CA ARCserve® Backup for Windows

Implementation Guide

r12

CA Product References

This documentation set references the following CA products:

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

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

Contact Technical Support

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

Contents

Chapter 1: Introducing CA ARCserve Backup

This section contains the following topics:

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
- 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

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 × minbandwidth
```

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

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

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

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

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

Data Path Considerations

If you cannot decrease the amount of data that you need to move in the time available, then a possible solution is to increase the available bandwidth. You can do this either on the network that links data hosts to the 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.

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.

Note: You can simplify the pilot tests by using file system devices. You can set file system devices to /dev/null, thereby eliminating the requirement of dedicated disk space for pilot 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.

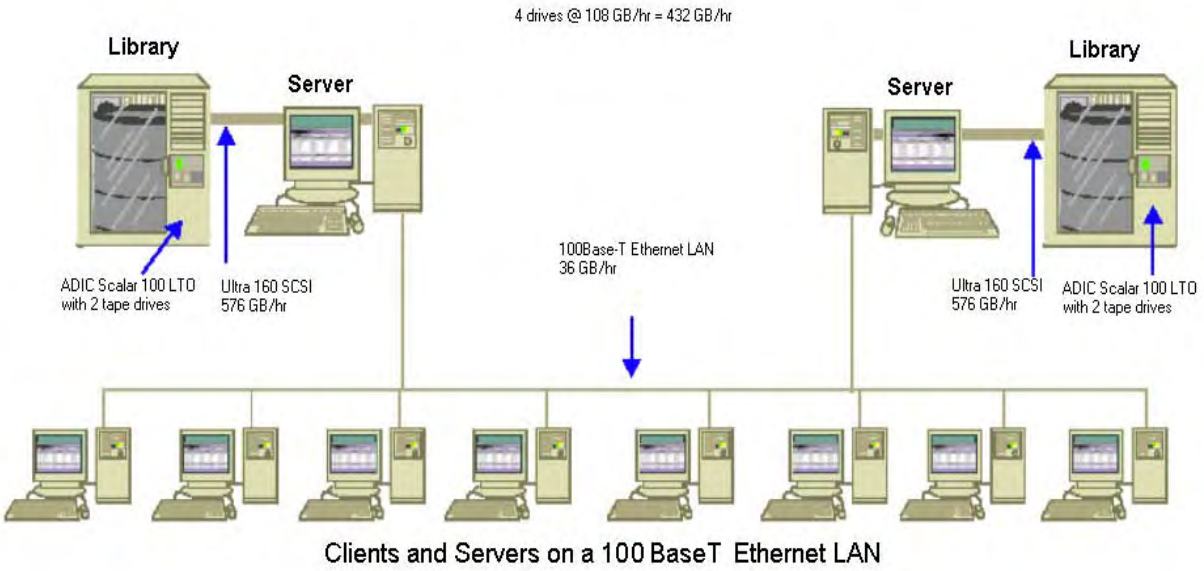
Sample Calculations

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

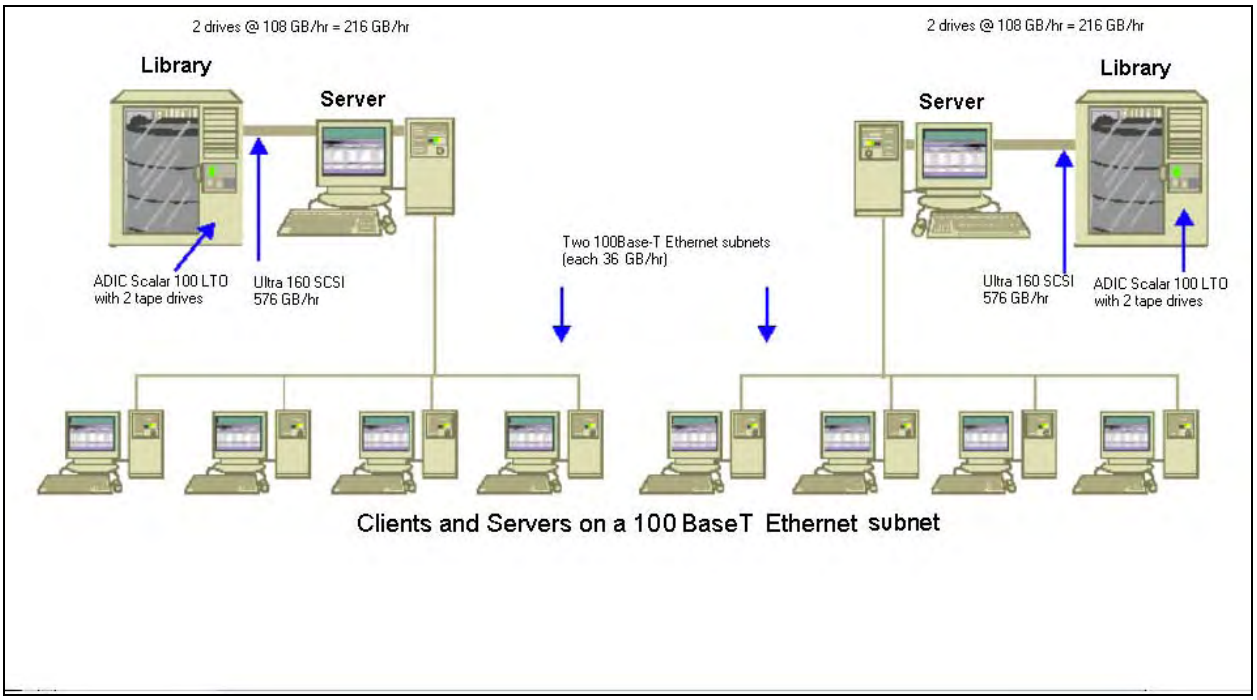
In this configuration, data cannot move across the network faster than 36 GB per hour, regardless of the number of servers and libraries available. To back up 1 Terabyte of data, the backup operation must run for 28 hrs.



Clients and Servers on a 100 BaseT Ethernet LAN

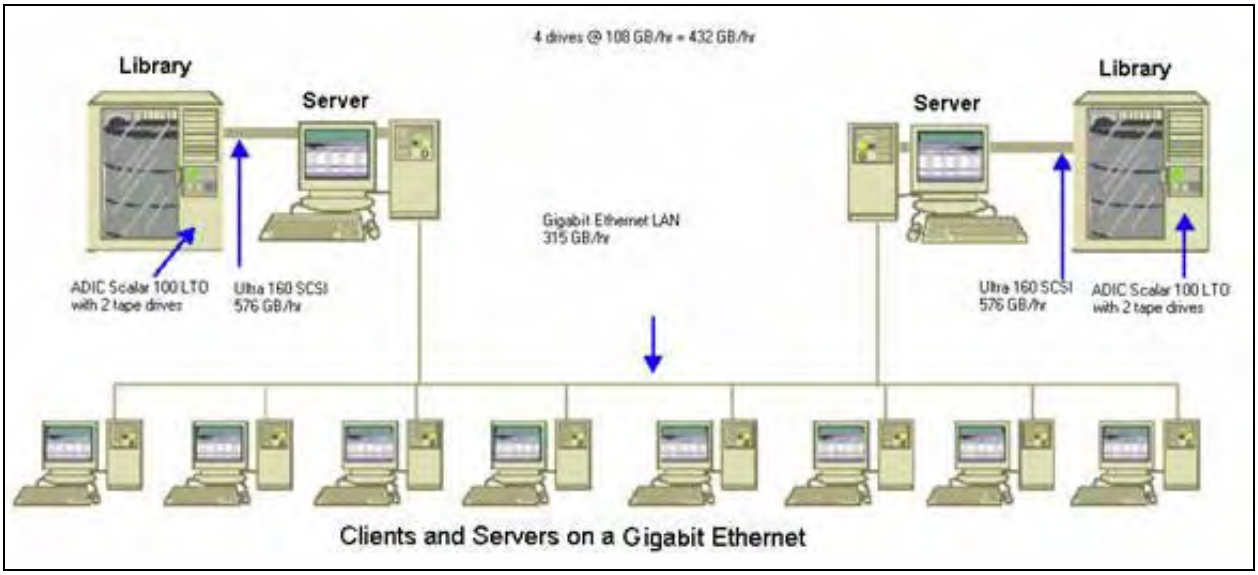
Transfer Rate for Clients and Servers on Two 100Base-T Ethernet Subnets

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.



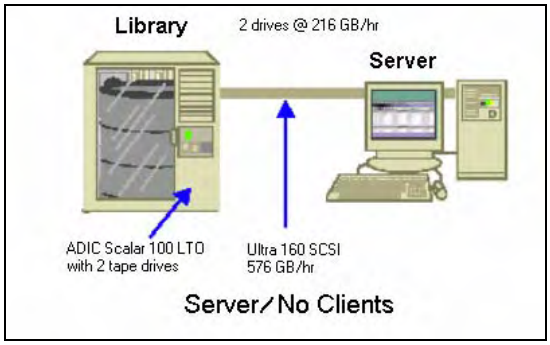
Transfer Rate for Clients and Servers on a Gigabit Ethernet Network

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.



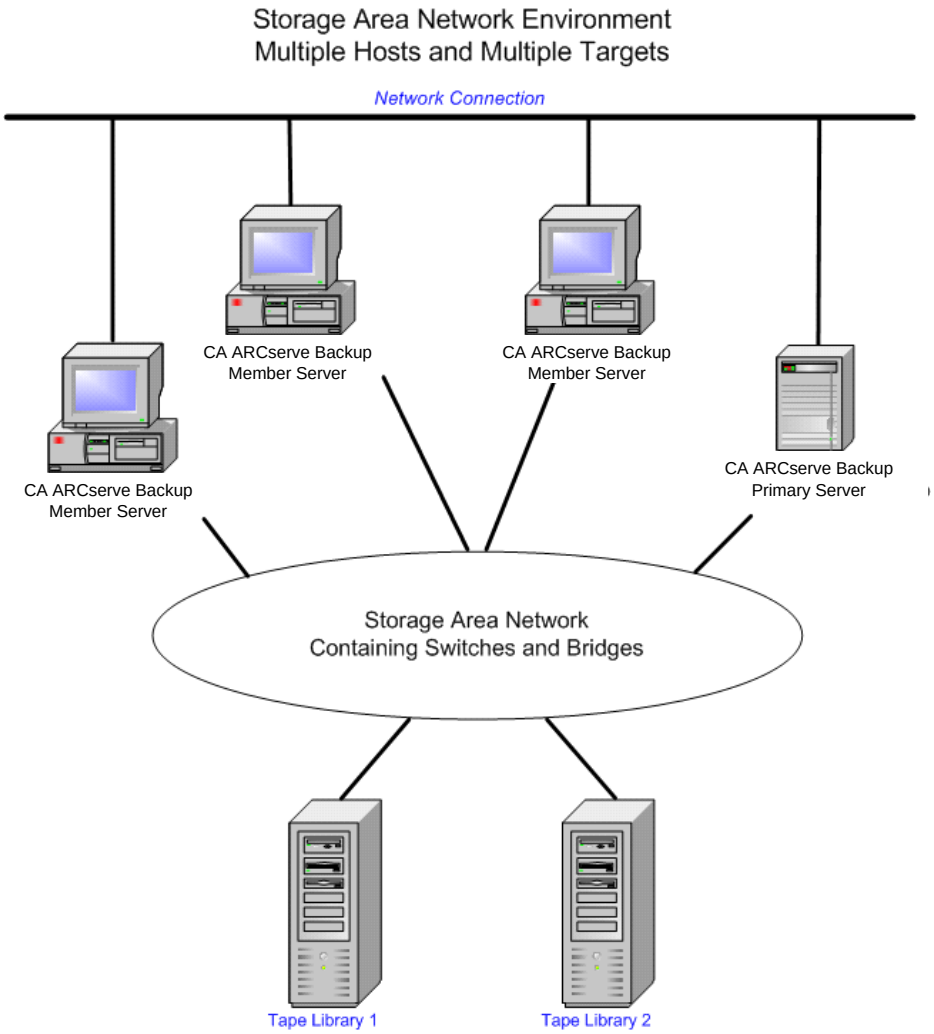
Transfer Rate for a Server With No Clients

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

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.

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 40).

  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 2005 Express Edition or Microsoft SQL Server.

  Microsoft SQL Server 2005 Express is a free database application that is packaged with CA ARCserve Backup. Microsoft SQL Server 2005 Express Edition must be installed on the CA ARCserve Backup server. For more information, see Microsoft SQL Server 2005 Express Edition Considerations (see page 44).

  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 45).

- **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.

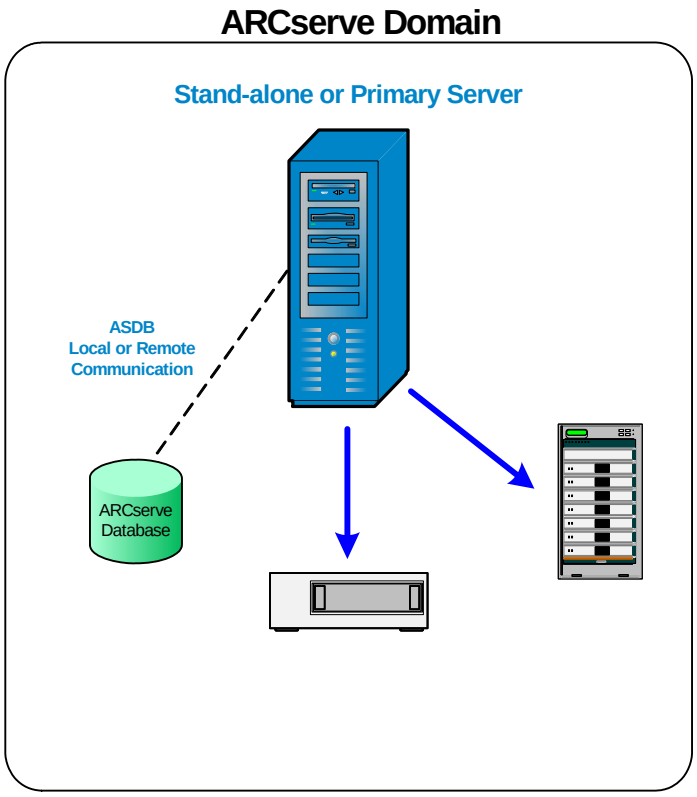
  For information about silent installation and Unicenter Software Delivery installation, see Create a Silent Installation Response File (see page 71) and Install CA ARCserve Backup Using Unicenter Software Delivery (see page 76).

Types of CA ARCserve Backup Server Installations

CA ARCserve Backup supports the following types of installations:

ARCserve Stand-alone Server

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 must install and manage the CA ARCserve Backup database on the primary server.

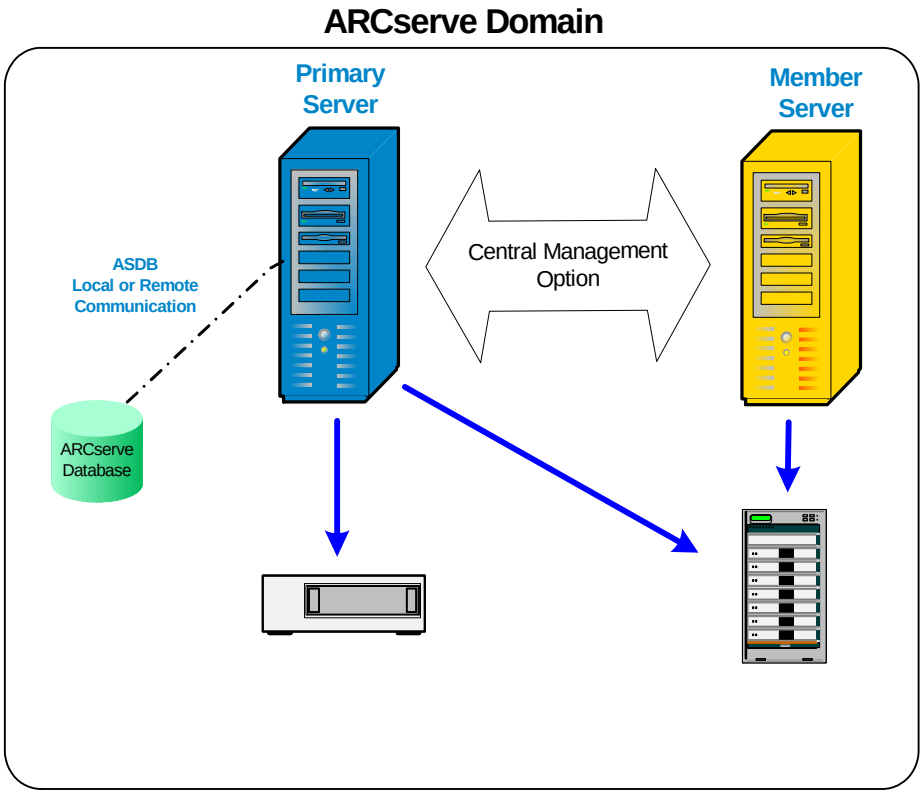
To enable centralized management capabilities, you must install and license the Central Management Option.

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.



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.

Custom Installation

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

CA ARCserve Backup Server Options

The following table describes the CA ARCserve Backup options available for each CA ARCserve Backup server type.

Option	Stand-alone Server	Primary Server	Member Server
Central Management Option		Available	
Tape Library Option	Available	Available	
Disk to Disk to Tape Option	Available	Available	
Storage Area Network (SAN) Option		Available	
Agent for VMware	Available	Available	
Enterprise Module	Available	Available	Available
Disaster Recovery Option	Available	Available	Available
NDMP NAS Option	Available	Available	
Unicenter Integration Option	Available	Available	Available

Database Requirements

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

- Microsoft SQL Server 2005 Express Edition (see page 44)
- Microsoft SQL Server (see page 45)

If you are upgrading to this release of CA ARCserve Backup, you can migrate data from a previous ARCserve database to Microsoft SQL Server 2005 Express Edition or Microsoft SQL Server.

Note: For a complete list of ARCserve products that you can upgrade from, see Supported Upgrades (see page 50).

Microsoft SQL Server 2005 Express Edition Considerations

Review the following information if you are considering using Microsoft SQL Server 2005 Express Edition to support the CA ARCserve Backup database:

- SQL Server 2005 Express Edition is a free, lightweight version of Microsoft SQL Server and is packaged with CA ARCserve Backup.
- Microsoft SQL Server 2005 Express Edition is the recommended database application for installations that consist of a stand-alone server or a primary server with less than ten member servers in the domain.
- Ensure that the ARCserve system account has administrative privileges on Microsoft SQL Server 2005 Express Edition databases.
- Microsoft SQL Server 2005 Express does not support remote operations. You must install the ARCserve database locally to your CA ARCserve Backup server.
- Microsoft SQL Server 2005 Express Edition is not supported on IA-64 (Intel Itanium) operating systems.
- To function properly, SQL Server 2005 Express Edition requires that .NET Framework 2.0 be installed on your system. Microsoft .NET Framework 2.0 is packaged with CA ARCserve Backup and is provided for you on the CA ARCserve Backup installation media.
- If you are currently using Microsoft SQL Server 2005 Express in your environment, you can use your current installation for the CA ARCserve Backup underlying database.
- If you determine that Microsoft SQL Server 2005 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 2005 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 2005 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.

Microsoft SQL Server Database Considerations

Review the following information if you are considering using Microsoft SQL Server to support the CA ARCserve Backup database:

- If you are upgrading to this release and currently running Microsoft SQL Server to support the ARCserve database instance, you must deploy Microsoft SQL Server in this release to support the ARCserve database instance.
- By default, CA ARCserve Backup creates the ARCserve 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 install the ARCserve database locally or remotely to your CA ARCserve Backup server.

  Note: For more information, see Remote Database Considerations.
- Microsoft SQL Server maintains the following disk space requirements:
  - Every file (record) you back up consumes about 105 to 115 bytes of the database space.
  - 150 MB of the SQL database contains approximately one million records.

  Based upon the needs of your organization, you should plan to have a sufficient amount of free disk space to support the growth of the database.
- 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 CA ARCserve Backup domain.
- If you are backing up operating systems that support case-sensitive naming conventions, you should create the SQL instance that will contain the ARCserve database with a case-sensitive server collation.
- 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 (which has the right to create devices) when prompted for the CA ARCserve Backup Database (SQL) System Account during installation of CA ARCserve Backup with Microsoft SQL support.
- If the Microsoft SQL Server account is changed, make the corresponding changes in the Server Admin in the CA ARCserve Backup program group.

- 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, 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`

- If you specify Microsoft SQL 2000 or Microsoft SQL 2005 as the CA ARCserve Backup database during setup, you can use Windows NT authentication or SQL authentication to communicate with the Microsoft SQL database.
- 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 ARCserve database instance on a remote system.

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 48).

Important! Microsoft SQL Server 2005 Express Edition does not support remote database communication.

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

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

If you are hosting the ARCserve database instance using Microsoft SQL Server 2000 or Microsoft SQL Server 2005, and the ARCserve 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 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

To enable TCP/IP communication on Microsoft SQL Server 2005 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.

Agent for ARCserve Database

The Agent for ARCserve Database is a form of the CA ARCserve Backup Agent for Microsoft SQL Server. It is either installed automatically when you install CA ARCserve Backup, or manually using a special utility after the location of the CA ARCserve Backup database is changed. By itself, the Agent for ARCserve Database allows you to back up and restore the ARCserve database itself, and the system databases and Disaster Recovery Elements from the Microsoft SQL Server instance which contains the ARCserve database. When installed with the Agent for Microsoft SQL Server, it allows the Agent for Microsoft SQL Server to recognize the presence of an ARCserve database, and to work with CA ARCserve Backup to provide the special recovery mechanisms that are available for the ARCserve database.

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 which installs the Agent for ARCserve Database in any of the following situations:

- When the ARCserve 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 it directly

This utility is placed in the "Packages" sub-folder of the CA ARCserve Backup home directory, in a folder called "ASDBSQLAgent", when you install CA ARCserve Backup. If you need to install the agent on a computer which is not a CA ARCserve Backup server, you will need to copy the "ASDBSQLAgent" folder to the system where you are installing the agent, and run the utility on that machine.

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\_BS*.tmp`

  For each installation session, CA ARCserve Backup creates a unique _BS*.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.

Upgrade Considerations

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

Supported Upgrades

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

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

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

- BrightStor ARCserve Backup Version 9.01--includes the GA release and all of the latest service packs.

  Note: CA ARCserve Backup does not support upgrading BrightStor ARCserve Backup Version 9.01 in a cluster-aware environment to this release. To upgrade to this release, you must uninstall BrightStor ARCserve Backup for Windows Version 9.01 and then install this release into a cluster-aware environment.

- BrightStor Enterprise Backup Version 10.5 Service Pack 1

  Note: CA ARCserve Backup does not support upgrading BrightStor Enterprise Backup Version 10.5 Service Pack 1 in a cluster-aware environment to this release. To upgrade to this release, you must uninstall BrightStor Enterprise Backup Version 10.5 Service Pack 1 and then install this release into a cluster-aware environment.

For all other releases, you must uninstall ARCserve before you install CA ARCserve Backup.

Backward Compatibility

This release of the CA ARCserve Backup server component can back up data using agents from the following releases:

- BrightStor ARCserve Backup r11.5, General Availability release and the latest service packs
- BrightStor ARCserve Backup r11.1, Service Pack 2
- BrightStor ARCserve Backup r9.0, Service Pack 1

You must retain the previous BrightStor ARCserve Backup Manager to view and manage ARCserve servers that are running the following releases:

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

Note: For more information, see Manager Console Support for Previous Releases (see page 52).

In addition, you can restore data from backup tapes and load job scripts created using all previous versions BrightStor ARCserve Backup and BrightStor Enterprise Backup.

Note: When backing up using agents, the version of CA ARCserve Backup that you use must be equal to or greater than the version of the agent you want to back up. You cannot use agents from this release of CA ARCserve Backup with any previous version of the base product.

Manager Console Support for Previous Releases

This release of CA ARCserve Backup provides you with a redesigned Manager Console. To manage other servers in your ARCserve environment that are running older releases of this product, you must retain the previous Manager Console. You must specify that you want to retain the previous Manager Console when you are upgrading CA ARCserve Backup from a previous release.

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

Upgrade your CA ARCserve Backup installation to the redesigned user interface

Requires you to upgrade all ARCserve systems 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
```

