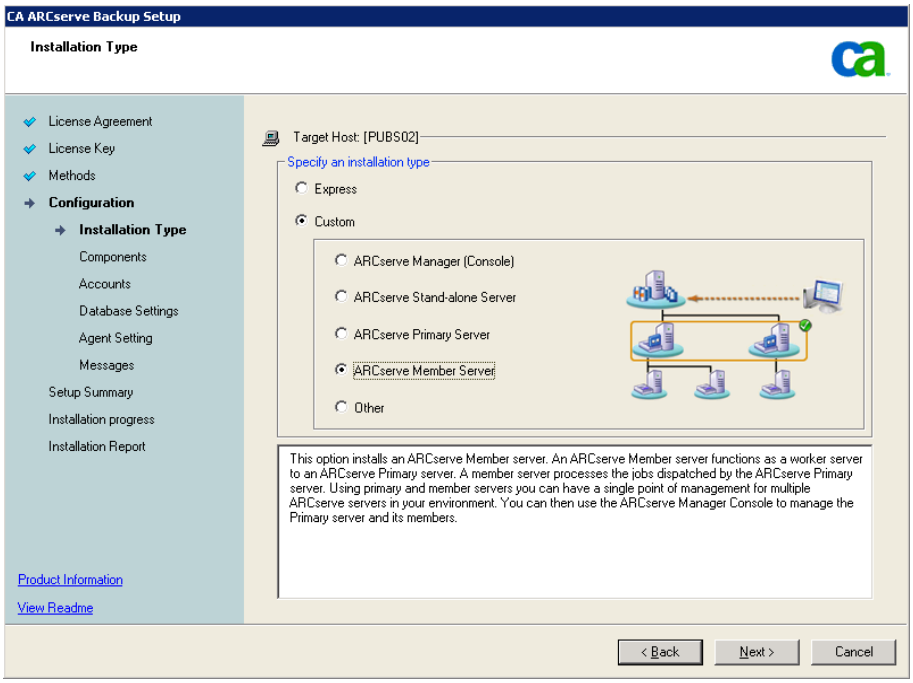
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the CA ARCserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

CA 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 CA 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

Complete the following tasks to upgrade a SAN environment to a SAN environment in this release.

1. Install the CA 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 CA 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 CA ARCserve Backup database.

   When you are prompted, migrate the data from the previous release to the new database.

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

More information:

Upgrade Considerations (see page 76)
Upgrade CA ARCserve Backup from a Previous Release (see page 97)

How to Verify a Centralized Management Environment Upgrade+

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

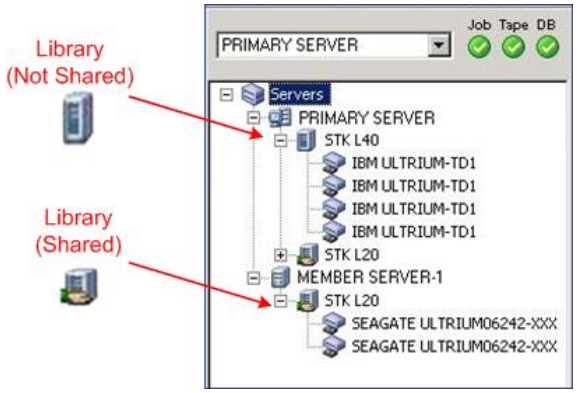
   Ensure that all previous backup data migrated successfully.

   Note: CA 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 CA 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 online help or 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

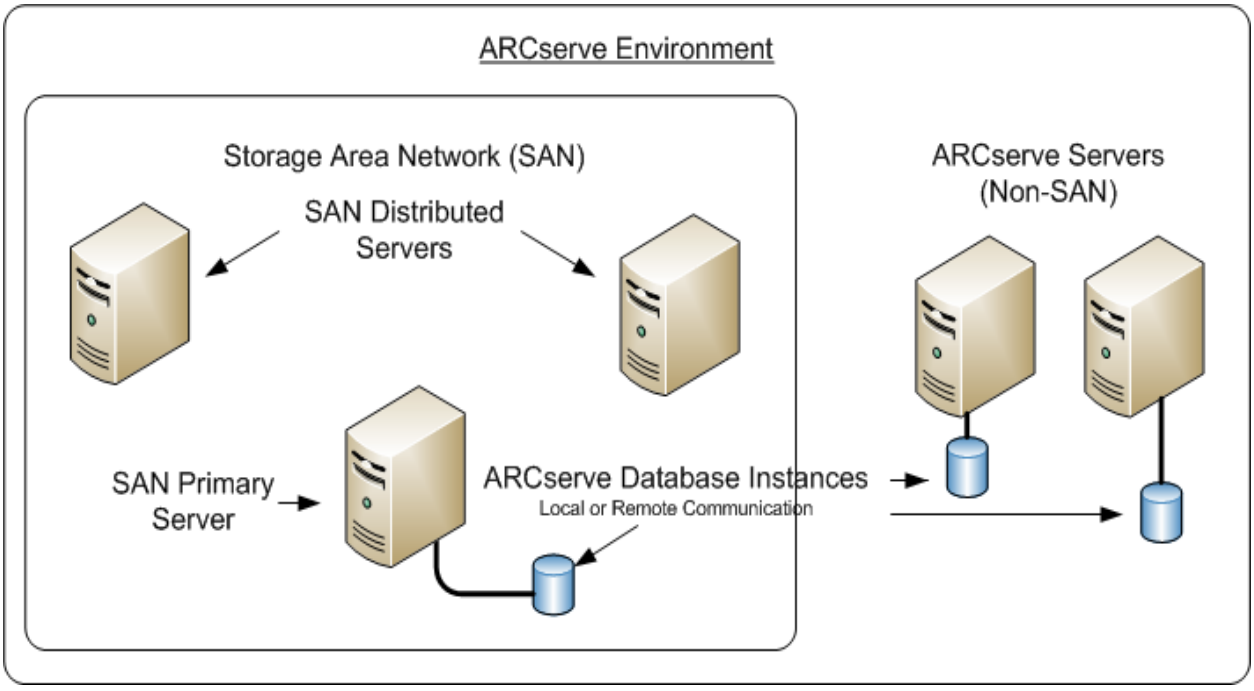
The following sections describe best practices that you can use to upgrade multiple ARCserve servers in a SAN and non-SAN environment to this release.

This section contains the following topics:

Current Configuration - Multiple ARCserve Servers in a SAN and Non-SAN Environment (see page 356)
Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers (see page 357)
New Components You Must Install (see page 359)
Components You Must Upgrade (see page 361)
How to Upgrade Multiple ARCserve Servers in a SAN and a Non-SAN Environment to this Release (see page 362)
How to Verify a Centralized Management Upgrade (see page 362)

Current Configuration - Multiple ARCserve Servers in a SAN and Non-SAN Environment

The following diagram illustrates the architecture of multiple CA ARCserve Backup servers in a SAN environment and non-SAN environment, using a local or remote database, in previous releases:



Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers

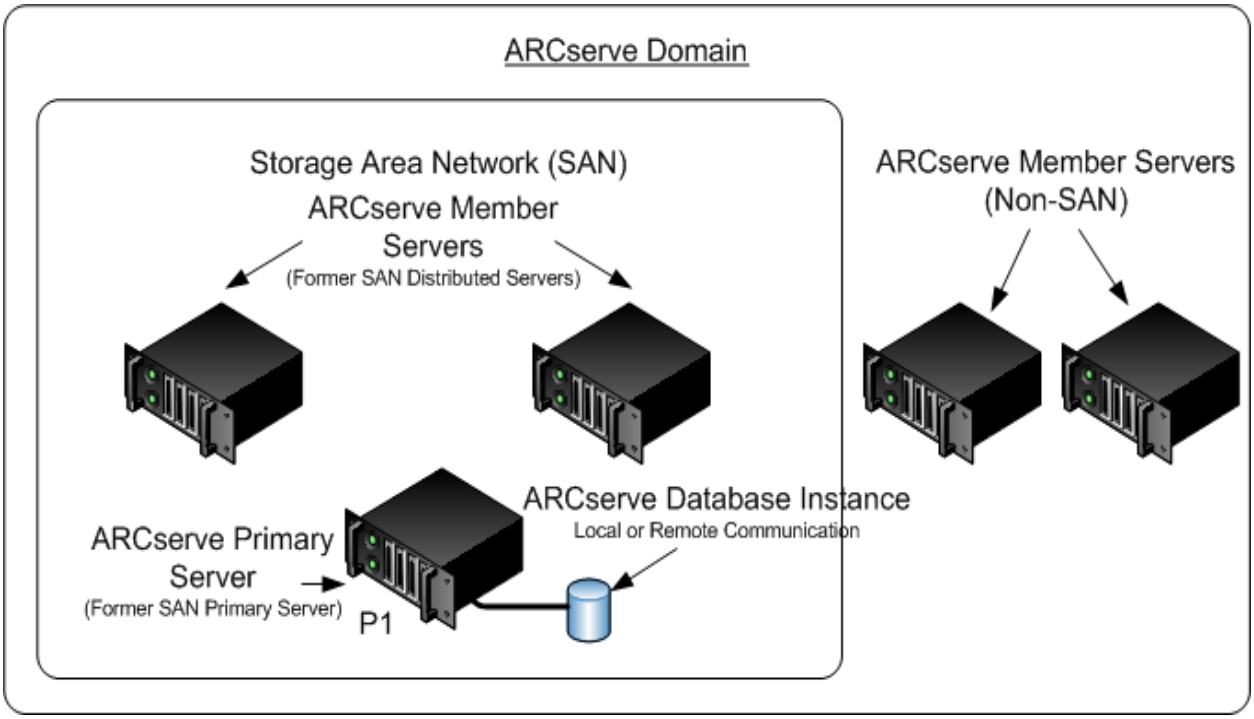
If your current configuration consists of a SAN environment where CA ARCserve Backup servers reside on the SAN and other CA ARCserve Backup servers do not reside on the SAN, the best practice is to install CA ARCserve Backup in a centrally managed environment.

To upgrade your current SAN environment to a centralized management environment, you must upgrade your current SAN primary server to a CA ARCserve Backup Primary Server, and then upgrade your SAN distributed servers to CA ARCserve Backup Member Servers.

To install member servers, the installation must be able to detect the CA ARCserve Backup domain name and the primary server name in your environment. You should therefore install CA 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 CA 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.



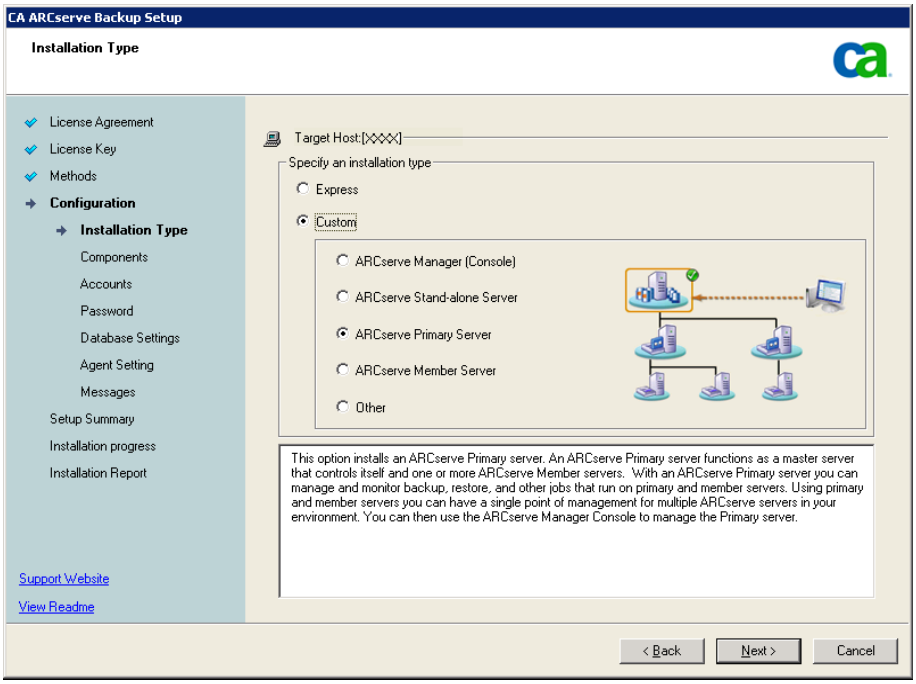
New Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 5: Setup: Installation Type dialog. ARCserve Primary Server is specified.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Tape Library Option

Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.

CA ARCserve Backup Storage Area Network (SAN) Option

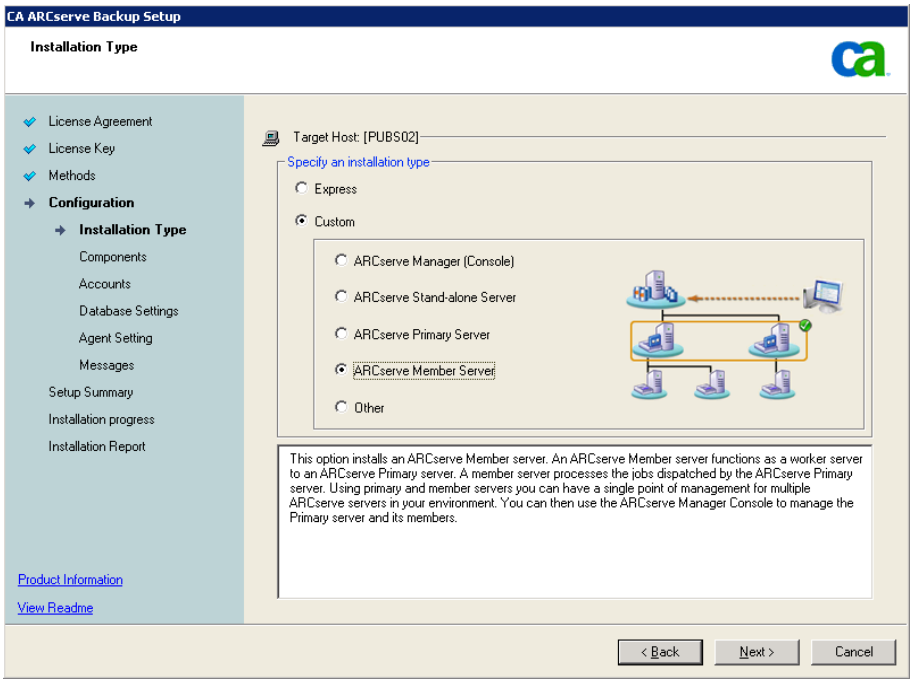
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Be aware of the following:

- The Tape Library Option is a prerequisite component for the Storage Area Network (SAN) Option.
- You must specify the CA ARCserve Backup Primary Server installation option to install the Storage Area Network (SAN) Option.

CA 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 CA 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

Complete the following tasks to upgrade ARCserve servers in a SAN and non-SAN environment to this release.

1. Install the CA 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 CA 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 CA ARCserve Backup database.

   When you are promoted, migrate the data from the previous release to the new database.

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

More information:

Upgrade Considerations (see page 76)
Upgrade CA ARCserve Backup from a Previous Release (see page 97)

How to Verify a Centralized Management Upgrade

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

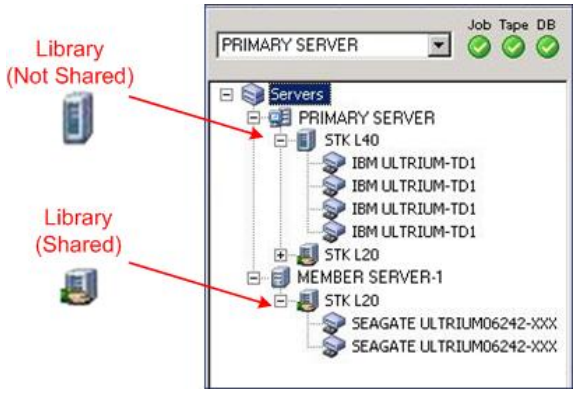
   Ensure that all previous backup data migrated successfully.

   Note: CA 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 CA 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 online help or 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.