Upgrade your CA ARCserve Backup installation to the redesigned user interface and retain the Manager console from your previous release

Lets you upgrade some ARCserve systems in your environment and retain systems running the previous release.

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.

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
```

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 ARCserve database to the new ARCserve database.

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

Authentication

The upgrade process migrates all ARCserve System Account data from the previous database, such as user names, passwords, and so on.

Note: For upgrades to ARCserve 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.

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 to the new database.

Note: The process of migrating session data can take a lot of time. However, after the migration is complete, 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 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:

- On the back of 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 following table 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
BrightStor ARCserve Backup Client Agent for UNIX	r11.5 SP3
BrightStor ARCserve Backup Client Agent for Linux	r11.5 SP3
BrightStor ARCserve Backup Client Agent for Mainframe on Linux OS/390	r11.5 SP3
CA ARCserve Backup Client Agent for Windows	r12
BrightStor ARCserve Backup Client Agent for NetWare	r11.1 SP3
BrightStor ARCserve Backup Client Agent for Mac OS X (Supported on Windows Only)	r11.5 SP3
BrightStor ARCserve Backup Client Agent for OpenVMS (Supported on Windows Only)	r11.5 SP3
CA ARCserve Backup Agent for Oracle (Windows)	r12
BrightStor ARCserve Backup Agent for Oracle (UNIX)	r11.5 SP3
BrightStor ARCserve Backup Agent for Oracle (Linux)	r11.5 SP3
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

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 ARCserve servers you are installing.

  Note: For more information, see Types of CA ARCserve Backup Server Installations (see page 40).

ARCserve Database

Determine the database application that you will use for your CA ARCserve Backup installation. For more information, see Database Requirements (see page 43).

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 50).

Cluster Installations

When you install CA ARCserve Backup, the installation wizard can detect 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.

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 automatically 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 Stk 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 an unlimited number of 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 eTrust InoculateIT or eTrust 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 agents installation media available to you while you run the installation wizard.

Install CA ARCserve Backup

This section describes how to 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 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.

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 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.

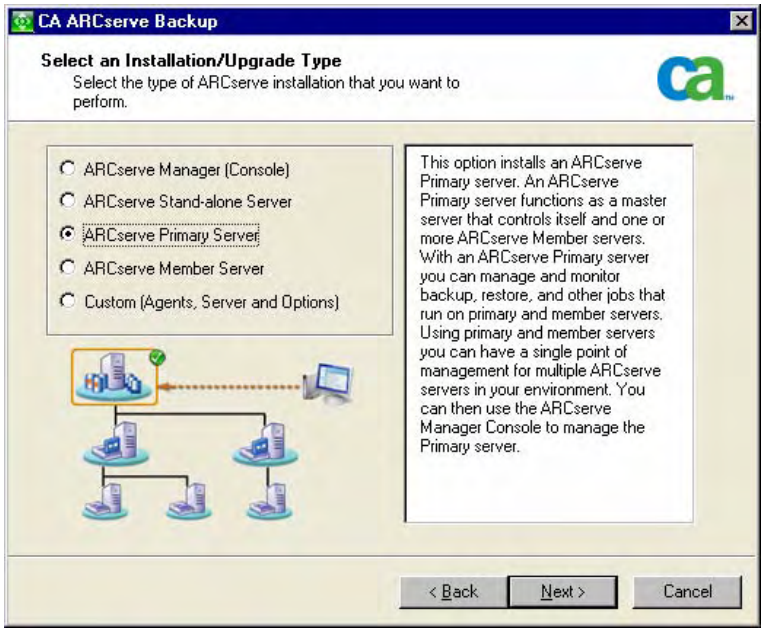
   With remote installations, the target remote systems can consist of different ARCserve server types, different CA ARCserve Backup agents and options, or both.

   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 SQL agent or Exchange agent) only applies if you use a virtual host. Remote installation of CA ARCserve Backup agents using the physical hosts of clusters is supported.

   Select an Installation/Upgrade Type dialog

   Lets you specify the type of ARCserve components that you want to install.

   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.



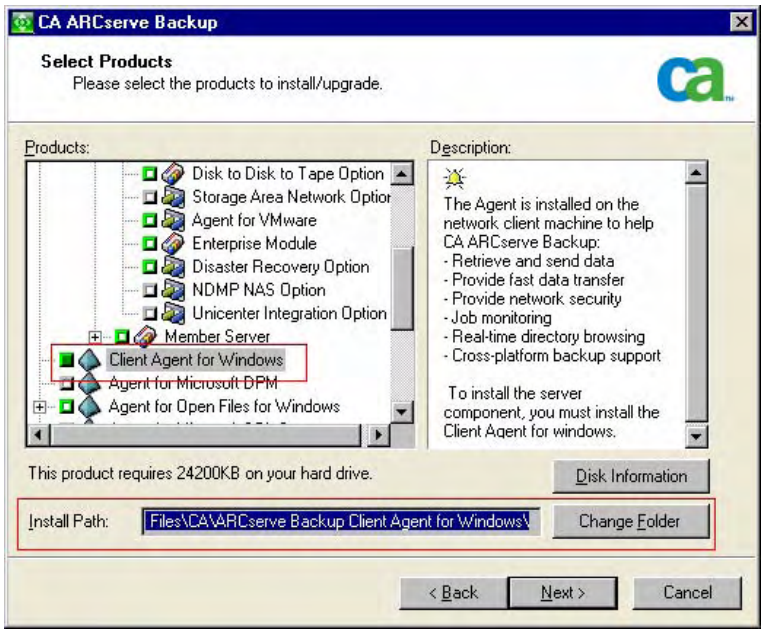
Select Products dialog

If you are installing a primary server, you must install the 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 install CA ARCserve Backup on at least one primary server before you install member servers.

If you are performing a remote installation, a silent installation, or installing CA ARCserve Backup using Unicenter Software Delivery, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA ARCserve Backup base product.

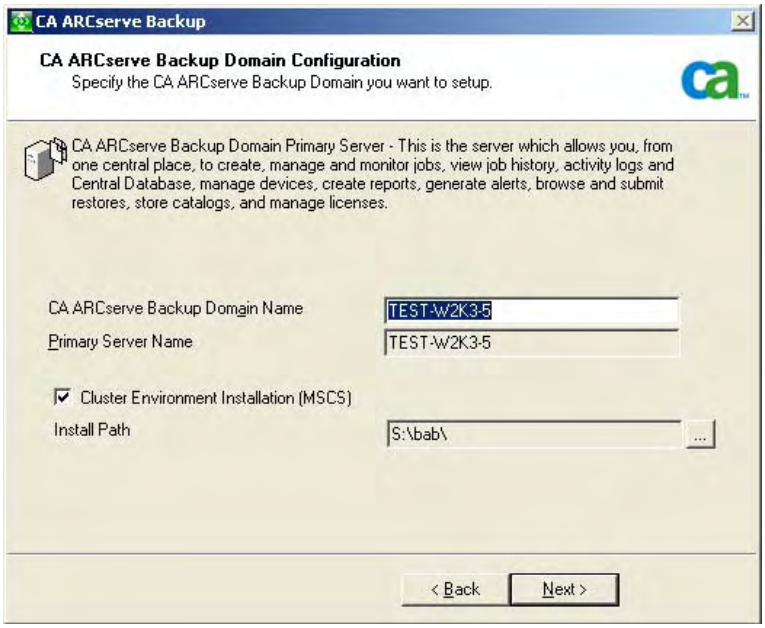
The following diagram illustrates the default installation path for the Client Agent for Windows:



Note: 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 ARCserve server that you want to install, and check the check boxes corresponding to the components that you want to install.

CA ARCserve Backup Domain Configuration 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 to the shared disk where you want to install CA ARCserve Backup.



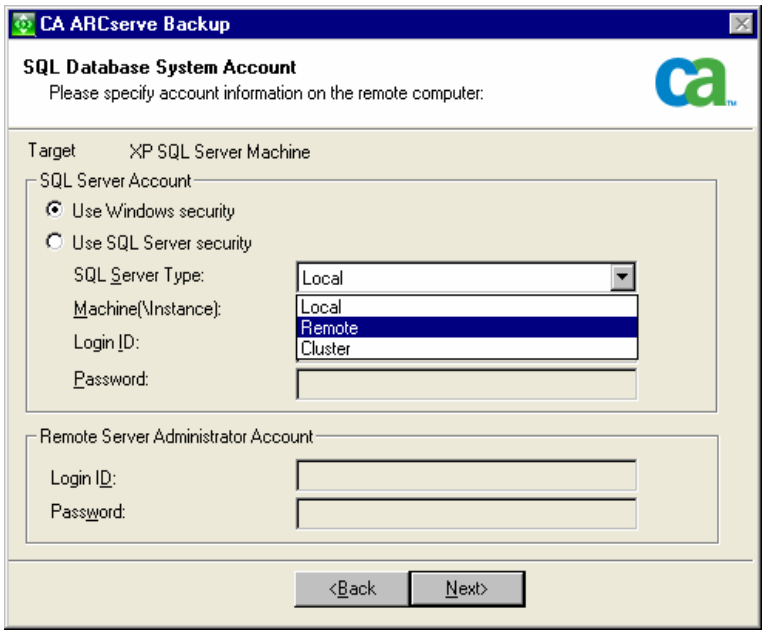
Note: CA ARCserve Backup server names and CA ARCserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

Select Database dialog

If you specify Microsoft SQL Server and you are backing up operating systems that support case-sensitive naming conventions, you should create the SQL instance that will contain the ARCserve database with a case-sensitive server collation.

For Cluster Installations:

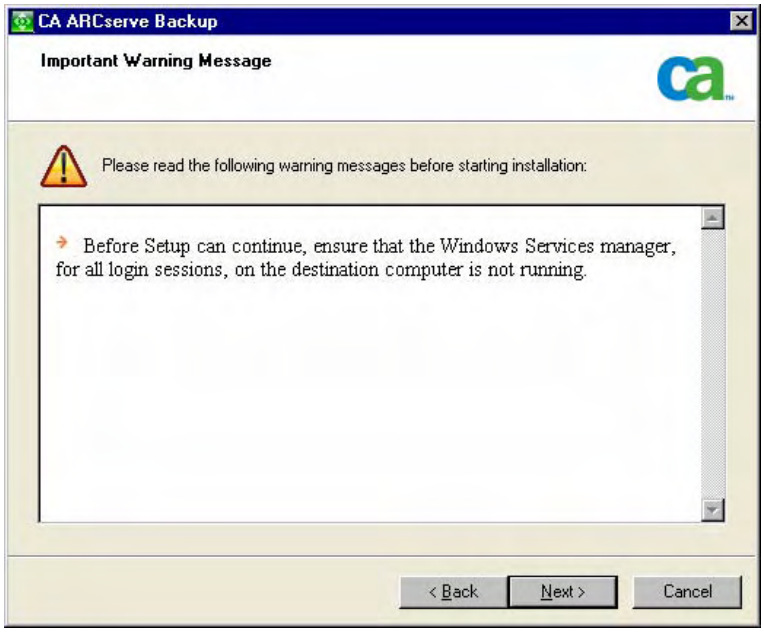
- CA ARCserve Backup does not support local Microsoft SQL Server installations on CA ARCserve Backup servers in NEC ClusterPro environments. In NEC ClusterPro environments, you must install the ARCserve database instance on a remote system.
- You must specify the Remote SQL Server Type option if the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



Important Warning Messages dialog

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

The following graphic illustrates the Important Warning Messages dialog:



Product List dialog

To modify your installation options, click the Back button 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.

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.

Note: You may be required to restart the server when installing CA ARCserve Backup. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.

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 BrightStor ARCserve Backup or BrightStor Enterprise Backup, you can upgrade to this release from the following products:

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

  Note: CA ARCserve Backup does not support upgrading BrightStor ARCserve Backup for Windows r11.1 in a cluster aware environment to this release. To upgrade to this release, you must uninstall BrightStor ARCserve Backup for Windows r11.1 and then install this release into a cluster-aware environment.
- BrightStor ARCserve Backup Version 9.01--includes the GA release and all of the latest service packs.

  Note: CA ARCserve Backup does not support upgrading BrightStor ARCserve Backup Version 9.01 in a cluster-aware environment to this release. To upgrade to this release, you must uninstall BrightStor ARCserve Backup for Windows Version 9.01 and then install this release into a cluster-aware environment.
- BrightStor Enterprise Backup Version 10.5 Service Pack 1

  Note: CA ARCserve Backup does not support upgrading BrightStor Enterprise Backup Version 10.5 Service Pack 1 in a cluster-aware environment to this release. To upgrade to this release, you must uninstall BrightStor Enterprise Backup Version 10.5 Service Pack 1 and then install this release into a cluster-aware environment.

For all other releases, you must uninstall ARCserve before you install CA ARCserve Backup.

For more information about upgrading to this release, see Upgrade Considerations (see page 50).

To upgrade CA ARCserve Backup from a previous release

1. Insert the CA ARCserve Backup installation media into your 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.

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 upgrading CA ARCserve Backup from a previous release.

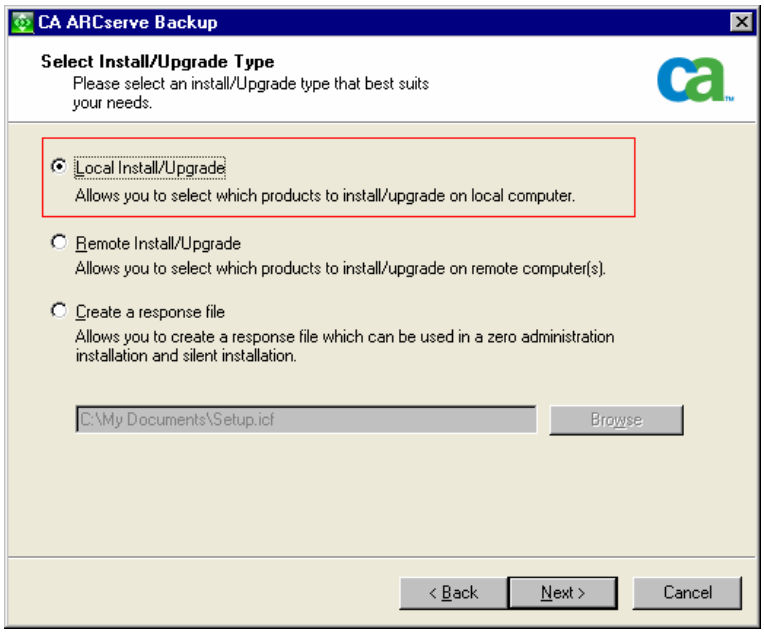
   Select Install/Upgrade Type dialog

   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 52).

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



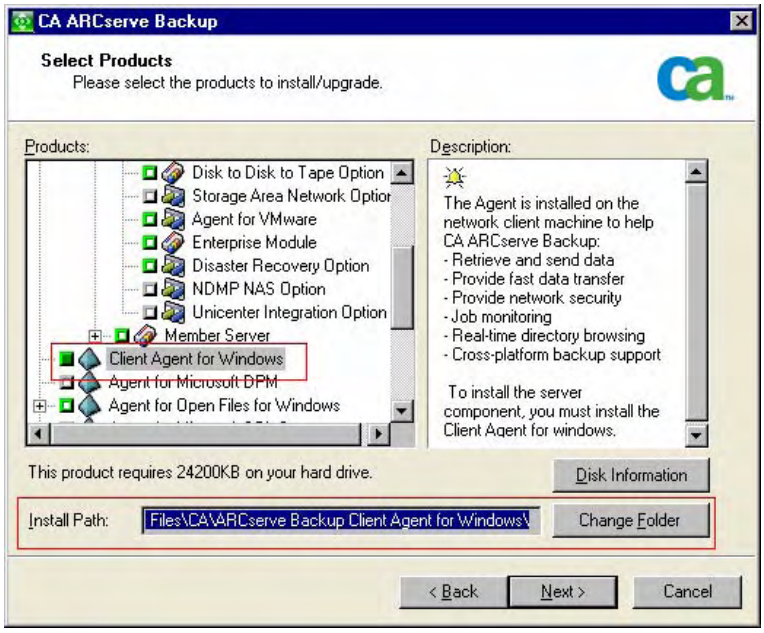
Select Products dialog

If you are upgrading your current installation to an ARCserve Primary Server, you must install the Central Management Option on the primary server.

To upgrade your current installation to an ARCserve Member Server, the installation wizard must be able to detect the CA ARCserve Backup domain name and primary server name in your network. You should therefore upgrade at least one CA ARCserve Backup Primary Server before you upgrade to ARCserve Member Servers.

If you are performing a remote installation, a silent installation, or installing CA ARCserve Backup using Unicenter Software Delivery, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA ARCserve Backup base product.

The following diagram illustrates the default installation path for the Client Agent for Windows:



Note: 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 ARCserve server that you want to install, and check the check boxes corresponding to the components that you want to install.

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.

CA ARCserve Backup Domain Configuration 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.

Select Database dialog

If you specify Microsoft SQL Server and you are backing up operating systems that support case-sensitive naming conventions, you should create the SQL instance that will contain the ARCserve database with a case-sensitive server collation.

Important Warning Messages dialog

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

Product List dialog

To modify your installation options, click the Back button 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.

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.

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 53).

Note: 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.

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 optical drive and 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.

   Select Install/Upgrade Type dialog

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

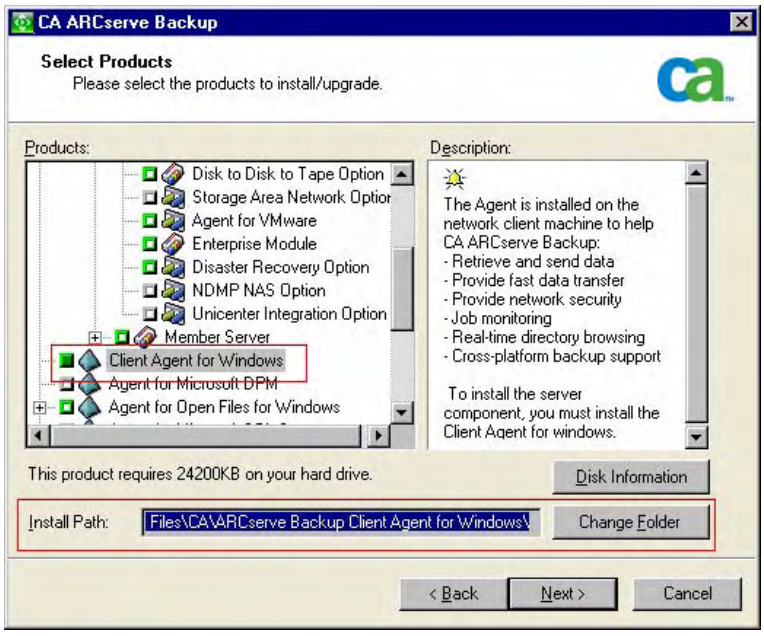
   Select Products dialog

   If you are installing a primary server, you must install the 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. You should therefore install CA ARCserve Backup on at least one primary server before you install member servers.

   If you are performing a remote installation, a silent installation, or installing CA ARCserve Backup using Unicenter Software Delivery, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA ARCserve Backup base product.

   The following diagram illustrates the default installation path for the Client Agent for Windows:



Note: 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 ARCserve server that you want to install, and check the check boxes corresponding to the components that you want to install.

CA ARCserve Backup Domain Configuration 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.

Select Database dialog

If you specify Microsoft SQL Server and you are backing up operating systems that support case-sensitive naming conventions, you should create the SQL instance that will contain the ARCserve database with a case-sensitive server collation.

Product List dialog

To modify your installation options, click the Back button 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.

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

   ```
   mastersetup /?
   ```

   Example:

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

   In this example, the response file is located in 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 your system after the installation completes. To determine if you have to restart your machine, check the ProdWiz.log for a restart message.

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 66).
2. After the upgrade process is complete, 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
```

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. The following sections include information about each of these alternate installation methods.

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.

Base Components

Component	Prerequisites
CA ARCserve Backup server	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License
CA License	■ Microsoft Installer and vcredist
Diagnostic Utility	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist
Microsoft Installer	■ None
Unicenter Integration Option	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA ARCserve Backup Server

CA ARCserve Backup Client Agents for Windows

Component	Prerequisites
Windows Client Agent	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist
Windows 64-bit Client Agent	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and vcredist

CA ARCserve Backup Agents

Component	Prerequisites
CA ARCserve Backup Agent for Open Files	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License

Component	Prerequisites
CA ARCserve Backup Agent for Open Files 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup Agent for Microsoft Exchange	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup Agent for Microsoft Exchange 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup Agent for IBM Informix	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup Agent for Lotus Domino	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup Agent for Oracle	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup for Microsoft SQL Server	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup for Microsoft SQL Server 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and vcredist ■ CA License
CA ARCserve Backup Agent for Sybase	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License

Component	Prerequisites
CA ARCserve Backup Agent for Microsoft SharePoint	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License ■ CA ARCserve Backup Server
CA ARCserve Backup Agent for Microsoft SharePoint 64-bit	■ CA ETPKI for Windows ■ CA ETPKI for Windows 64-bit ■ Microsoft Installer and vcredist ■ CA License ■ CA ARCserve Backup Server

CA ARCserve Backup Options

Component	Prerequisites
CA ARCserve Backup Disaster Recovery Option	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA ARCserve Backup Server
CA ARCserve Backup NDMP NAS Option	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License ■ CA ARCserve Backup Server
CA ARCserve Backup Enterprise Module	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License ■ CA ARCserve Backup Server
CA ARCserve Backup Enterprise Option for SAP R/3 for Oracle	■ CA ETPKI for Windows ■ Microsoft Installer and vcredist ■ CA License

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 machine has the correct configuration to install and run the component. This information is available in the documentation for the individual 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 71).

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 CA ARCserve Backup ensure that you complete the following tasks:

- To ensure that all jobs start on schedule, synchronize the system time between the primary server and all of its member servers.

  Note: Use Windows Time Service to synchronize the time on all ARCserve 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 157), or the *Administration Guide*.

Uninstall CA ARCserve Backup

The following procedure describes how to uninstall CA ARCserve Backup from your system.

To ensure that CA ARCserve Backup is completely uninstalled from your system, you should uninstall all CA ARCserve Backup components that appear in the Add or Remove Programs 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.

The uninstallation routine removes all CA ARCserve Backup components, directories, files, and so on from your system, except for following directories and all of their contents:

- C:\Program Files\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\1.4.2_16

  If you upgraded from a previous ARCserve release, and the previous ARCserve release was integrated with a previous version of Java Runtime Environment (JRE), the uninstallation routine does not remove the directory and files associated JRE 1.4.2_16 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 the 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 the Remove button.

   The CA ARCserve Backup base product is uninstalled from your system.

Important! The uninstallation routine does not uninstall the ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

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

This section contains the following topics:

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 and NEC ClusterPro/ExpressCluster X 1.0 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:

- **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 SQL agent or Exchange agent) 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.

Deploy CA ARCserve Backup Server on MSCS

The following sections provide information on deploying CA ARCserve Backup servers on a MSCS cluster.

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:

- Operating system is a 32/64 bit Windows 2000, Windows Server 2003
- HA platform is configured for a MSCS cluster

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 SQL agent or Exchange agent) 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.

- Install CA ARCserve Backup into a MSCS cluster (quorum) group. (Does not apply to NEC clusters)

  "Cluster Group" is a special group used for MSCS management, which includes a cluster management virtual IP/name and quorum disk created during MSCS configuration. Although you can install CA ARCserve Backup into "Cluster Group" without creating a new virtual IP/name and share disk resource, it is recommended that you do not do so to avoid an unnecessary tight-couple with MSCS.

Which CA ARCserve Backup database type to use?

CA ARCserve Backup primary server supports using a local Microsoft SQL Server 2005 Express Edition installation and 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 2005 Express Edition (SQLE)

  If you do not purchase a SQL Server cluster and can accept the limitations imposed by SQL Server 2005 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 (MSCS only)

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

  Note: Local SQL Server is not supported when NEC ClusterPro/ExpressCluster is used to make CA ARCserve Backup highly available.

- 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.

MSCS Cluster Resource Preparation

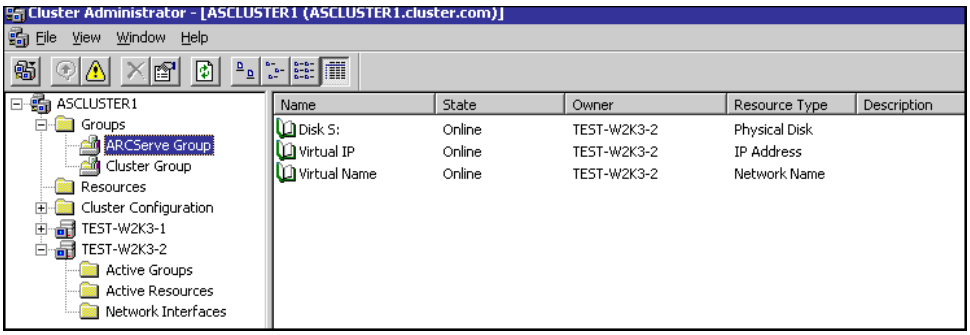
If you are installing CA ARCserve Backup into a dedicated group, you need to create the required resources into the new dedicated group, including a virtual IP address, virtual name, and a shared disk.

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 a MSCS Cluster-aware Environment

This section describes how to install CA ARCserve Backup in a MSCS Cluster-aware environment using the installation wizard.

To install CA ARCserve Backup

1. Insert the CA ARCserve Backup installation media into your 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.

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 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.

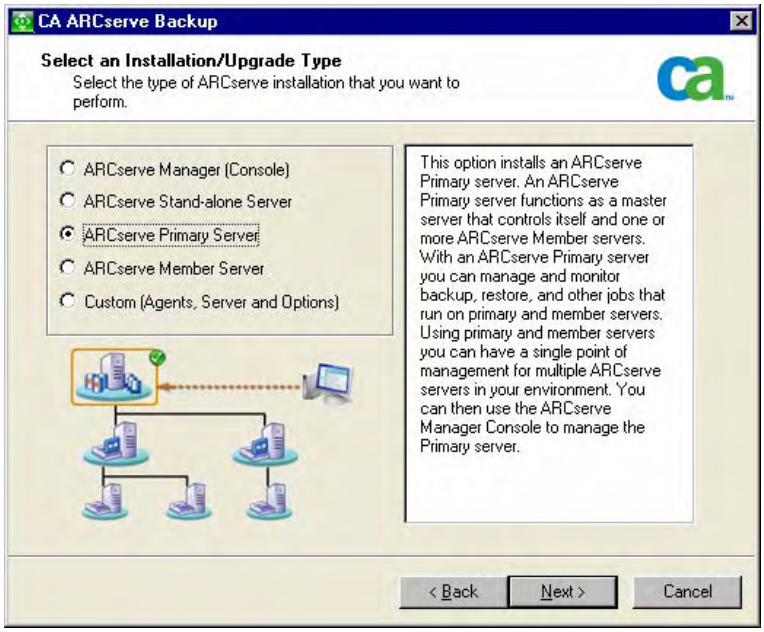
   With remote installations, the target remote systems can consist of different ARCserve server types, different CA ARCserve Backup agents and options, or both.