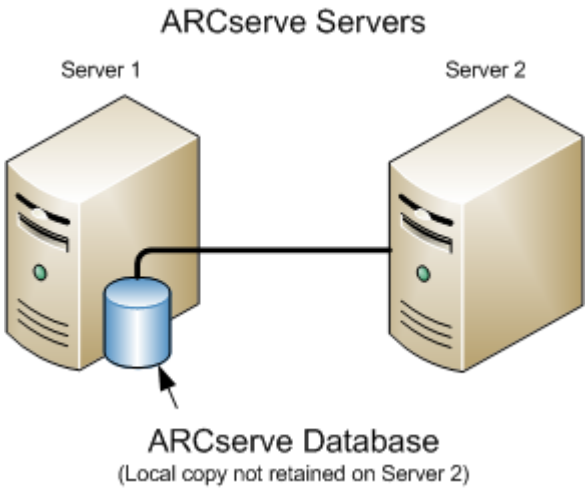
This section contains the following topics:

Current Configuration - Multiple ARCserve Servers Using a Central Database (see page 365)
Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers (see page 366)
New Components You Must Install (see page 367)
Components You Must Upgrade (see page 369)
How to Upgrade Multiple ARCserve Servers Using a Remote Database to a Centralized Management Environment (see page 369)
How to Verify a Centralized Management Upgrade (see page 370)

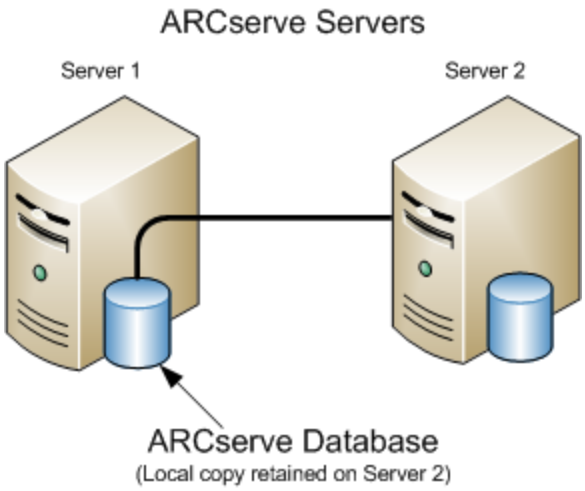
Current Configuration - Multiple ARCserve Servers Using a Central Database

The following diagram illustrates the architecture of multiple CA ARCserve Backup servers using a centralized database in previous releases.

In the following diagram, multiple CA ARCserve Backup servers are sharing a centralized database. A copy of the CA ARCserve Backup database is not retained on one of the servers sharing the database.



In the following diagram, multiple CA ARCserve Backup servers are sharing a centralized database. A copy of the CA ARCserve Backup database is retained on one of the servers sharing the database.



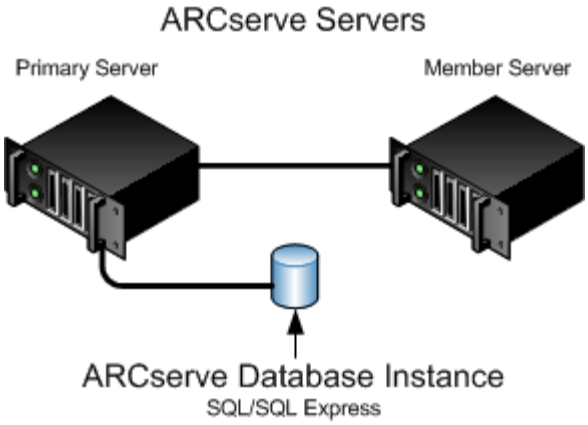
Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers

If your current configuration consists of multiple CA 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 CA ARCserve Backup database on the primary server or a remote system. You do not need to install CA ARCserve Backup on the system that hosts the CA ARCserve Backup database instance.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install CA 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 CA ARCserve Backup Primary Server and then upgrade all other systems to CA ARCserve Backup Member Servers.

The following diagram illustrates the architecture of a centralized management environment with a remote system hosting the CA ARCserve Backup database.



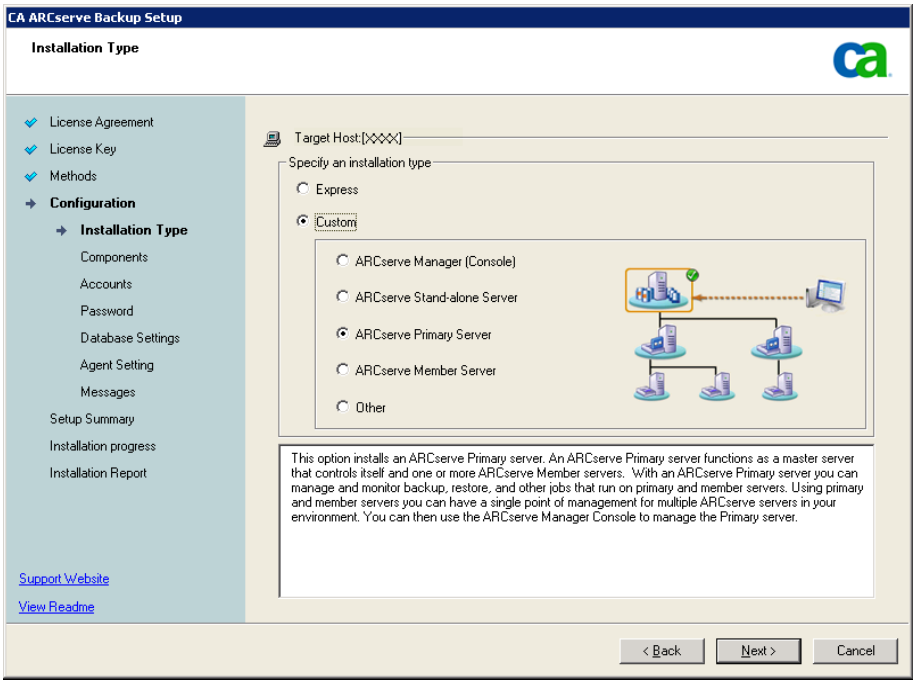
New Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 6: Setup: Installation Type dialog. ARCserve Primary Server is specified.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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 CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA 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 CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

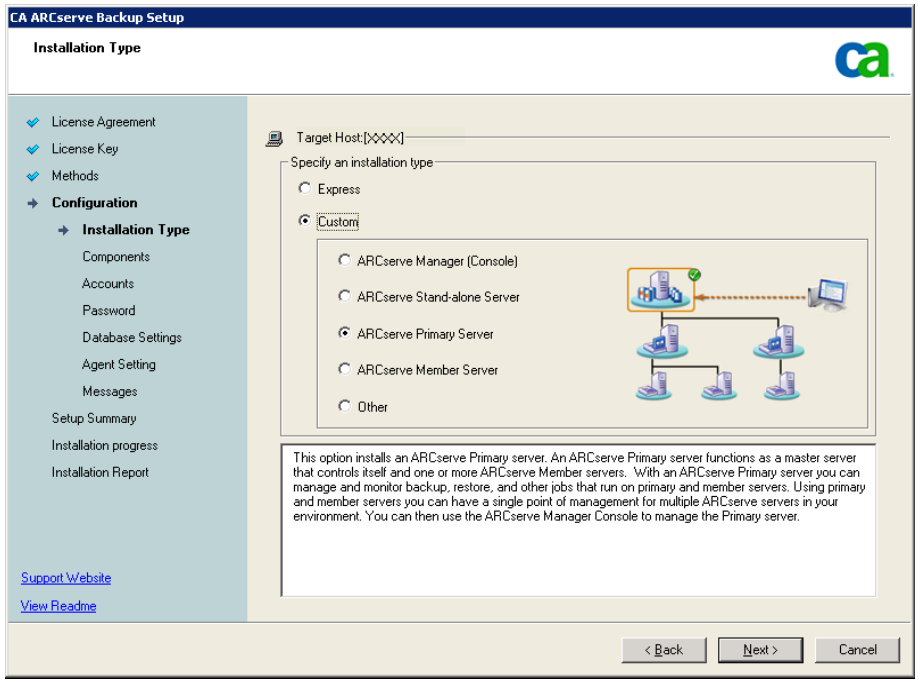
CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 7: Setup: Installation Type dialog. ARCserve Primary Server is specified.



Components You Must Upgrade

To deploy this configuration in your environment, you must upgrade the following CA 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

Complete the following tasks to upgrade multiple ARCserve servers using a centralized database to this release.

1. Install the CA 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 CA ARCserve Backup Primary Server.

   You can specify Microsoft SQL Server 2008 Express or Microsoft SQL Server for the CA ARCserve Backup database.