   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 SQL agent or Exchange agent) only applies if you use a virtual host. Remote installation of CA ARCserve Backup agents using the physical hosts of clusters is supported.

   Select an Installation/Upgrade Type dialog

   Lets you specify the type of ARCserve components that you want to install.

   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.



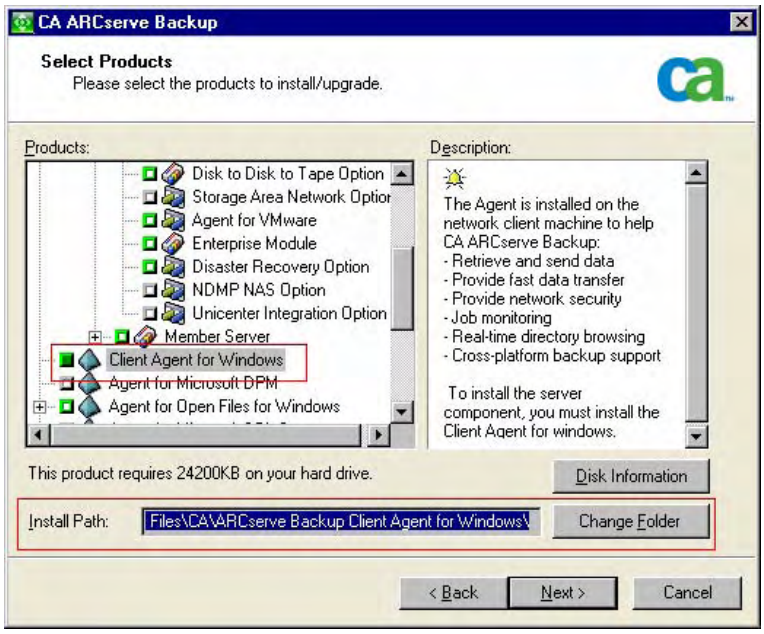
Select Products dialog

If you are installing a primary server, you must install the 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 install CA ARCserve Backup on at least one primary server before you install member servers.

If you are performing a remote installation, a silent installation, or installing CA ARCserve Backup using Unicenter Software Delivery, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA ARCserve Backup base product.

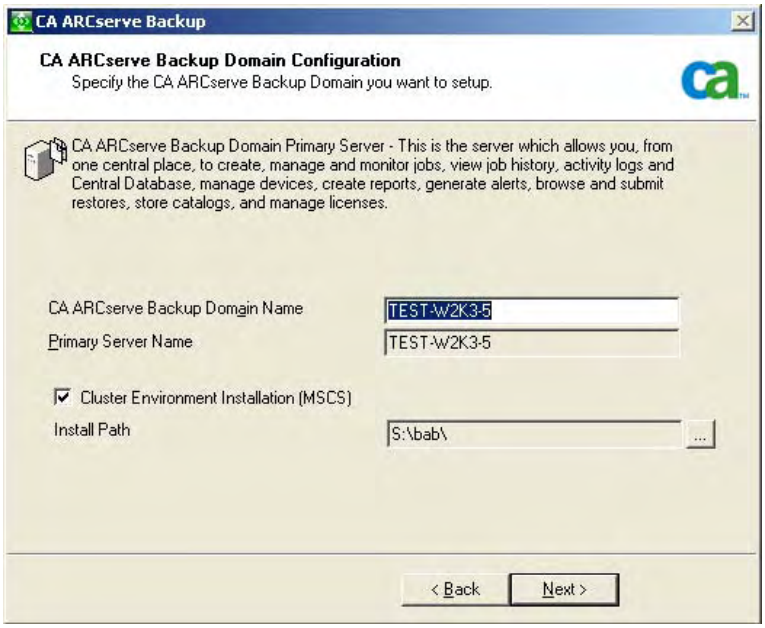
The following diagram illustrates the default installation path for the Client Agent for Windows:



Note: 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 ARCserve server that you want to install, and check the check boxes corresponding to the components that you want to install.

CA ARCserve Backup Domain Configuration 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 to the shared disk where you want to install CA ARCserve Backup.



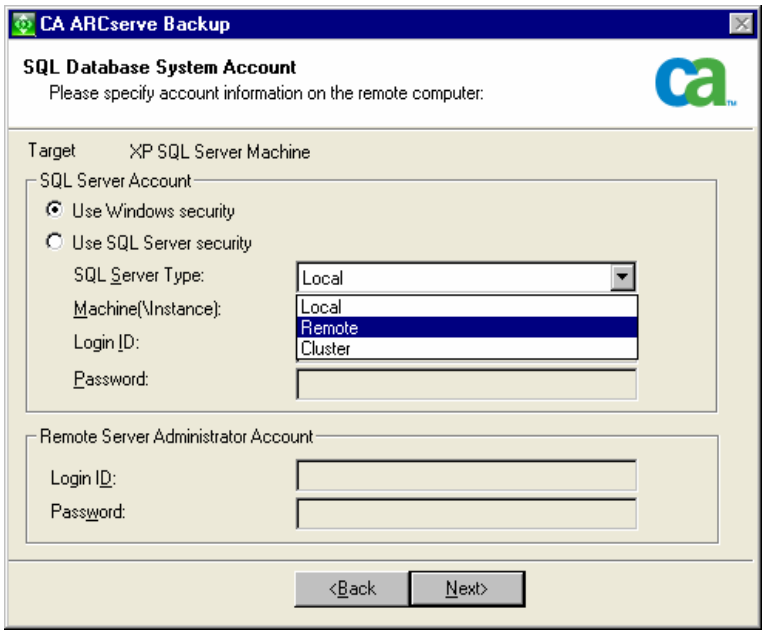
Note: CA ARCserve Backup server names and CA ARCserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

Select Database dialog

If you specify Microsoft SQL Server and you are backing up operating systems that support case-sensitive naming conventions, you should create the SQL instance that will contain the ARCserve database with a case-sensitive server collation.

For Cluster Installations:

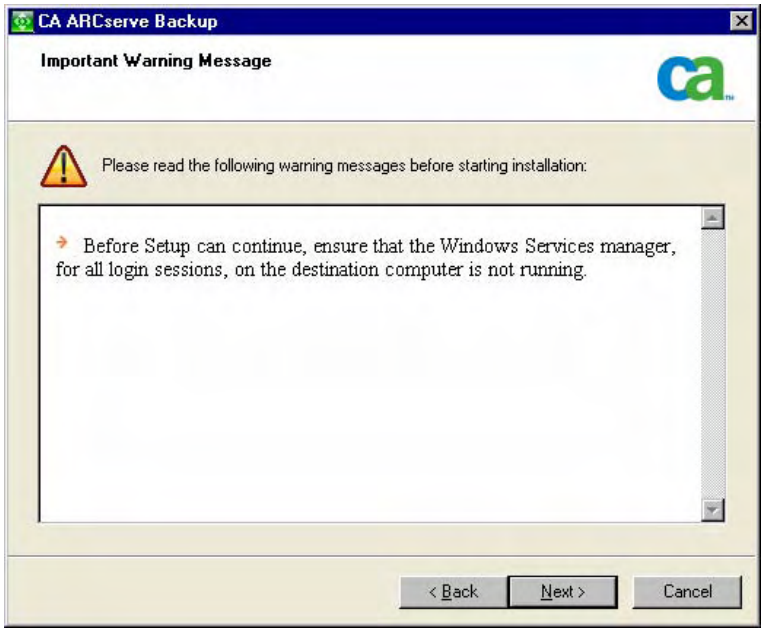
- CA ARCserve Backup does not support local Microsoft SQL Server installations on CA ARCserve Backup servers in NEC ClusterPro environments. In NEC ClusterPro environments, you must install the ARCserve database instance on a remote system.
- You must specify the Remote SQL Server Type option if the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



Important Warning Messages dialog

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

The following graphic illustrates the Important Warning Messages dialog:



Product List dialog

To modify your installation options, click the Back button 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.

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.

Note: You may be required to restart the server when installing CA ARCserve Backup. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.

Installation of CA ARCserve Backup in Each MSCS Cluster Node

In a CA ARCserve Backup HA cluster environment, CA ARCserve Backup is installed in each cluster node, but only one instance will be running. In this cluster, the active node will automatically take control of the backup resources and is referred to as the backup server. Other instances of CA ARCserve Backup that are hosted in passive nodes are referred as standby (or failover) servers and the cluster system will only activate one of them in case of failover.

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.

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.

When a cluster-aware installation is successfully finished, a Post Setup pop-up screen appears with an option to create HA resources. You should only check this option when you have completed the CA ARCserve Backup installation on the last node in the cluster.

Upgrade CA ARCserve Backup from r11.5 to r12 in a MSCS Cluster Environment

When upgrading CA ARCserve Backup from r11.5 to r12 in a MSCS cluster 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 a MSCS cluster environment:

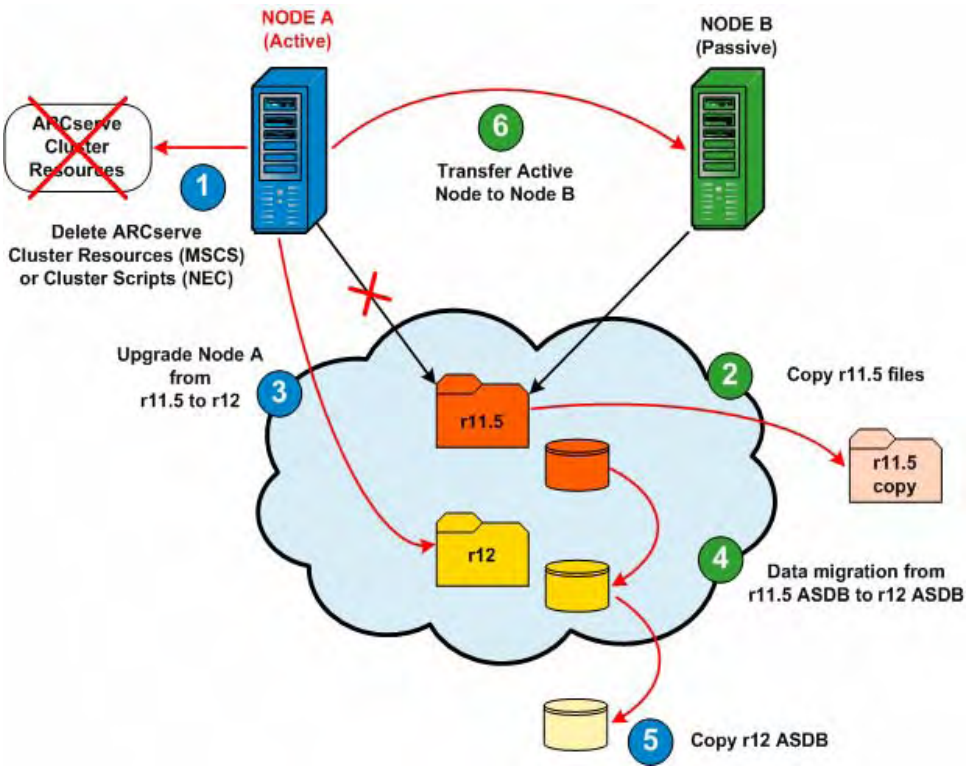
- Primary server upgrade RAIMA to SQL Express
- Primary server upgrade RAIMA to SQL Server
- Primary server upgrade SQL Server to SQL Server
- Member server upgrade RAIMA to r12
- Member server upgrade SQL Server to r12

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 r12 in a 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 r12 upgrade installation for Node A. See Upgrade CA ARCserve Backup from a Previous Release (see page 66).

   Important! During the upgrade installation, you will be prompted to specify the installation path location for r12. 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 r12 installation.

   - CA ARCserve Backup for Node A is upgraded from r11.5 to r12. 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. Using the Windows Service manager, right-click the CA ARCserve Backup database engine and from the pop-up window, select Start.

   When the CA ARCserve Backup database engine is started, the corresponding status will indicate Started.

5. From the Server Data Migration dialog (displayed at the completion of the upgrade process), launch the data migration.

   The specified CA ARCserve Backup data is migrated from r11.5 to r12.

6. 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.

7. 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.

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

   a. Access the Cluster Administrator.

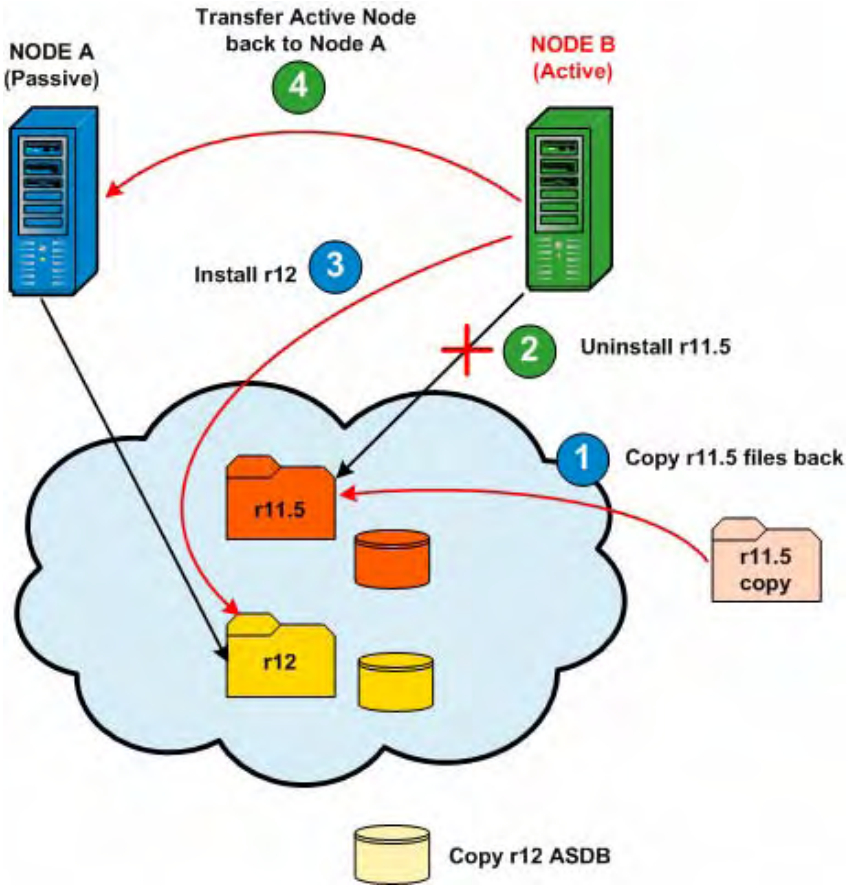
      The Cluster Administrator dialog opens.

   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 r12 new installation on Node B, do not select the "Overwrite DB" option to prevent overwriting the ARCserve database that was migrated during the r12 upgrade to Node A.

3. Perform CA ARCserve Backup r12 new installation for Node B with the same settings selected for Node A (domain name, server type, install path, installed options …). For example, if r12 was installed on Node A as a primary server, then r12 must be installed on Node B also as a primary server. See Install CA ARCserve Backup.

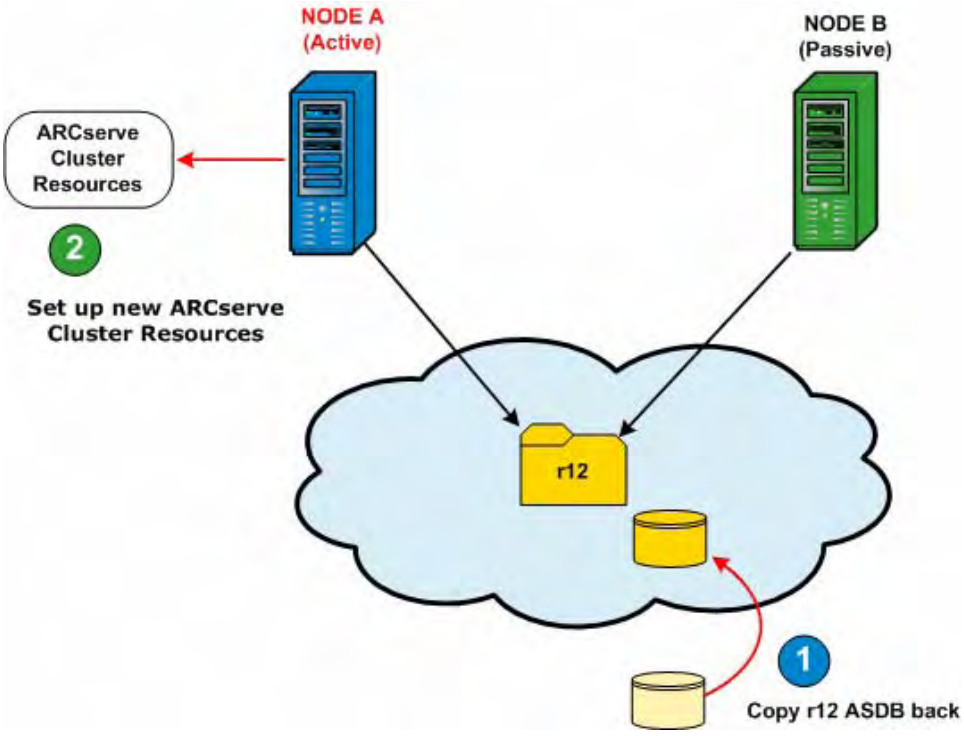
   CA ARCserve Backup r12 is installed on Node B. Do not set up new ARCserve cluster resources at this time.