   When you are promoted, migrate the data from the previous release to the new database.

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

More information:

Upgrade Considerations (see page 76)
Upgrade CA ARCserve Backup from a Previous Release (see page 97)

How to Verify a Centralized Management Upgrade

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA ARCserve Backup Manager Console on the primary server.
2. Open the Server Admin.

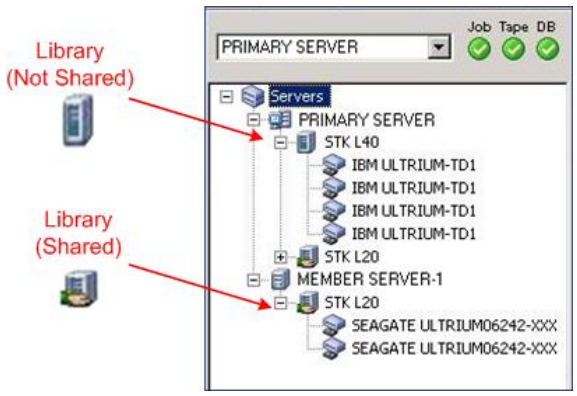
   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.
3. Open the Database Manager and the Job Status Manager.

   Ensure that you can view database information and Activity Log data.

   CA 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 CA 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 online help or 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.

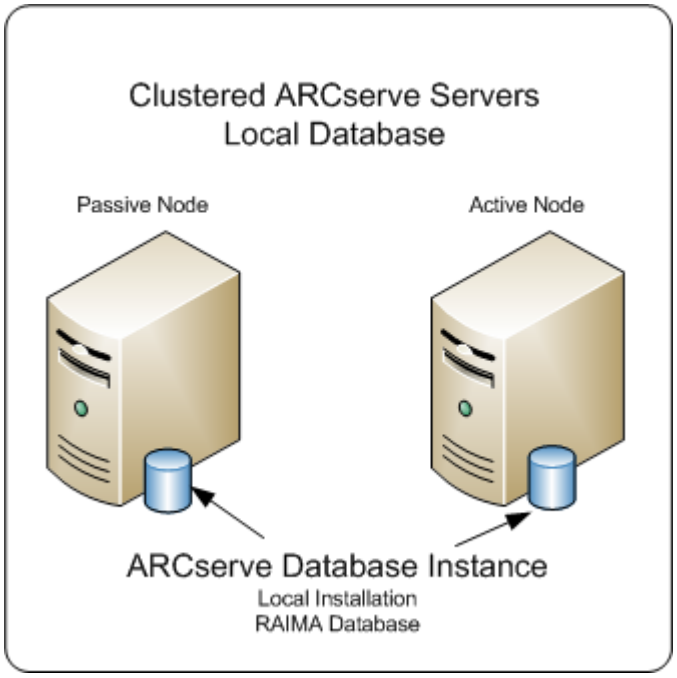
Important! The following best practices only apply to upgrading a BrightStor ARCserve Backup r11.5 cluster-aware environment. For all other releases, you must uninstall the previous release and then install CA ARCserve Backup into the cluster-aware environment.

This section contains the following topics:

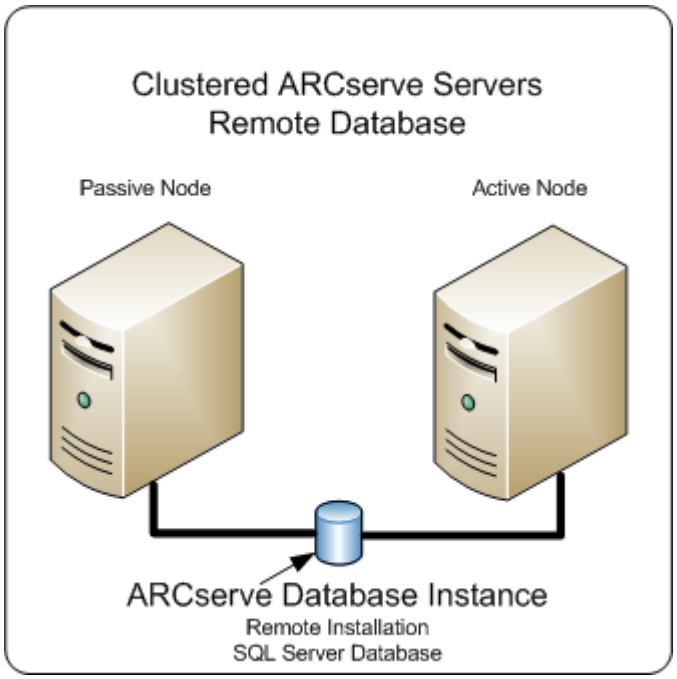
Current Configuration - Multiple ARCserve Servers in a Cluster (see page 372)
Recommended Configuration - ARCserve Primary and Members Servers Installed in a Cluster-aware Environment (see page 373)
New Components You Must Install (see page 376)
Components You Must Upgrade (see page 377)
How to Upgrade an ARCserve Cluster-aware Environment to this Release (see page 378)
How to Verify a Cluster-aware Upgrade (see page 378)

Current Configuration - Multiple ARCserve Servers in a Cluster

The following diagram illustrates the architecture of multiple CA ARCserve Backup servers in a cluster-aware environment in previous releases. The CA ARCserve Backup database is hosted by a RAIMA database and the CA ARCserve Backup database instance resides on the CA ARCserve Backup server.



The following diagram illustrates the architecture of multiple CA ARCserve Backup servers in a cluster-aware environment in previous releases. The CA ARCserve Backup database is hosted by Microsoft SQL Server and the CA ARCserve Backup database instance resides on a remote system.



Recommended Configuration - ARCserve Primary and Members Servers Installed in a Cluster-aware Environment

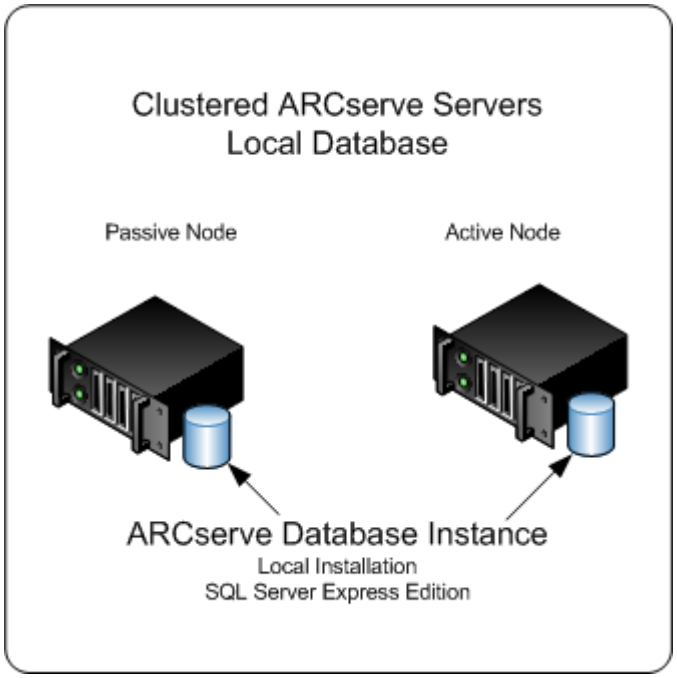
If your current configuration consists of multiple CA ARCserve Backup servers in a cluster-aware environment, the best practice is to upgrade to multiple CA ARCserve Backup Primary Servers or multiple CA ARCserve Backup Stand-alone Servers.

This architecture lets you centrally manage your CA ARCserve Backup environment and maintain the high availability capabilities of a cluster-aware environment.