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 r12 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.

Uninstall CA ARCserve Backup from a 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.

   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 share 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.

Deploy CA ARCserve Backup Server on NEC Cluster

The following sections provide information on deploying CA ARCserve Backup on a NEC cluster. CA ARCserve Backup cluster support is provided for NEC ClusterPro/ExpressCluster for Windows 8.0 and NEC ClusterPro/ExpressCluster X 1.0 for Windows.

Note: For more information about the differences of using each version of NEC ClusterPro/ExpressCluster, see the corresponding documentation provided by NEC.

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:

- Operating system is a 32/64 bit Windows2000, Windows2003 Server

  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 or NEC ClusterPro/ExpressCluster X 1.0 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.

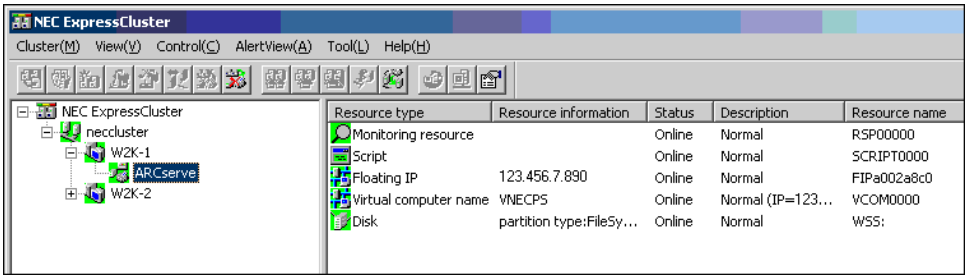
Cluster Manager and Task Manager are utilities provided by NEC and are installed on servers that have NEC ClusterPro/ExpressCluster installed.

- 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

This section describes how to install CA ARCserve Backup in an NEC Cluster-aware environment using the installation wizard.

To install CA ARCserve Backup

1. Insert the CA ARCserve Backup installation media into your 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.

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 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.

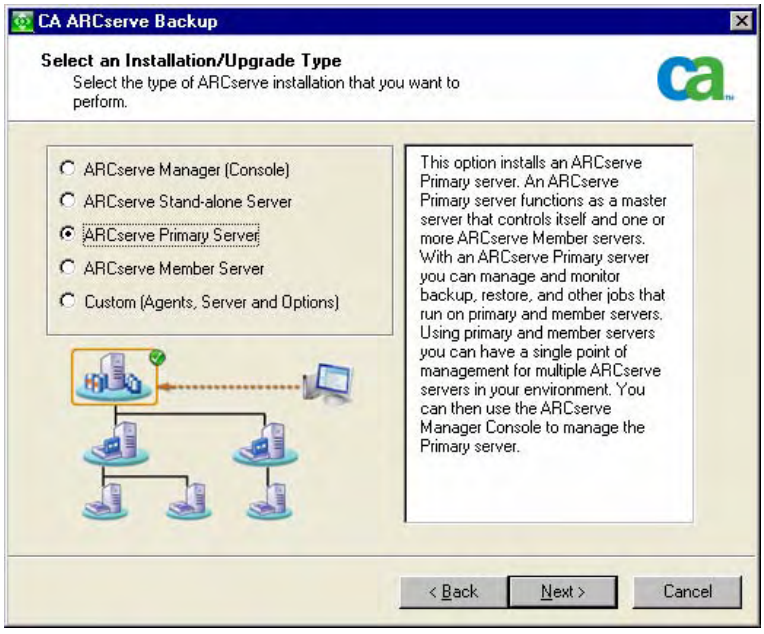
   With remote installations, the target remote systems can consist of different ARCserve server types, different CA ARCserve Backup agents and options, or both.

   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 SQL agent or Exchange agent) only applies if you use a virtual host. Remote installation of CA ARCserve Backup agents using the physical hosts of clusters is supported.

   Select an Installation/Upgrade Type dialog

   Lets you specify the type of ARCserve components that you want to install.

   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.



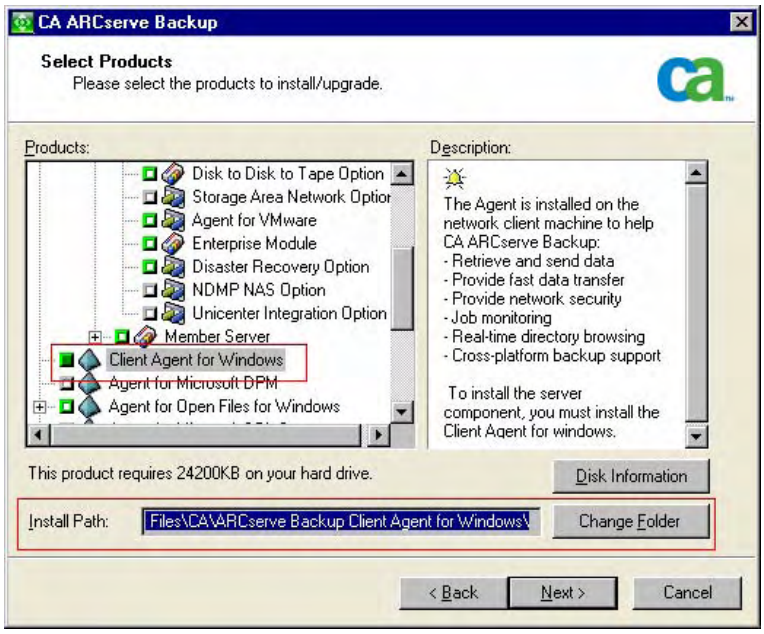
Select Products dialog

If you are installing a primary server, you must install the 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 install CA ARCserve Backup on at least one primary server before you install member servers.

If you are performing a remote installation, a silent installation, or installing CA ARCserve Backup using Unicenter Software Delivery, do not install the CA ARCserve Backup Client Agent for Windows into the same directory as the CA ARCserve Backup base product.

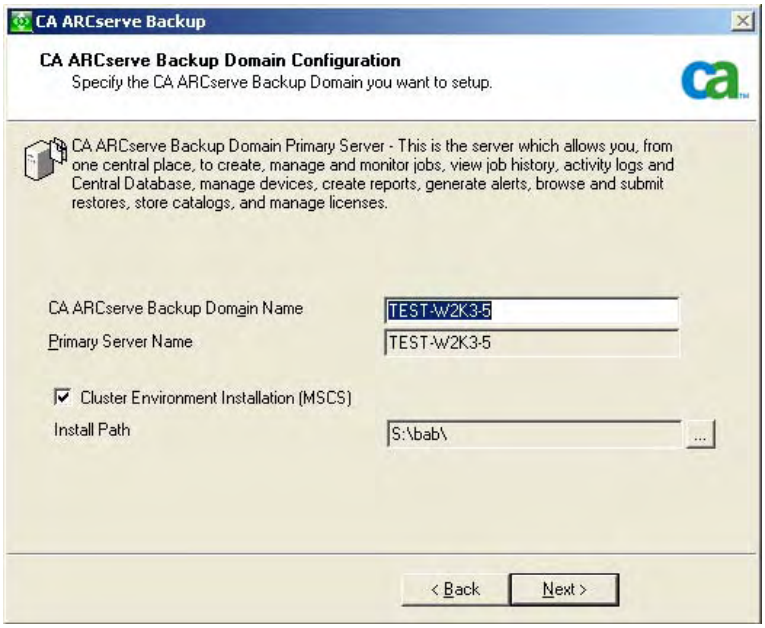
The following diagram illustrates the default installation path for the Client Agent for Windows:



Note: 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 ARCserve server that you want to install, and check the check boxes corresponding to the components that you want to install.

CA ARCserve Backup Domain Configuration 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 to the shared disk where you want to install CA ARCserve Backup.



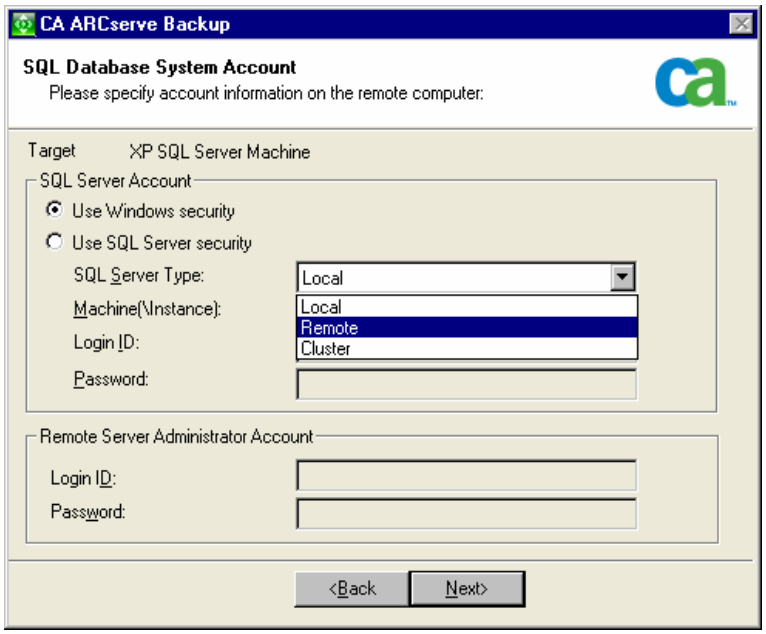
Note: CA ARCserve Backup server names and CA ARCserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

Select Database dialog

If you specify Microsoft SQL Server and you are backing up operating systems that support case-sensitive naming conventions, you should create the SQL instance that will contain the ARCserve database with a case-sensitive server collation.

For Cluster Installations:

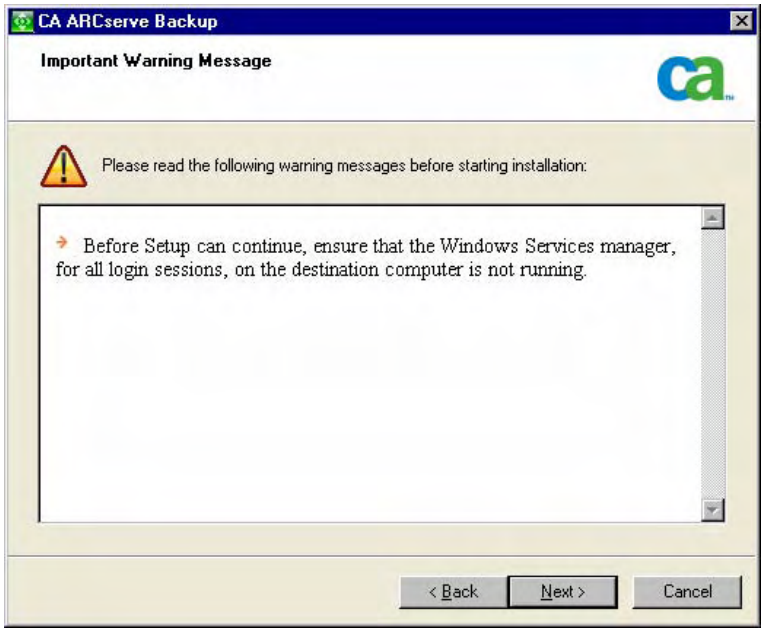
- CA ARCserve Backup does not support local Microsoft SQL Server installations on CA ARCserve Backup servers in NEC ClusterPro environments. In NEC ClusterPro environments, you must install the ARCserve database instance on a remote system.
- You must specify the Remote SQL Server Type option if the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



Important Warning Messages dialog

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

The following graphic illustrates the Important Warning Messages dialog:



Product List dialog

To modify your installation options, click the Back button 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.

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.

Note: You may be required to restart the server when installing CA ARCserve Backup. This depends on whether all of the files, services, and registry settings have been updated on the operating system level.

Installation of CA ARCserve Backup in Each NEC ClusterPro/ExpressCluster Node

In a CA ARCserve Backup HA cluster environment, CA ARCserve Backup is installed in each cluster node, but only one instance will be running. In this cluster, the active node will automatically take control of the backup resources and is referred to as the backup server. Other instances of CA ARCserve Backup that are hosted in passive nodes are referred as standby (or failover) servers and the cluster system will only activate one of them in case of failover.

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 112).
- 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 113).
- For SQL Express primary servers only, use the start.bat script contained in start.bat Script Changes for SQL Express Primary Servers (see page 114).
- For SQL Express primary servers only, use the stop.bat script contained in stop.bat Script Changes for SQL Express Primary Servers (see page 115).

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 2005 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

: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 2005 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
%ARCSERVE_HOME%\babha.exe -killjob
armkill CASMgmtSvc
armkill CASTapeEngine
armkill CASJobEngine
armkill CASDBEngine
armkill CASMessageEngine
armkill CASunivDomainSvr
armkill CASSvcControlSvr
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 2005 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

: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 2005 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
%ARCSERVE_HOME%\babha.exe -killjob
armkill CASMgmtSvc
armkill CASTapeEngine
armkill CASJobEngine
armkill CASDBEngine
armkill CASMessageEngine
armkill CASunivDomainSvr
armkill CASSvcControlSvr
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 r12 in an NEC ClusterPro Environment

When upgrading CA ARCserve Backup from r11.5 to r12 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:

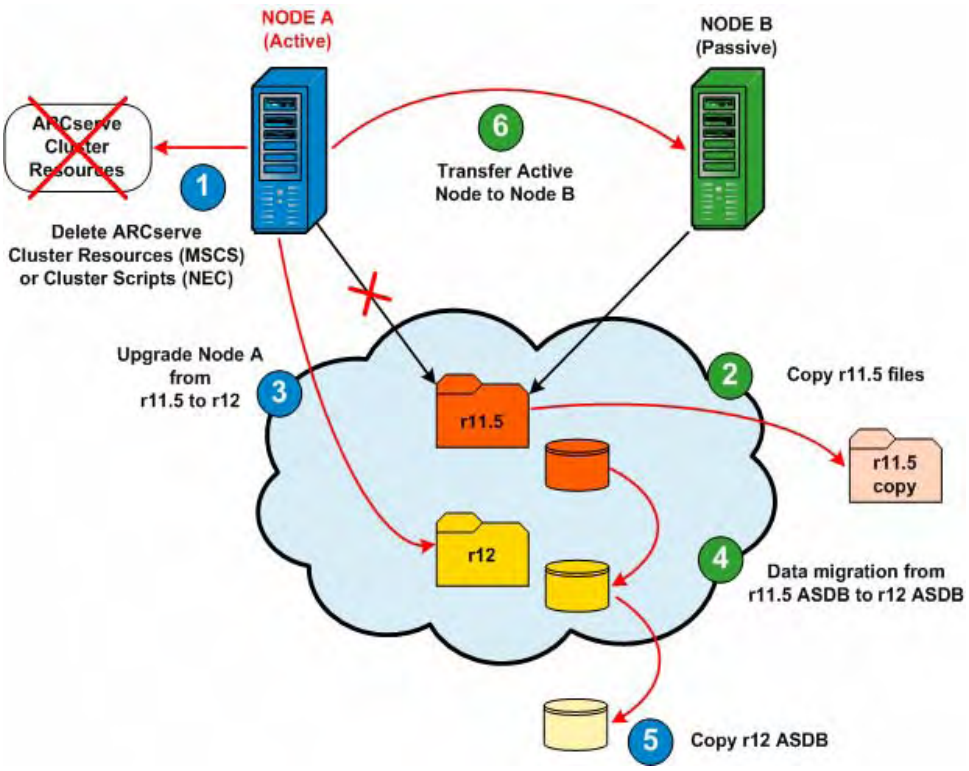
- Upgrade BrightStor ARCserve Backup r11.5 with a RAIMA database to CA ARCserve Backup r12 on a Primary Server with a Microsoft SQL Server 2005 Express Edition database
- Upgrade BrightStor ARCserve Backup r11.5 with a remote Microsoft SQL Server database to CA ARCserve Backup r12 on a Primary Server with a Microsoft SQL Server database
- Upgrade BrightStor ARCserve Backup r11.5 with a RAIMA database to CA ARCserve Backup r12 on a Member Server
- Upgrade BrightStor ARCserve Backup r11.5 with a remote Microsoft SQL Server database to CA ARCserve Backup r12 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 r12 in an NEC ClusterPro environment

On Node A:

The following diagram provides an 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 122).
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 a another location from the original files.

3. Perform CA ARCserve Backup r12 upgrade installation for Node A. For more information, see Upgrade CA ARCserve Backup from a Previous Release (see page 66).

   Important! During the upgrade installation, you will be prompted to specify the installation path location for r12. 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 r12 installation.

   - CA ARCserve Backup for Node A is upgraded from r11.5 to r12. 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. Using the Windows Service manager, right-click the CA ARCserve Backup database engine and from the pop-up window, select Start.

   When the CA ARCserve Backup database engine is started, the corresponding status will indicate Started.

5. From the Server Data Migration dialog (displayed at the completion of the upgrade process), launch the data migration.

   The specified CA ARCserve Backup data is migrated from r11.5 to r12.

6. 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.

7. 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 another location from the original directory.

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

   a. Access the Cluster Manager.

      The Cluster Manager dialog appears.