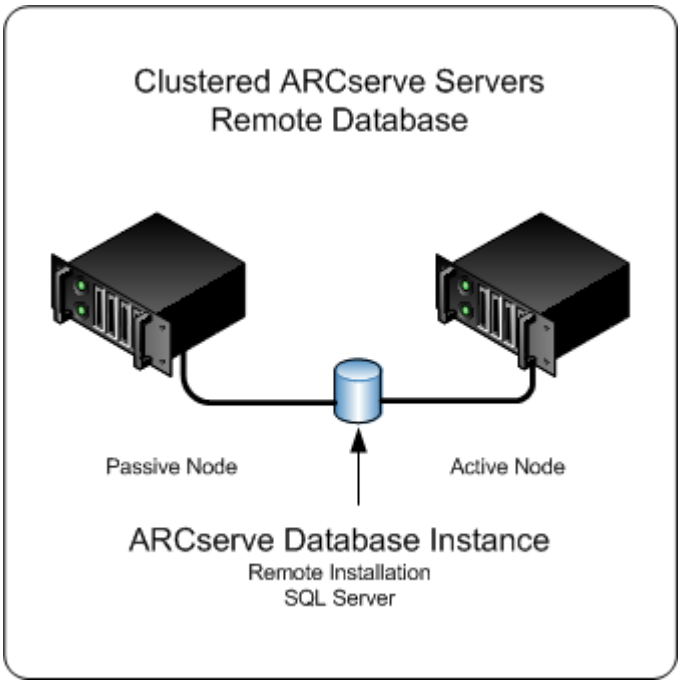
To deploy this configuration in your environment, you can use Microsoft SQL Server 2008 Express Edition or Microsoft SQL Server to host the CA ARCserve Backup database.

Note: Microsoft SQL Server 2008 Express Edition does not support remote communication. When you install CA 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 CA ARCserve Backup servers in a cluster-aware environment in this release. The CA ARCserve Backup database is hosted using Microsoft SQL Server 2008 Express Edition and the CA ARCserve Backup database instance resides on the CA 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.



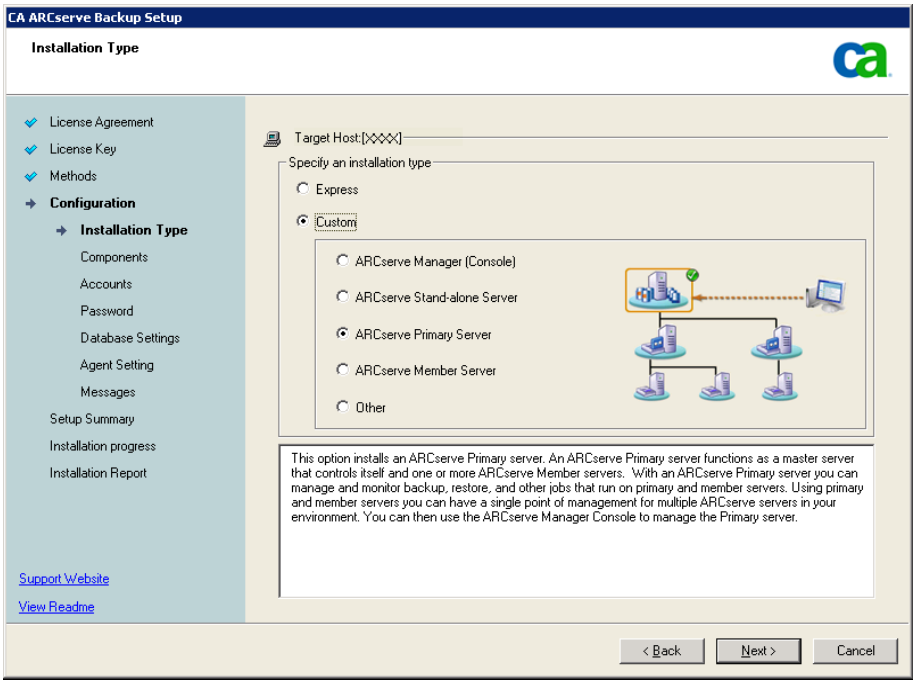
New Components You Must Install

To deploy this configuration in your environment, you must install the following CA ARCserve Backup components:

CA ARCserve Backup Primary Server

Lets you install CA 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.

Equation 8: Setup: Installation Type dialog. ARCserve Primary Server is specified.



CA ARCserve Backup Central Management Option

Lets you manage the primary server and all member servers in a CA ARCserve Backup domain from a central computer.

Note: The CA ARCserve Backup Primary Server is a prerequisite component.

CA ARCserve Backup Agent for Microsoft SQL Server

Lets you protect the CA 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.

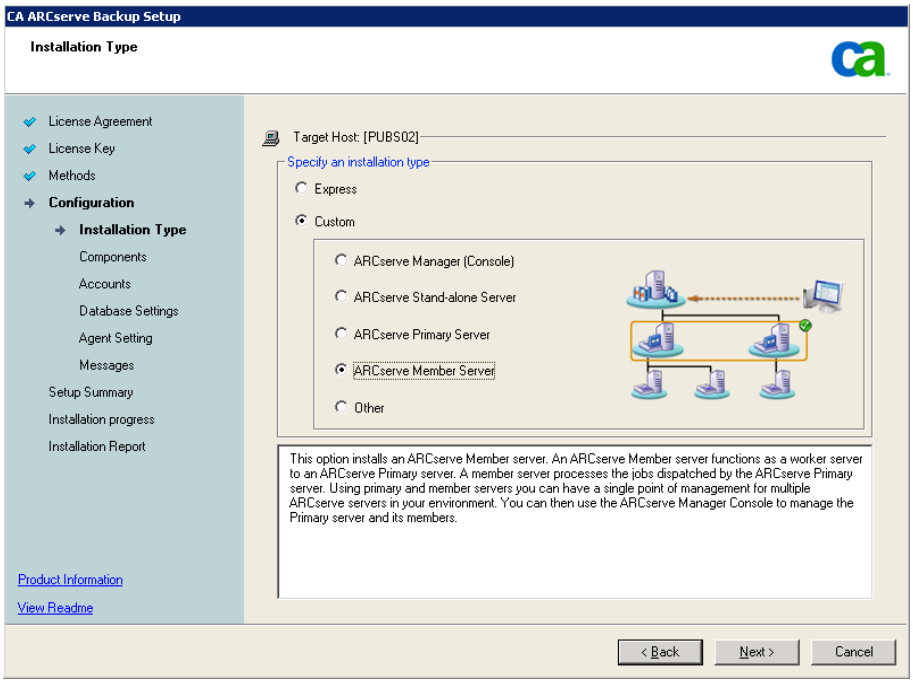
Important! The uninstallation routine does not uninstall the CA ARCserve Backup database instance from your computer. If you find it necessary to reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2008 Express Edition database instance on your system. As a result, the installation wizard automatically selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

CA ARCserve Backup Client Agent for Windows

Lets you back up data locally to the CA ARCserve Backup server.

CA 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 CA ARCserve Backup components:

- All components that are installed in your current ARCserve environment.

How to Upgrade an ARCserve Cluster-aware Environment to this Release

You can upgrade CA ARCserve Backup to a cluster environment with job failover capability on the following cluster platforms:

- Microsoft Cluster Server (MSCS) in x86/AMD64/IA64 Windows Server
- NEC CLUSTERPRO/ExpressCluster for Windows 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, and CLUSTERPRO/ExpressCluster X 2.0 for Windows.

Important! CA ARCserve Backup supports upgrading from BrightStor ARCserve Backup r11.5 to this release. For all previous releases, you must uninstall BrightStor ARCserve Backup and then install CA ARCserve Backup.

To upgrade an ARCserve cluster-aware environment to this release

1. Upgrade CA ARCserve Backup using one of the following procedures:
   - Upgrade CA ARCserve Backup from r11.5 to r15 in a MSCS Cluster Environment (see page 151).
   - Upgrade CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO Environment (see page 180).
2. Verify the upgrade.
3. (Optional) CA ARCserve Backup does not support recovering the CA ARCserve Backup database when the last backup of the CA ARCserve Backup database was completed before you upgraded to this release. As a best practice, you should back up the CA ARCserve Backup database as soon as possible after the upgrade is complete. For information about backing up the CA ARCserve Backup database, see the *Administration Guide*.

How to Verify a Cluster-aware Upgrade

To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

1. Open the CA 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.

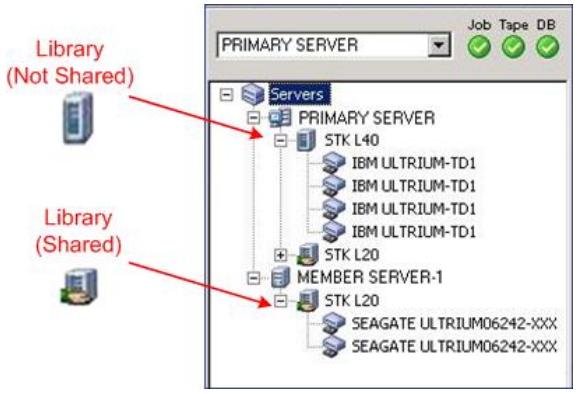
5. Open the Job Status Manager.

   Ensure that all data from the previous installation migrated to the new primary server. CA 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 CA 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 online help or 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 CA ARCserve Backup.

This section contains the following topics:

Where to Install the Manager Console (see page 381)
How to Install and Manage Licenses (see page 381)
How to Install CA ARCserve Backup Server-Based Options (see page 385)

Where to Install the Manager Console

The CA 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 CA 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 CA ARCserve Backup Server components. Refer to the readme file for a description of the minimum system requirements that your system needs to install the CA 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 CA ARCserve Backup licenses.

This section contains the following topics:

Manage CA ARCserve Backup Component Licenses (see page 382)
Release Licenses from Servers (see page 384)

Manage CA ARCserve Backup Component Licenses

The CA ARCserve Backup Server Admin lets you perform the following license management tasks:

- View the CA ARCserve Backup products installed on a primary server, stand-alone server, member servers, and agent servers in a CA ARCserve Backup domain.
- Identify the total number of licenses applied and the number of active licenses for each component in a CA ARCserve Backup domain.
- View the names of the servers using the component licenses in a CA ARCserve Backup domain.
- Release licenses from servers to make the licenses available to other servers in your domain.

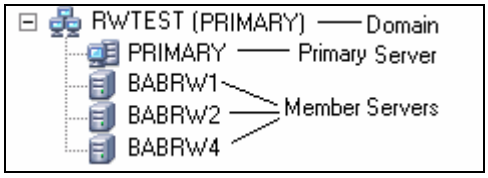
  Note: For information about releasing licenses from servers, see Release Licenses from Servers (see page 384).

To manage CA ARCserve Backup component licenses

1. From the CA ARCserve Backup Manager Console, open the Server Admin by clicking Server Admin in the Quick Start menu.

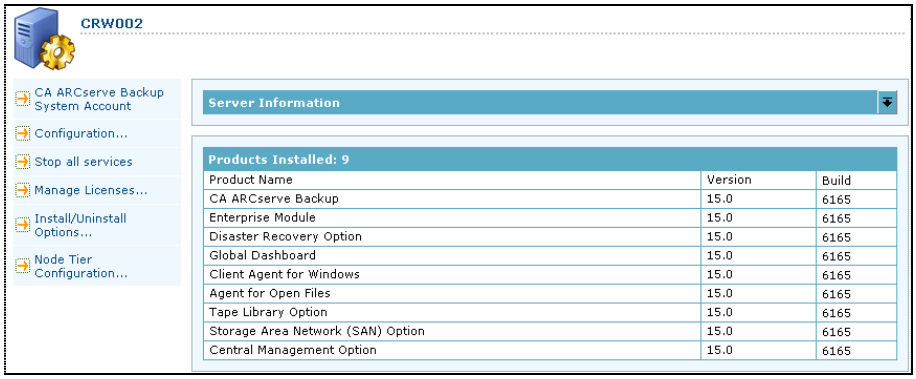
   The Server Admin opens.

   The CA ARCserve Backup primary server and its member servers display in a directory tree structure as illustrated by the following:



2. To view the CA 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 CA 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.

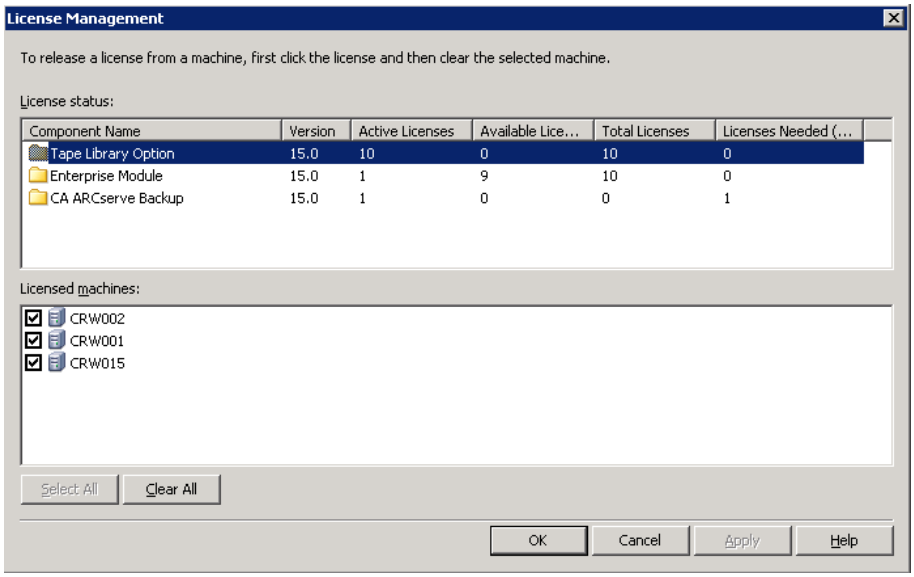
     Examples:

     - You are using one purchased license and one trial license for a component. CA 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. CA 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

CA 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 CA 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 CA 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 CA 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 CA ARCserve Backup Primary Server.

- Tape Library Option
- Storage Area Network (SAN) Option

There are two methods that you can use to install the CA ARCserve Backup server-based options:

- Install these options when you install CA 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:

RSA Data Security, Inc. Acknowledgement (see page 387)

RSA Data Security, Inc. Acknowledgement

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.

Index

A

about this guide • 14
Acknowledgements • 389
Additional Resources - Firewall Ports Specifications • 259
Agent for ARCserve Database • 72
Agent for Microsoft Exchange Server Communication Ports • 251
Agent for Microsoft SharePoint Server Communication Ports • 250
Agent for Microsoft SharePoint Server Database Communication Ports • 252
Agent for Microsoft SQL Server Communication Ports • 252
Allow Database Agents that Reside on Remote Subnets to Communicate with the ARCserve Server • 218
ALP Key Certificate • 81
Alternate Data Path Considerations • 23
Amount of Disk Space Required to Install CA ARCserve Backup • 60
ARCserve database
  data migration from a previous release • 80
  installation methods • 61
  start the ARCserve database protection job • 219
  supported applications • 67
ARCserve servers
  ARCserve server types • 61, 62
  member server • 62
  primary server • 62
  server options • 66
  stand-alone server • 62

B

Backup Data Storage Requirements • 26
Backup Schedule Requirements • 18
Backup Scope • 24
Backward Compatibility • 78
backwards compatibility • 78
Base Product Communicating with the Agent for Microsoft SQL Server • 255
Base Product Communication with CA ARCserve Backup Agents and Options • 248
Best Practices for Installing CA ARCserve Backup • 283
Best Practices for Upgrading CA ARCserve Backup from a Previous Release • 325
Binary Files Containing Incorrect File Version Information • 53
Binary Files that are not Uninstalled Completely • 54
Binary Files that do not Contain an Embedded Manifest • 56
Budget Considerations • 16

C

CA Antivirus • 199
CA Antivirus Integration • 199
CA ARCserve Backup Agent Deployment • 111
CA ARCserve Backup Dashboard for Windows Firewall Communication Configuration • 258
CA ARCserve Backup Database Agents Communication Ports • 253
CA ARCserve Backup File System Agents Release Levels • 82
CA ARCserve Backup Home Page • 203
CA ARCserve Backup MSI Installer Package Identification • 58
CA ARCserve Backup Patch Manager Integration • 200
CA ARCserve Backup Server Options • 66
CA ARCserve Backup Services Fail to Initialize • 278
CA ARCserve Backup System Account • 214
CA ARCserve Backup, introduction • 13
CA ARCserve Replication Integration • 199
CA Product References • iii
caroot User Account • 66
Catastrophic Events • 29
Client Agent for Windows Communication Ports • 250
Cluster HA Resources Not Created • 282
clusters
  deployment considerations • 135
clusters, MSCS clusters
  cldelete cluster resources • 162
  deployment planning • 136
  hardware requirements • 139