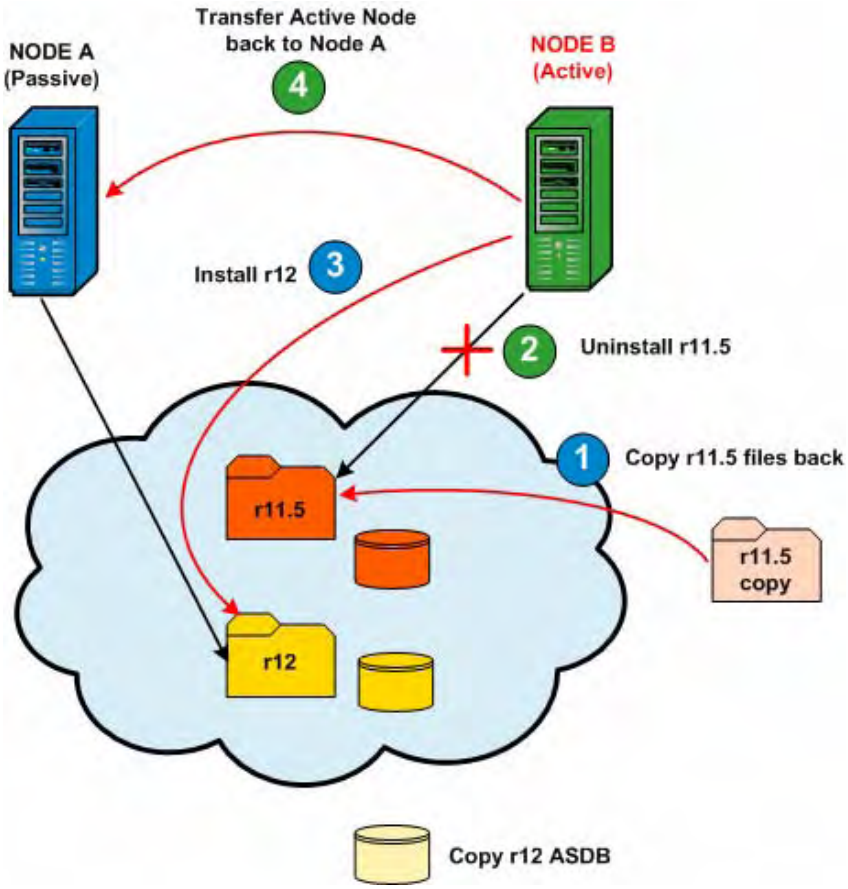
      Note: Cluster Manager is a utility provided by NEC and is installed on servers that have NEC ClusterPro installed. Cluster Manager is accessed from the NEC ExpressCluster Server group of the Start menu. From the Cluster Manager, you perform most of the configuration and management tasks associated with 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 an 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 r12 new installation on Node B, do not select the "Overwrite DB" option to prevent overwriting the ARCserve database that was migrated during the r12 upgrade to Node A.

3. Perform CA ARCserve Backup r12 new installation for Node B with the same settings selected for Node A (domain name, server type, install path, installed options …). For example, if r12 was installed on Node A as a primary server, then r12 must be installed on Node B also as a primary server. For more information, see Install CA ARCserve Backup.

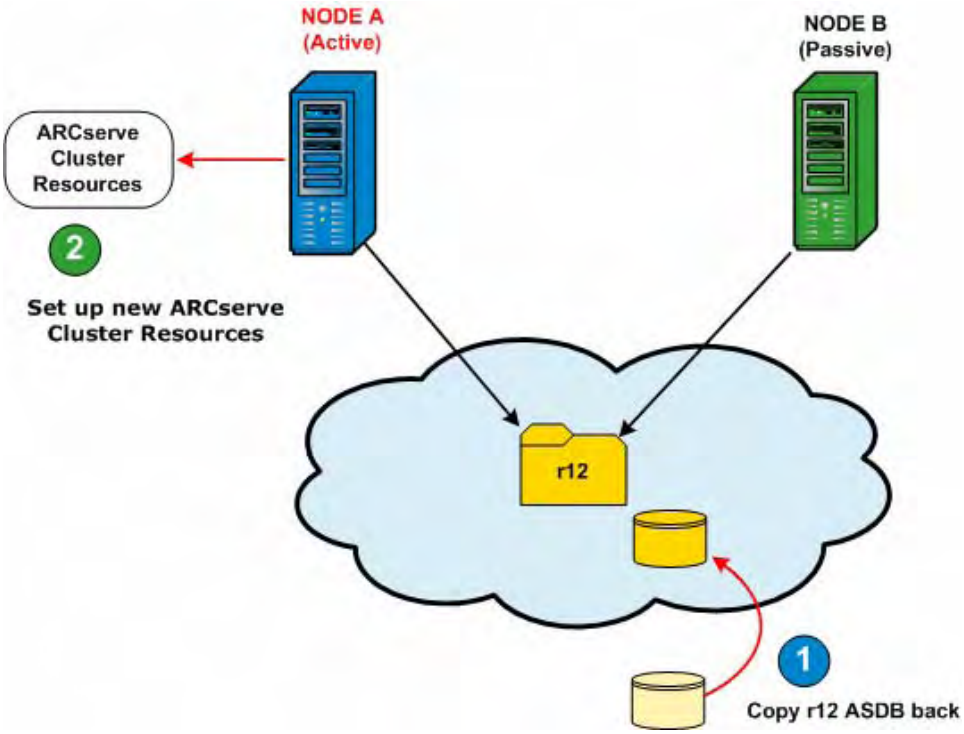
   CA ARCserve Backup r12 is installed on Node B. Do not set up new ARCserve cluster resources at this time.

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 an 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 r12 installation.

2. Rebuild the NEC Cluster Scripts and Registry Sync. For more information, see Enable CA ARCserve Backup in NEC Cluster Scripts (see page 124).

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

Disable CA ARCserve Backup in NEC Cluster Scripts

Cluster scripts and registry keys are inserted during the NEC post-setup process. When upgrading to r12, these cluster scripts need to be disabled and the registry key need to be deleted.

To disable the NEC Cluster Scripts and Registry Key

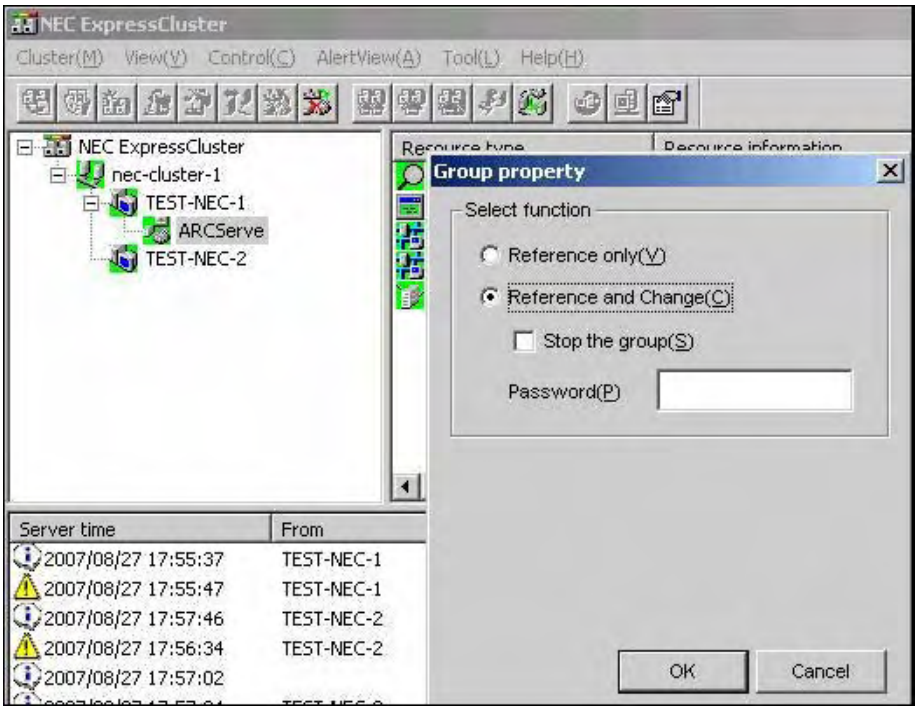
1. Access the Cluster Manager.

   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.

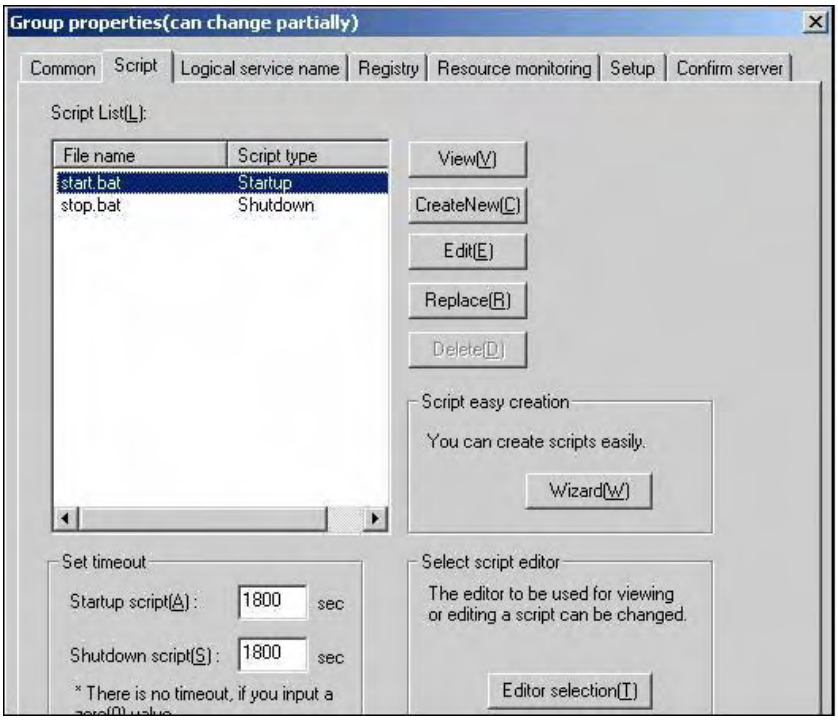
2. Select the NEC Group that the ARCserve server is deployed in, and locate the corresponding ARCserve cluster resources. Right-click on each ARCserve cluster resource and from the pop-up menu, select Property.

   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:

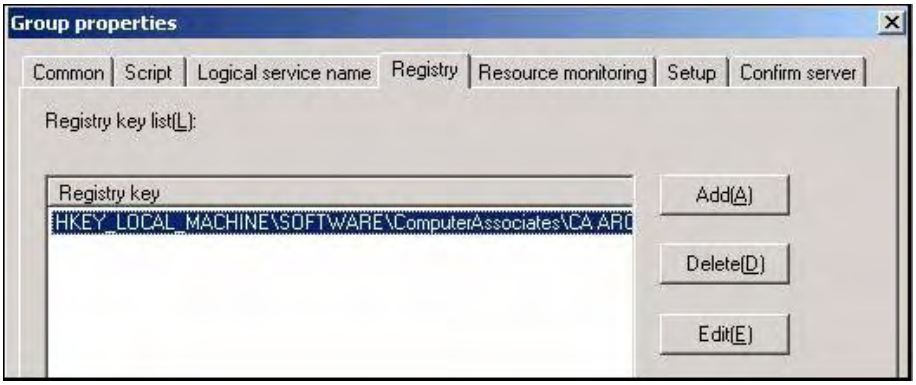
   ```
   SET process=0
   ```

   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 to CA ARCserve Backup r12, part of these 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.

To enable the NEC Cluster Scripts and Registry Key

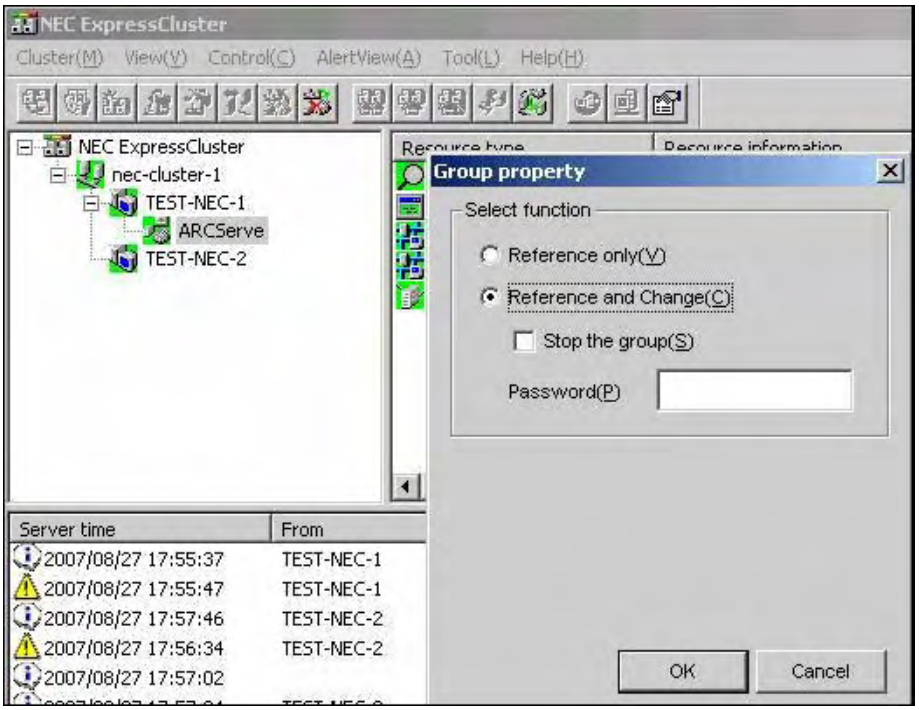
1. Access Cluster Manager.

   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.

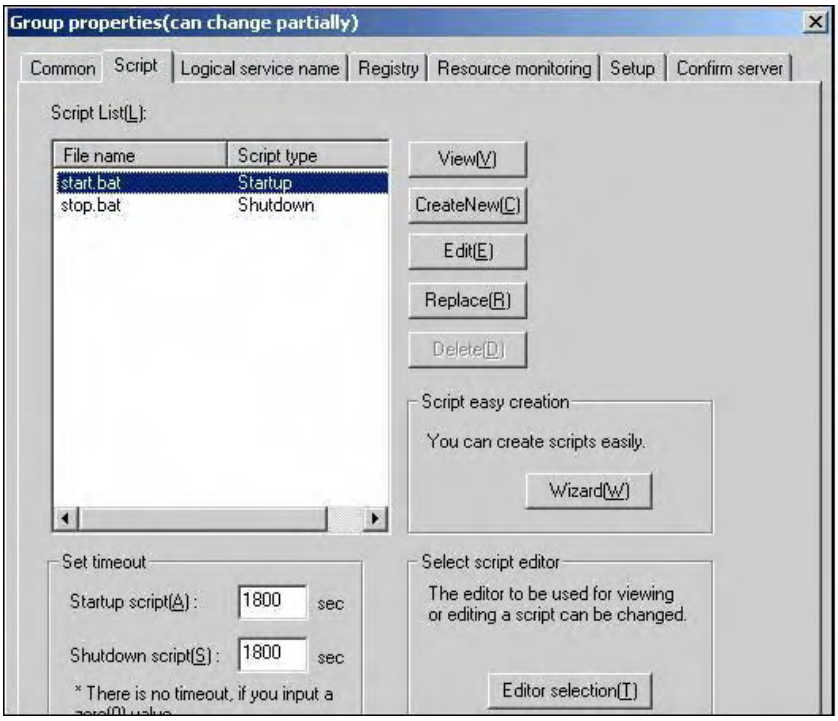
2. Select the NEC Group that the ARCserve server is deployed in, and locate the corresponding ARCserve cluster resources. Right-click on each ARCserve cluster resource and from the pop-up menu, select Property.

   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:

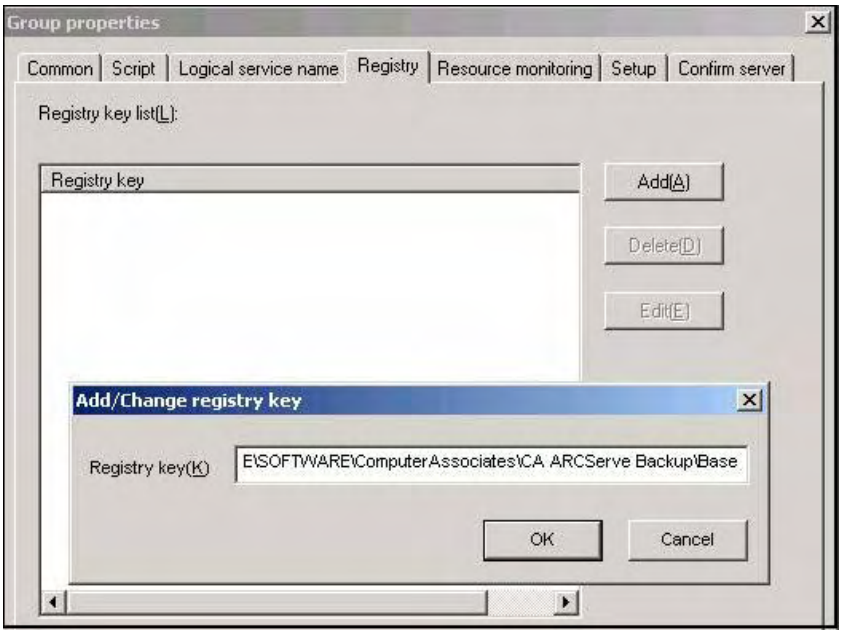
   ```
   SET process=1
   ```

   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.

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 122).

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 into an 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. After the installation or upgrade is complete, open the CA ARCserve Backup Manager Console on a stand-alone server.

   Note: Do not log in to the cluster node at this time.

3. From the Manager Console on the stand-alone system, log in to the newly installed or upgraded system using the virtual name.

4. 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.
5. 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.
6. Open the Server Admin. Ensure that the primary server detects all member servers.
7. Open the Device Manager. Ensure that CA ARCserve Backup detects your devices.
8. 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.
9. 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 ARCserve Backup for Laptops & Desktops

CA ARCserve Backup offers integration with BrightStor ARCserve Backup for Laptops & Desktops. The product is a policy-based solution that provides continuous, intelligent backup of data from both desktop and laptop computers. It can back up all the important data on your company's laptops, remote workstations, and other computers that are frequently disconnected from the network.

However, even after this data has been backed up, the BrightStor ARCserve Backup for Laptops & Desktops server itself is still vulnerable to failure. By using CA ARCserve Backup to back up your BrightStor ARCserve Backup for Laptops & Desktops data to media, you can protect yourself against the possibility of a disaster on your BrightStor ARCserve Backup for Laptops & Desktops server. To back up your BrightStor ARCserve Backup for Laptops & Desktops data, the CA ARCserve Backup Client Agent for Windows must be installed on the computer running the BrightStor ARCserve Backup for Laptops & Desktops Server, even if the server is the local computer.

Note: For information about backing up and restoring BrightStor ARCserve Backup for Laptops & Desktops data using CA ARCserve Backup, see the *Administration Guide*.

eTrust Antivirus Integration

eTrust 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 the eTrust Antivirus program to download updated virus signature files and program modules. These updates are then distributed to the participating applications. When this is complete, eTrust Antivirus broadcasts a message stating that the update has been completed. Under certain conditions, you must stop and restart the job engine to fully update the antivirus protection.

Note: CA ARCserve Backup provides only the scanning and curing components. It does not provide a full install of eTrust Antivirus.

For more information, see the *Administration Guide*.

Integrate with Microsoft Management Console

CA ARCserve Backup lets you integrate with Microsoft Management Console when you are running the following Windows operating systems:

- Windows 2000
- Windows XP
- Windows 2003
- Windows Server 2008

This capability lets you customize your access to CA ARCserve Backup. Using Microsoft Management Console, you can create shortcuts so that you can quickly open the CA ARCserve Backup components you need, rather than accessing them using the program group.

Important! You must install CA ARCserve Backup and restart your system before you can use Microsoft Management Console to customize your access.

To integrate with Microsoft Management Console

1. Open a command prompt, enter mmc and press Enter or click OK.

   The Console screen appears.

2. From the File menu (the Console menu on Windows), select the Add/Remove Snap-in.

   The Add/Remove Snap-in dialog opens.

3. From the Add/Remove Snap-in dialog, click Add.

   The Add Standalone Snap-in dialog appears.

4. From the Add Standalone Snap-in dialog, select CA ARCserve Backup, click Add, and then click Close.

   CA ARCserve Backup appears in the Snap-in field in the Add Standalone dialog.

5. Click OK.

6. From the File menu (the Console menu on Windows), select Save As, and enter a name for your console.

   You can now access CA ARCserve Backup using the customized console you created. After you save and close your console, you can access it again using the command prompt. To do so, enter mmc and press the Enter key or click OK. When the Console screen appears, from the File menu (the Console menu on Windows 2000), select Open, select the name of your console, and click Open.

Unicenter NSM Integration

CA ARCserve Backup integrates with the WorldView and the Job Management Option components of Unicenter Network and Systems Management (NSM) (formerly known as Unicenter TNG).

Note: Before Unicenter NSM r11, the Job Management Option was known as Workload Management.

The following sections include information on integration with each of these components.

WorldView Integration

The WorldView Integration component supports Unicenter NSM and Unicenter CA Common Services (CCS) (formerly known as Unicenter TNG framework).

WorldView Integration Requirements

To integrate with WorldView, the following components are required:

- Unicenter NSM or CCS
- CA ARCserve Backup
- CA ARCserve Backup Unicenter Integration Option

Note: You must install the CA ARCserve Backup Unicenter Integration Option on the same system that has the Unicenter WorldView components installed.

Create Objects Using the Object Creation Program

To integrate with WorldView, you must run the Object Creation program. The Object Creation program discovers CA ARCserve Backup servers on the network and creates objects for each server in the Unicenter NSM repository. It creates these objects under each CA ARCserve Backup server's Unispace

The Object Creation program also creates a business process view called CA ARCserve Backup View, which represents a view of all CA ARCserve Backup objects.

Note: Run the Unicenter Auto Discovery program before running the Object Creation program. If any new servers have been installed or the repository was rebuilt, Unicenter Auto Discovery discovers machines and synchronizes CA ARCserve Backup servers on the network and objects in the repository. However, the discovery program cannot discover BrightStor ARCserve Backup UNIX on subnets not containing any Windows NT, Windows 2000, Windows 2003, and Windows XP machines. To discover these machines, you must specify the subnet containing the CA ARCserve Backup UNIX machines you want to discover. To do this, use the DSCONFIG.EXE utility located in the CA ARCserve Backup home directory. After specified, click the Discover Now button to discover the BrightStor ARCserve Backup Object Creation Utility.

Note: If you are working with a remote repository, see Remote Repositories (see page 135).

To create objects

1. From the CA ARCserve Backup program group, select Object Creation.
2. If you want to delete all CA ARCserve Backup objects in the repository before creating new ones, select Delete existing objects. This lets you synchronize CA ARCserve Backup servers on the network and CA ARCserve Backup objects in the repository. If you do not select this, the program adds new CA ARCserve Backup objects and updates existing ones if necessary.
3. Click Start to proceed. When you are asked to sign on to the repository, enter the repository user ID and password, and then click OK.
4. Wait until the process completes or click Stop to cancel the operation.
5. Click Start to re-start or Close to exit the program.

   Note: The setup program also creates CA ARCserve Backup class definitions in the Unicenter object repository. If you rebuild the repository, all CA ARCserve Backup class definitions will be removed. To recreate class definitions, re-install the program or run the CSTNGCLS.EXE utility. The CSTNGCLS.EXE utility is in the TNGWV\BIN directory (TNGFW\BIN if you are running CCS).

Remote Repositories

By default, the Object Creation program creates CA ARCserve Backup objects in the local Unicenter repository. If the local WorldView is set up to work with a repository on a remote machine, the Object Creation program requires an additional parameter. To enter this parameter, run the Object Creation program from a command prompt and, from the CA ARCserve Backup home directory, enter one of the following commands:

```
CSTNGX.EXE /R REPOSITORY_NAME
```

```
CSTNGX.EXE /R
```

If you do not specify the repository name with "/R" and click Start, a dialog appears, prompting you to enter an available repository.

Note: CCS does not support remote repository configuration.

Unicenter Notification

CA ARCserve Backup offers Alert Manager, which supports Unicenter Notification. Using Alert Manager you can send all events to the Unicenter Event Manager Console and WorldView repository. The Alert Notification Service must be running to send events to the Unicenter Event Management Console and WorldView repository.

Note: For more information on using the Alert Manager with Unicenter, see the *Administration Guide*.

Managing CA ARCserve Backup Using Unicenter

Using the Unicenter 2D or 3D Map, you can see the CA ARCserve Backup View and CA ARCserve Backup Objects. When you right-click an object, the context menu opens. From the context menu, you can launch the Job Status Manager, Backup Wizard, Restore Wizard, Device Wizard, and the Manager Console.

Integrate with the Job Management Option

CA ARCserve Backup integrates with the Job Management Option when you submit a backup job from the command line using the following command line syntax:

```
ca_backup.exe -waitForJobStatus

ca_restore.exe -waitForJobStatus

ca_merge.exe -waitForJobStatus

ca_scan.exe -waitForJobStatus

ca_qmgr.exe -waitForJobStatus
```

These utilities provide automation by using the /J (returns the job return code) and /W (wait for job completion) switches.

Note: Before Unicenter NSM r11, the Job Management Option was known as Workload Management.

When you use these utilities, CA ARCserve Backup waits until the operation is completed, and then exit with a return code that indicates the success or failure of the job. For more information on ca_backup, ca_restore, ca_merge, ca_scan, ca_qmgr, and cabatch, see the *Command Line Reference Guide*.

To integrate with the Job Management Option

1. From the Command Prompt, enter caugui settings.
2. Click the Options tab on the right-hand side of the notebook.
3. Click the Job Management Option tab on the bottom of the notebook.
4. Enter Y in the Submit jobs on behalf of another user field.
5. From the Control Panel, select Administrative Tools, Services. When the Services dialog appears, highlight CA-Unicenter, right-click and select Stop. Then, right-click CA-Unicenter again and select Start.
6. Enter a Job Set.
7. Enter a Job with the following detail on the Submission Run-As tab:
   - Filename
   - User
   - Domain
   - Password
8. Demand Job.

CA XOsoft Integration

CA XOsoft a data protection solution that uses 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 XOsoft is a separately-sold CA product.

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

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

The Manager Console is an interface that lets you administer backup and restore operations in your environment. With the Manager Console, you can log in to and administer local and remote ARCserve servers and domains.

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

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

     The Manager Console opens.

   - 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.

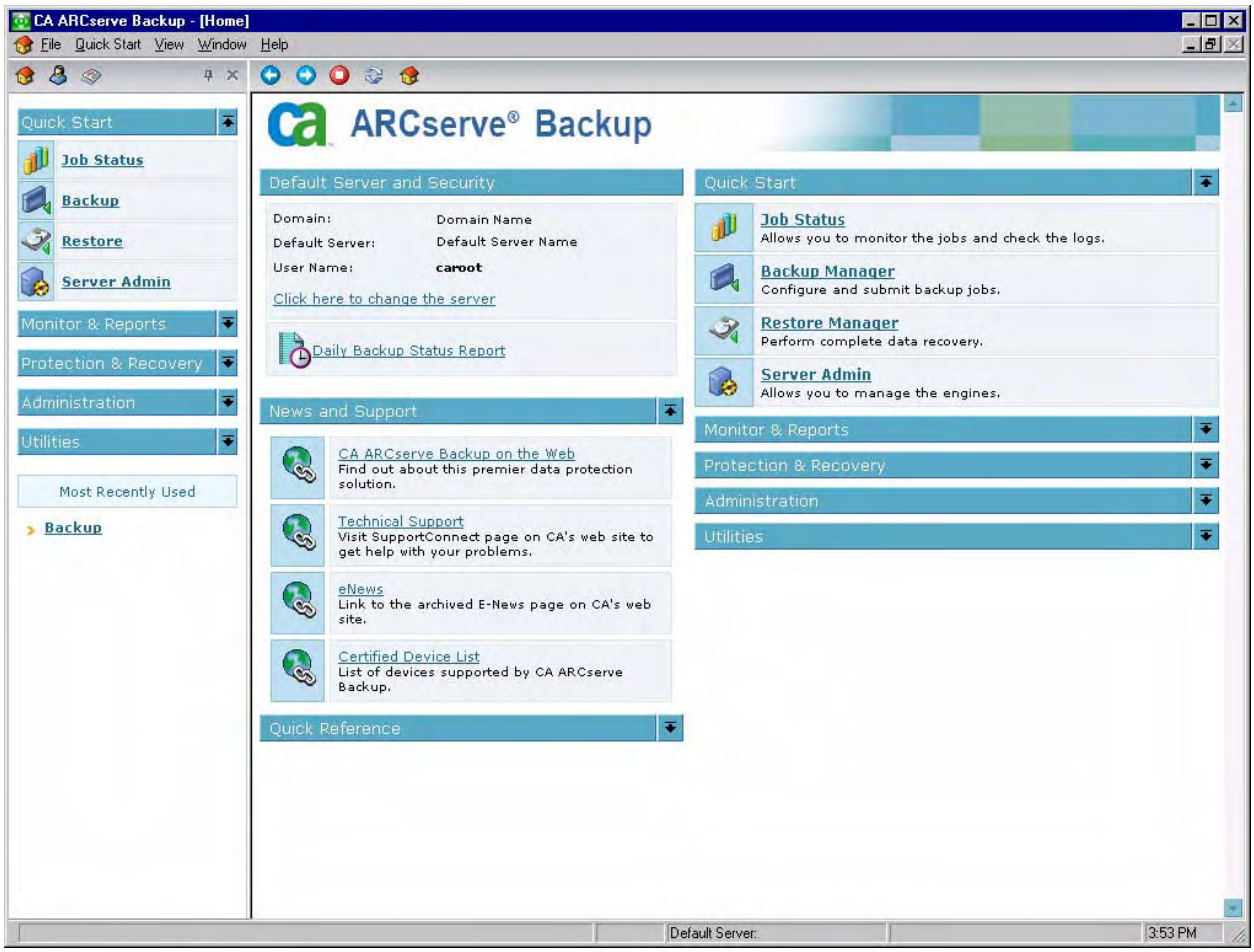
     The Manager opens.

     Note: If you installed the previous release in the default installation directory, and used the upgrade process to install CA ARCserve Backup, you can open the Manager by doing the following:

     Click the Windows Start button, select Programs, CA, ARCserve Backup, and click Manager.

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, as shown in the following illustration:



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 log in to a different CA ARCserve Backup primary or stand-alone server, see Log On to CA ARCserve Backup (see page 145).

- View the Daily Backup Status Report.

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.

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.

Protection and Recovery

Lets you open the following managers and wizards:

- **Backup Manager--**Lets up configure and submit backup jobs.
- **Restore Manager--**Lets you perform complete data recovery.
- **CA XOsoft--**Indicates a data protection solution that uses asynchronous real-time replication to provide disaster recovery capabilities. This link is active when you install CA XOsoft. For information, see the *CA XOsoft Integration Guide*.
- **Backup Wizard--**Guides you through the process of creating and submitting a backup job of a single machine without running the Backup Manager.
- **Restore Wizard--**Guides you through the process of restoring your data. Using this wizard, you can submit a restore job to the job queue without using the Restore Manager.

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.
- **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 the 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.

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.
- **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 machine.
- **Count--**Lets you count the files and directories on a machine.
- **Copy--**Lets you copy or move files from one hard disk to another.
- **Purge--**Lets you delete files and directories from a machine.

News and Support

The News and 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.
- **Technical Support--**Offers the latest news and information from Technical Support, including white papers, how-to documents, troubleshooting guides, patches, and more.
- **eNews--**Links you to the Storage E-News Archive page, allowing you to access technical newsletter archives providing helpful technical information from service packs, hints and tips, product updates or upgrades, and more.
- **Certified Device List--**Links you to an up-to-date list of all devices currently supported by CA ARCserve Backup.

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

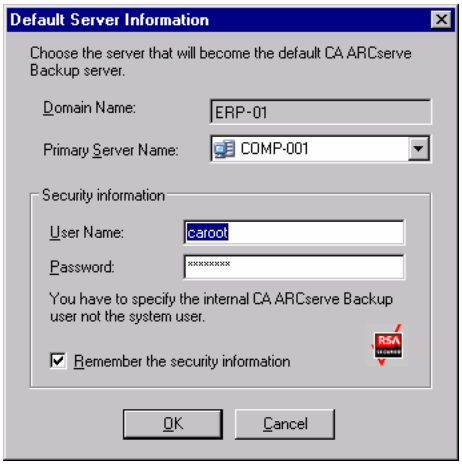
From the home page, you can log on to CA ARCserve Backup. The first time you log on to CA ARCserve Backup, you must log on as caroot (which automatically has administrator privileges) and provide the appropriate password in the password field. If you do not log on as caroot, you cannot use wizards, managers, or utilities, or perform any action.

After you log on, you can change the password for the caroot user and add new users using the command line utility, ca_auth.exe.

Note: For more information on caroot and managing user profiles, see the *Command Line Reference Guide.*

To log in to CA ARCserve Backup

1. Select the Click Here to Change Server link on the upper-left side of the CA ARCserve Backup Home Page. The Default Server Information page appears.
2. To change the default server, select a new server, and specify the server type, as shown in the following screen:



3. To save the user name and password information you enter for this server, select the option Remember the Security Information. If you do not save this information, a server security dialog appears the first time you open a manager, and you are required to enter a 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 on 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 on. 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 write-protected media in all Format and Erase dialogs.

   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.

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 tree items 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 tree items 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 the 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 2003 Server 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)

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:

Important! On Windows 2003 Server SP1 configurations, start at Step 5.

1. From the Start menu, open the Run dialog, enter gpedit.msc, and click OK.

   The Group Policy window opens.

2. In the Group Policy window, browse to Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, Local Policies, and select Security Options.

   From the list of polices, locate and right-click the Network access:Sharing and security model for local accounts security option and select Properties.

   The properties dialog for this option opens.

3. From the drop-down list, change the setting from Network access:Sharing and security model for local accounts to Classic - local users authenticate as themselves. Click Apply to save this setting and click OK to close the dialog.

4. From the Start menu, open the Run dialog, enter regedit.exe, and click OK.

   The Windows Registry Editor opens.