remove CA ARCserve Backup from cluster • 161
resource preparation • 139
software requirements • 139
clusters, NEC clusters • 163
deployment planning • 136
disable cluster scripts • 187
enable cluster scripts • 190
hardware requirements • 163
remove CA ARCserve Backup from cluster • 197
resource preparation • 164
software requirements • 164
code pages
about • 212
configuration, Backup Manager • 213
configuration, Restore Manager • 214
Code Pages • 212
Common Agent for UNIX and Linux Communication Ports • 249
communication port, Global Dashboard • 248
communication ports, firewall • 239, 259
Components and Prerequisites • 127
Components You Must Install • 287, 292, 299, 306, 314, 321
Components You Must Upgrade • 332, 338, 345, 354, 363, 371, 379
Configure a Branch Site • 228
Configure Devices Using the Device Wizard • 222
Configure Enterprise Module Components • 223
Configure Global Dashboard • 223
Configure the Central Site • 225
Configure the Windows Firewall to Optimize Communication • 216
Configuring CA ARCserve Backup • 201
Configuring Your Firewall to Optimize Communication • 236
Contact CA • v
Create a Silent Installation Response File • 105
Create File System Devices • 232
Current Configuration - ARCserve Stand-alone Server • 328
Current Configuration - Multiple ARCserve Servers in a Cluster • 374
Current Configuration - Multiple ARCserve Servers in a Domain • 335
Current Configuration - Multiple ARCserve Servers in a SAN and Non-SAN Environment • 358
Current Configuration - Multiple ARCserve Servers in a SAN Using a Local or Remote Database • 349
Current Configuration - Multiple ARCserve Servers Sharing a Remote Database • 342
Current Configuration - Multiple ARCserve Servers Using a Central Database • 367

D

Data Backup Window Considerations • 18
Data Migration from a Previous Release • 80
Data Path Considerations • 22
Data Transfer Requirements • 17
Data Transfer Requirements and Resources Calculations • 21
database
data migration from a previous release • 80
MS SQL configuration • 69, 221
ODBC data source configuration • 221
Database Consistency Checks • 221
Database Requirements • 67
Delete CA ARCserve Backup Cluster Resources • 162
Deploy Agents to Remote Hosts Using Automatic Upgrade • 114
Deploy Agents to Remote Hosts Using Custom Deployment • 116
Deploy Agents to VMs Using Virtual Machine Deployment • 120
Deploy CA ARCserve Backup Server on MSCS • 138
Deploy CA ARCserve Backup Server on NEC Cluster • 163
Deployment Considerations • 135
Device Configuration
Device Wizard • 222
Device Wizard • 222
devices, supported • 39
Disable CA ARCserve Backup in NEC Cluster Scripts • 187
Disaster Recovery Archive Considerations • 31
Disaster Recovery Testing • 31
Discovery Service Communication Ports • 249
Documentation Changes • vi

E

Enable CA ARCserve Backup in NEC Cluster Scripts • 190
engines
  service state icons • 208
Enterprise Storage Requirements • 16
Examples of How You Can Modify the Ports Configuration File • 261
External Ports Used for Communication • 239

F

Factors Affecting Storage Capacity Calculations • 29
file system agents, release levels • 82
file system devices, creating • 232
Fine-Tune the CA ARCserve Backup SQL Server Database • 220
firewall configuration • 236, 237, 238
firewall configuration, Windows • 216
First-Time Home Page and User Tutorial • 207

G

General Best Practices • 382
Global Dashboard
  configure Branch Primary Server • 228
  configure Central Primary Server • 225
  configure Global Dashboard • 223, 225, 228
  considerations • 75
  installation prerequisites • 83
  server communication • 248
Global Dashboard Considerations • 75
Global Dashboard Data Storage Requirements • 27
Global Dashboard Server Communication • 248
Global Dashboard Upgrades • 79
GUI Communication to CA ARCserve Backup Agents • 254
GUI Managing the Agent for Microsoft Exchange Server Using Named Pipes • 256
GUI Managing the Base Product • 257

H

Hardware Data Transfer Rates • 18
home page • 203
How CA ARCserve Backup Manages Authentication • 215
How CA ARCserve Backup Supports Multiple Code Pages • 212
How the Installation Process Affects Operating Systems • 40
How to Allow Agents and Database Agents to Communicate through a Firewall • 254
How to Calculate the Number of Required SQL Connections • 221
How to Complete Prerequisite Tasks • 83
How to Complete Prerequisite Tasks for Installing CA ARCserve Backup • 284
How to Complete Prerequisite Tasks for Upgrading CA ARCserve Backup • 326
How to Define Include and Skip Parameters for CA ARCserve Backup Database Agents • 235
How to Enable TCP/IP Communication on Microsoft SQL Server Databases • 72
How to Install a Primary Server with Member Servers • 294
How to Install a Primary Server with Member Servers and Devices • 301
How to Install a Primary Server with Member Servers and Shared Devices in a SAN • 308
How to Install a Stand-alone Server or Primary Server • 288
How to Install and Manage Licenses • 383
How to Install CA ARCserve Backup into a Cluster-aware Environment • 323
How to Install CA ARCserve Backup Server-Based Options • 387
How to Install CA ARCserve Backup Using Unicenter Software Delivery • 126
How to Install Multiple Primary Servers with Member Servers in a SAN • 316
How to Upgrade an ARCserve Cluster-aware Environment to this Release • 380
How to Upgrade Multiple ARCserve Servers in a SAN and a Non-SAN Environment to this Release • 364
How to Upgrade Multiple ARCserve Servers in a SAN to This Release • 355
How to Upgrade Multiple ARCserve Servers Sharing a Database to a Centralized Management Environment • 346
How to Upgrade Multiple ARCserve Servers to a Centralized Management Environment • 339
How to Upgrade Multiple ARCserve Servers Using a Remote Database to a Centralized Management Environment • 371
How to Upgrade to an ARCserve Stand-alone Server • 332

How to Use the System Account for Job Security • 215
How to Verify a Centralized Management Environment Upgrade • 346
How to Verify a Centralized Management Environment Upgrade+ • 355
How to Verify a Centralized Management Upgrade • 364, 372
How to Verify a Cluster-aware Installation • 323
How to Verify a Cluster-aware Installation and Upgrade • 198
How to Verify a Cluster-aware Upgrade • 380
How to Verify a Domain with a Primary Server and Member Servers Upgrade • 339
How to Verify a Multiple Primary Servers with Member Servers in a SAN Installation • 317
How to Verify a Primary Server with Member Servers and Devices Installation • 301
How to Verify a Primary Server with Member Servers and Shared Devices in a SAN Installation • 309
How to Verify a Primary Server with Member Servers Installation • 294
How to Verify a Stand-alone Server Installation • 288
How to Verify a Stand-alone Server or Primary Server Upgrade • 332

I

install CA ARCserve Backup • 88
Install CA ARCserve Backup • 88
Install CA ARCserve Backup Components Using Unicenter Software Delivery • 132
Install CA ARCserve Backup in an MSCS Cluster-aware Environment • 140
Install CA ARCserve Backup in an NEC Cluster-aware Environment • 165
installation • 71
installation considerations
  Microsoft SQL Server • 69
  Microsoft SQL Server 2008 Express Edition • 67
  remote database • 71
  supported upgrades • 77
installation methods • 61
Installation Methods • 61
Installation Progress Logs • 74
installation wizard • 61
Installing a Primary Server with Member Servers • 289
Installing a Primary Server with Member Servers and Devices • 296
Installing a Primary Server with Member Servers and Shared Devices in a SAN • 303
Installing and Upgrading CA ARCserve Backup • 83
Installing and Upgrading CA ARCserve Backup in a Cluster-aware Environment • 135
Installing CA ARCserve Backup into a Cluster-aware Environment • 319
Installing CA ARCserve Backup into a Single-server Environment • 285
Installing Multiple Primary Servers with Member Servers in a SAN • 311
installtation progress logs • 74
Integrating CA ARCserve Backup with Other Products • 199
integrating products
  CA Antivirus • 199
Introducing CA ARCserve Backup • 13
Introduction • 13
Introduction to Cluster-aware Installations • 135
introduction, CA ARCserve Backup • 13

L

language settings • 212
licensing
  ALP certificate • 81
  managing • 384
  release licenses • 386
  requirements • 81
log in to CA ARCserve Backup • 208
Log in to CA ARCserve Backup • 208

M

Manage CA ARCserve Backup Component Licenses • 384
Manager Console
  opening • 201
  specify preferences • 210
  upgrades • 79
Manager Console Communication with the Base Product • 243
Manager Console Support for Previous Releases • 79
Mastersetup • 126

Media Capacities • 28
member server • 62
Microsoft SQL Server
  database consistency check • 221
  installation considerations • 69
  ODBC configuration • 221
  SQL connections • 221
Microsoft SQL Server 2008 Express Edition
  installation considerations • 67
Microsoft SQL Server 2008 Express Edition Considerations • 67
Microsoft SQL Server Database Considerations • 69
Modify the Ports Configuration File • 238
MSCS Cluster Resource Preparation • 139
MSCS clusters
  delete cluster resources • 162
  deployment planning • 136
  hardware requirements • 139
  remove CA ARCserve Backup from cluster • 161
  resource preparation • 139
  software requirements • 139
MSCS Hardware Requirements • 139
MSCS Software Requirements • 139

N

NDMP NAS Option Communication Ports • 253
NEC CLUSTERPRO/ExpressCluster Hardware Requirements • 163
NEC CLUSTERPRO/ExpressCluster Resource Preparation • 164
NEC CLUSTERPRO/ExpressCluster Software Requirements • 164
NEC clusters • 163
  deployment planning • 136
  disable cluster scripts • 187
  enable cluster scripts • 190
  hardware requirements • 163
  remove CA ARCserve Backup from cluster • 197
  resource preparation • 164
  software requirements • 164
Network and Computer Infrastructure Requirements • 17
Network Bandwidth Considerations • 20
Network Enhancements • 22
New Components You Must Install • 330, 337, 344, 352, 361, 369, 378

O

Off-Site Repository Considerations • 30
Online Recovery Data Storage Requirements • 26
Open the Manager or Manager Console • 201
options
  Discovery Configuration options • 249
  global preferences • 210

P

Parallel Storage Operations (Multiple Streaming) • 25
Plan Your CA ARCserve Backup HA Deployment • 136
Planning Your CA ARCserve Backup Installation • 39
planning your environment
  backup window • 18
  bandwidth • 20
  budget • 16
  capacities • 26
  data transfer rates • 21
  hardware throughput • 18
  infrastructure • 17
  network enhancements • 22
  parallel storage • 25
  recovering from a disaster • 31
  sample calculations • 31
  scheduling • 18
  vault accessibility and security • 30, 31
Planning Your Storage Environment • 15
platforms, supported • 39
ports configuration • 237, 238, 263
Ports Configuration File Configuration Considerations • 263
Ports Configuration File Guidelines • 237
Ports Used by CA ARCserve Backup Agents and Options • 249
Ports Used by CA ARCserve Backup Common Components • 248
Ports Used by CA ARCserve Backup Components • 239
Ports Used by the CA ARCserve Backup Base Product • 240
post-installation tasks • 133, 223
Post-Installation Tasks • 133
Preliminary Tasks • 15
prerequisite installation tasks • 83
primary server • 62

Primary Server and Member Server Communication Ports • 243
Product License Requirements • 81
Purpose of This Guide • 14

R

Recommended Configuration • 290, 297, 304, 312, 320
Recommended Configuration - ARCserve Primary and Members Servers Installed in a Cluster-aware Environment • 375
Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers • 335, 343, 359, 368
Recommended Configuration - CA ARCserve Backup Domain with a SAN Primary Server and SAN Distributed Servers • 350
Recommended Configuration - CA ARCserve Backup Stand-alone Server or Primary Server • 329
Recommended Configuration - Stand-alone Server • 285
Register CA ARCserve Backup on the Unicenter Software Delivery Server • 126
Release Licenses from Servers • 386
Remote Database Considerations • 71
response file, creating • 105
Risk Assessment • 30
RSA Data Security, Inc. Acknowledgement • 389

S

Sample Calculations • 32
SCSI Bus and Device Enhancements • 22
SCSI or Fibre Interface Considerations • 19
Segment Data • 23
Segment Your Network • 23
service state icons • 208
Service State Icons • 208
Setup Cannot Communicate with Remote Microsoft SQL Server Databases • 275
silent installation
  create a response file • 105
  installation methods • 61
Specify CA ARCserve Backup Manager Preferences • 210
Specify Code Pages in the Backup Manager Window • 213
Specify Code Pages in the Restore Manager Window • 214
specify Manager Console preferences • 210
Specify ODBC Communication for Remote Database Configurations • 221
stand-alone server • 62
start the ARCserve database protection job • 219
Start the CA ARCserve Backup Database Protection Job • 219
start.bat Script Changes for Member Servers and Non-SQL Express Primary Servers • 176
start.bat Script Changes for SQL Express Primary Servers • 178
stop.bat Script Changes for Member Servers and Non-SQL Express Primary Servers • 177
stop.bat Script Changes for SQL Express Primary Servers • 179
Storage Area Network (SAN) • 40
Storage Area Network (SAN) Installations • 40
Storage Area Networks • 22
Storage Capacities and Resources • 28
Storage Capacity for Two Sets of Recovery Data, One Full and One Incremental Backup • 37
Storage Capacity Requirements • 26
supported devices • 39
Supported Devices • 39
supported platforms • 39
Supported Platforms • 39
supported upgrades • 77
Supported Upgrades • 77
system account
  job security • 215
  manage authentication • 215
system requirements • 83

T

Tape Drive Considerations • 19
tape libraries • 40
Tape Library Installations • 40
Test Communication Through a Firewall • 265
Testing Plans and Assumptions • 29
The Tape Engine Does Not Start on Member Server Upgrades • 279
Transfer Rate for a Server With No Clients • 35
Transfer Rate for Clients and Servers on a 100Base-T Ethernet LAN With No Subnets • 33
Transfer Rate for Clients and Servers on a Gigabit Ethernet Network • 35

Transfer Rate for Clients and Servers on Two 100Base-T Ethernet Subnets • 34
Transfer Rate For Server With SAN Option • 36
Troubleshooting Your Installation • 275
Types of CA ARCserve Backup Server Installations • 62

U

Unable to Determine What Devices Are Supported by CA ARCserve Backup • 281
Unable to Log In to CA ARCserve Backup After Installing This Release • 277
Unable to Log in to CA ARCserve Backup After Upgrading to This Release • 280
Unicenter software delivery
  install CA ARCserve Backup • 126
  installation methods • 61
Uninstall Agent Deployment Setup Files • 273
uninstall CA ARCserve Backup
  MSCS cluster • 161
  NEC cluster • 197
  primary, member, and stand-alone server • 267
Uninstall CA ARCserve Backup • 267
Uninstall CA ARCserve Backup Components Using the Command Line • 270
Uninstall CA ARCserve Backup from a NEC CLUSTERPRO/ExpressCluster • 197
Uninstall CA ARCserve Backup from an MSCS Cluster • 161
Uninstalling CA ARCserve Backup • 267
Unsigned Binary Files • 47
Upgrade CA ARCserve Backup Agents Silently to the Current Release • 123
Upgrade CA ARCserve Backup from a Previous Release • 97
Upgrade CA ARCserve Backup from r11.5 to r15 in an MSCS Cluster Environment • 151
Upgrade CA ARCserve Backup from r11.5 to r15 in an NEC CLUSTERPRO Environment • 180
Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an MSCS Cluster Environment • 157
Upgrade CA ARCserve Backup from r12 or r12.5 to r15 in an NEC CLUSTERPRO Environment • 193
Upgrade Considerations • 76
upgrade, from a previous release • 88
upgrades
  backwards compatibility • 78
  data migration from a previous release • 80
  installation methods • 61
  Manager Console • 78
  supported • 77
Upgrading a Stand-alone Server or Primary Server • 328
Upgrading Multiple Servers in a Cluster-aware Environment • 374
Upgrading Multiple Servers in a SAN and Non-SAN Environment to this Release • 358
Upgrading Multiple Servers Using a Central Database • 366
Upgrading Multiple Stand-alone Servers in a Domain • 334
Upgrading Multiple Stand-alone Servers Sharing a Remote Database • 342
Upgrading Servers in a SAN Using a Local or Remote Database • 349
user tutorial • 207
Using Best Practices to Install and Upgrade CA ARCserve Backup • 283

V

Vault Accessibility Considerations • 31
Vault Expense Considerations • 31
Vault Security Considerations • 30

W

Where to Install the Manager Console • 383
Windows MSI Installer Package Custom Columns • 59