   Create the following key RPC and subkey called RestrictRemoteClients and set the value to 0:

   ```
   [DWORD]HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients
   ```

   Close the Windows Registry Editor.

5. Open the Security Center (Windows XP SP2) or Windows Firewall (Windows 2003 Server SP1) and enable the firewall.

Add the following executables, as applicable for your installation, to the Security Center or Windows Firewall Exceptions list:

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

- caauthd.exe
- cadiscovd.exe
- carunjob.exe
- casdscsvc.exe

  Note: This executable resides in the following directory:

  \CA\SharedComponents\ARCserve Backup\CADS

- caserved.exe
- catirpc.exe

  Note: This executable resides in the following directory:

  \CA\SharedComponents\ARCserve Backup\ASPortMapper

- dbeng.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.

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

Method 2:

1. From the Start menu, open the Run dialog, enter gpedit.msc, and click OK.

   The Group Policy window opens.

2. In the Group Policy window, browse to Local Computer Policy, Computer Configuration, Windows Settings, Security Settings, Local Policies, and select Security Options.

   From the list of polices, locate and right-click the Network access:Sharing and security model for local accounts security option and select Properties.

   The properties dialog for this option opens.

3. From the drop-down list, change the setting from Network access:Sharing and security model for local accounts to Classic - local users authenticate as themselves. Click Apply to save this setting and click OK to close the dialog.

   Note: This is the default setting on Windows 2003 Server SP1.

4. From the Start menu, open the Run dialog, enter regedit.exe, and click OK.

   The Windows Registry Editor opens.

   Create the following key RPC and subkey called RestrictRemoteClients and set the value to 0:

   ```
   [DWORD]HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\RPC\RestrictRemoteClients
   ```

   Close the Windows Registry Editor.

5. Open the Security Center (Windows XP SP2) or Windows Firewall (Windows 2003 Server SP1) and disable the firewall.

   Click OK and close the Windows Firewall dialog.

   Your new settings are saved.

6. 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 2003 Server 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 ARCserve 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 Protections 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 ASDBPROJOB. 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.

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 (OBDC), 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 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.

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 Finish.

7. Click Exit to close Device Configuration.

8. 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.

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 178).

- 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 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.

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, or Windows 2003.

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, caloggerd, 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 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 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

LQServer.exe

This service is 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

Mediasvr.exe

This service is 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

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|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]

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

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 169).

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

- Default Port: 41524
- Protocol: UDP

Discovery response

- Default Port: 41523
- Protocol: TCP

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 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 Database Communication Ports (see page 171).

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 Document Level Communication Ports

For the document level backups using the Agent for Microsoft Exchange, 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

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 Database Communication Ports

For the Agent for Microsoft SharePoint, you can configure the following ports for database communication in the PortsConfig.cfg file:

Backup Agent Remote Service

This services 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 Win2000/WinXP/W2003)

This service is used only for MSRPC using Named Pipes. This is not a configurable port.

- Default Port: 445
- Protocol: TCP

Agent for Microsoft Exchange Database Level and Brick Level Communication Ports

For the Exchange Database Level and Brick Level Agent, you can configure the following communication ports in the PortsConfig.cfg file:

Backup Agent Remote Service

This service is used for backup and restore operations.

- Default Port: 6074
- Protocol: TCP

Backup Agent RPC Service

This service is required for GUI Browsing and all 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 services is used only for MSRPC using Named Pipes. This is not a configurable port.

- Default Port: 139
- Protocol: TCP

MS port (only Win2000/WinXP/W2003)

This service is used 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): 6071
- 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)

The is service is used for MSRPC using Named Pipes. You cannot configure this port.

- Default Port: 139
- Protocol: TCP

MS port (only Win2000/WinXP/W2003)

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.

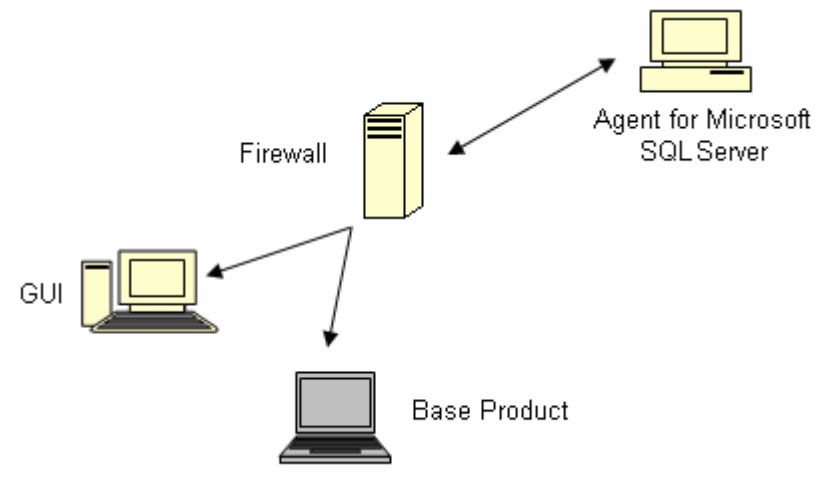
Note: For more information, see Ports Used by CA ARCserve Backup Agents and Options (see page 169).

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

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
```

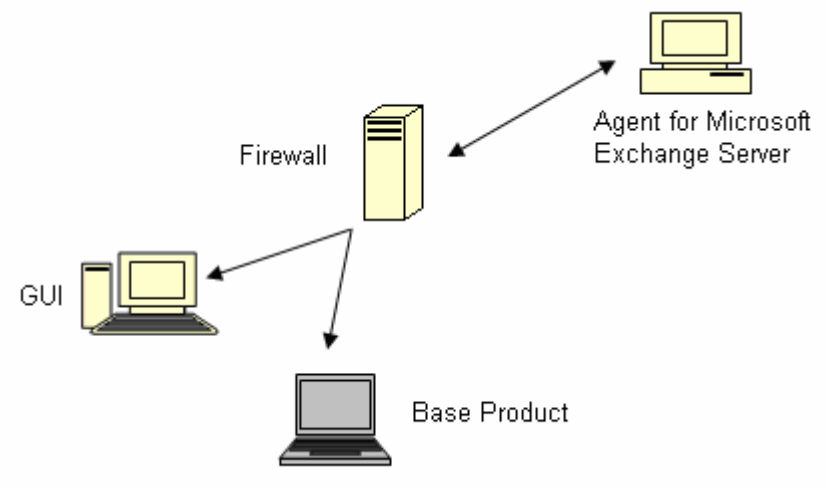
On the firewall, open thse four ports and additional port 135. Port 139 or Port 445 must be opened only if the Agent for Microsoft SQL Server is configured to use the Named Pipes transport. They should allow incoming connections to the agent machine.

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 Using Named Pipes

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
exchangeagenttcpserverlevel  6074
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:

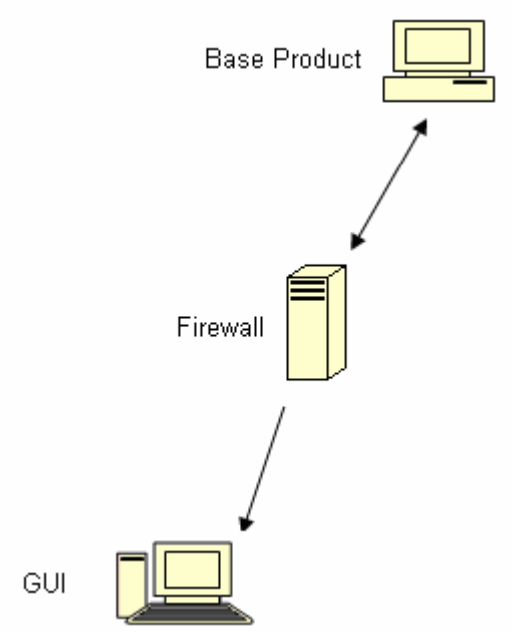
```
ENABLE_CONFIGURABLE_PORTS=1
Dbagentsrpcserver            6071      ExchangeAgentMachineName
```

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
caloggerd            9002
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
caloggerd            9002    BaseproductMachinename
caauthd              9003    BaseproductMachinename
casdscsvctcp         41523
casdscsvcudp         41524
```

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
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
Exchange server level backup	dbasvr.exe	exchangeagenttcpserverlevel	6074	TCP
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
Domain Server	caloggerd.exe	caloggerd	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
exchangeagenttcpserverlevel       6000    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 backup 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) and for document level backups using the CA ARCserve Backup Agent for Microsoft Exchange (exchangeagenttcpserverlevel) for TCP-based services (fsbackupservice, sqlagenttcpservice, exchangeagenttcpserverlevel).

- 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, 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, and the CA ARCserve Backup NDMP NAS Option). If you add a machine with a Windows NT, Windows 2000, Windows XP, or Windows 2003 operating system, browsing functionality is performed through the Universal Agent.
- Changing the ports for the CA ARCserve Backup Agent for Microsoft Exchange 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
   ```

Appendix A: 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

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

More information:

Supported Platforms (see page 37)
Supported Devices (see page 37)
Types of CA ARCserve Backup Server Installations (see page 40)
Database Requirements (see page 43)
Post-Installation Tasks (see page 82)

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 2005 Express Edition.
- If your new ARCserve environment will consist of an ARCserve domain with a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.
- Microsoft SQL Server 2005 Express Edition is not supported on IA-64 (Intel Itanium) operating systems.
- Microsoft SQL Server 2005 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 43).

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 and Microsoft SQL Server 2005 Express Edition, you can centrally manage up to ten member servers. If you require more than ten member servers, you should host the ARCserve database using Microsoft SQL Server. Additionally, a primary server lets you 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 (see page 40).

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.

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 ARCserve domain. You must install the Central Management Option when you install the Primary Server option.

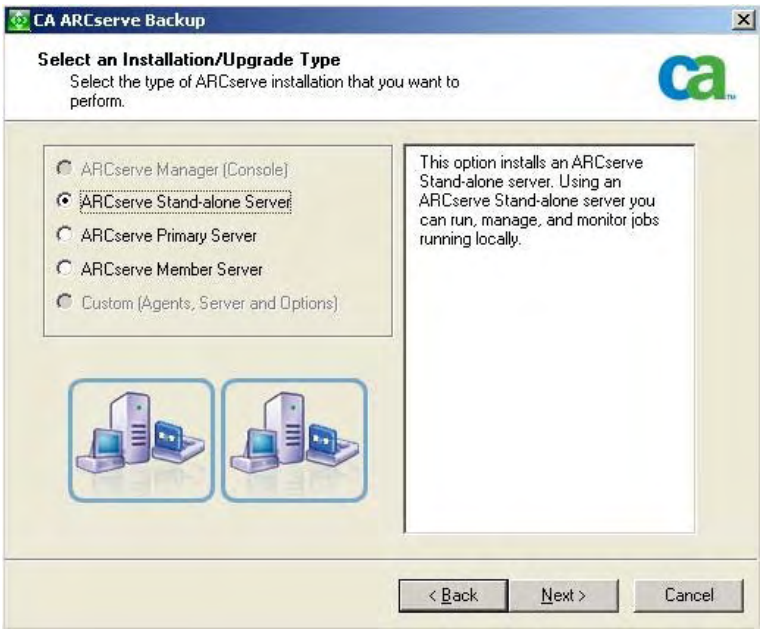
The following diagram illustrates the topology of a CA ARCserve Backup Stand-alone Server or a CA ARCserve Backup Primary Server.

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

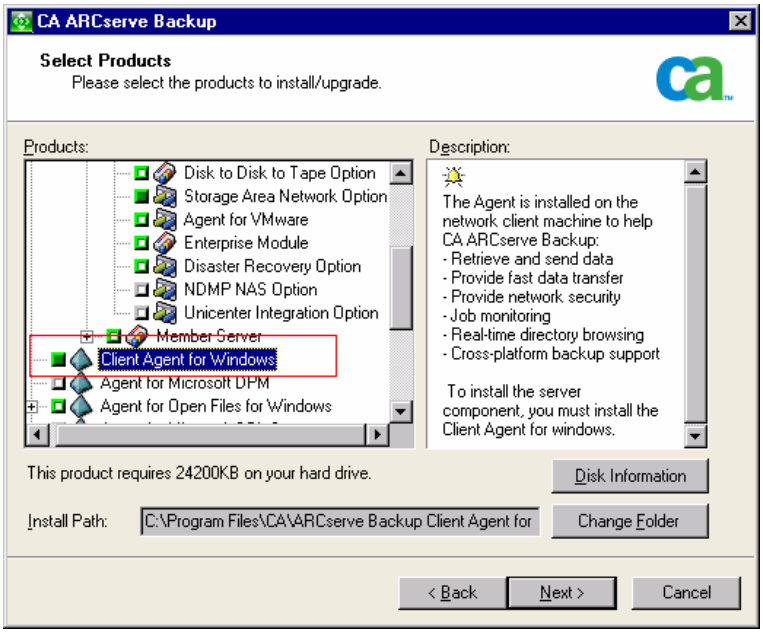
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard 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

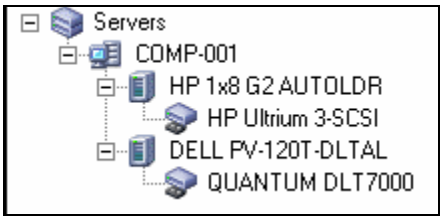
To ensure that your CA ARCserve Backup installation functions properly, complete the following tasks:

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.

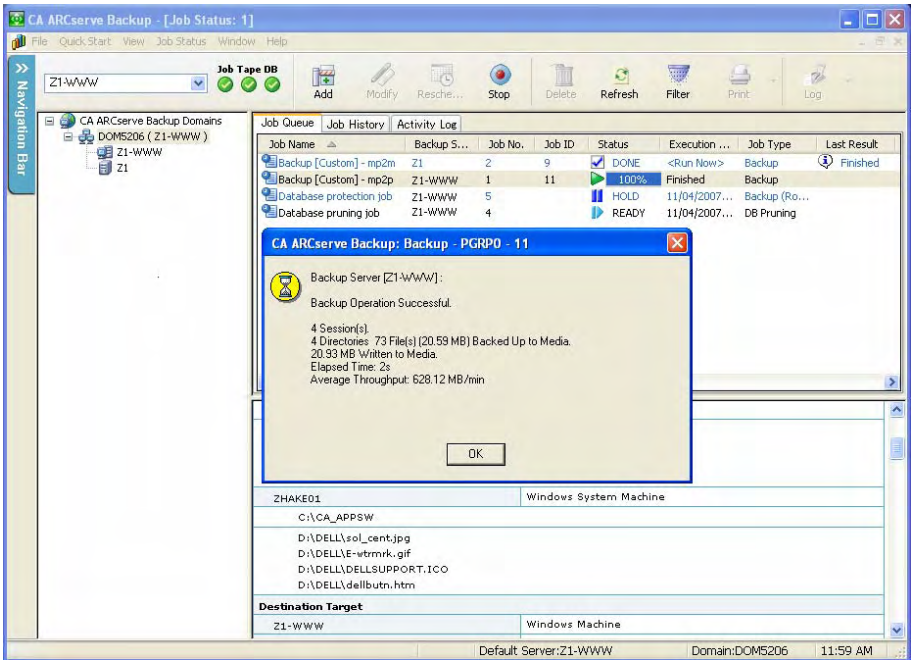
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following diagram illustrates a successful backup job:



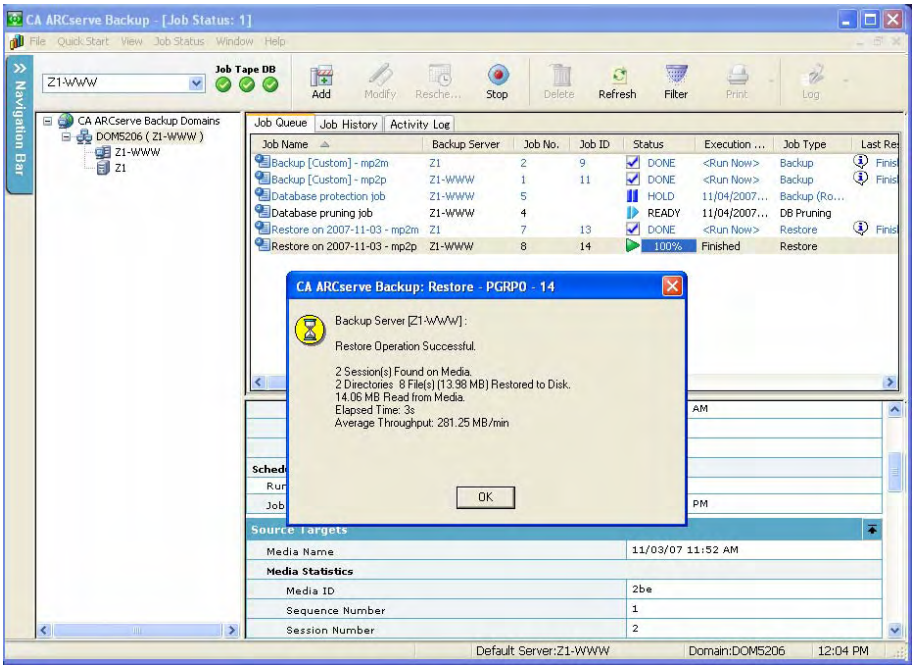
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following diagram illustrates a successful restore job:



   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.

Recommended Configuration

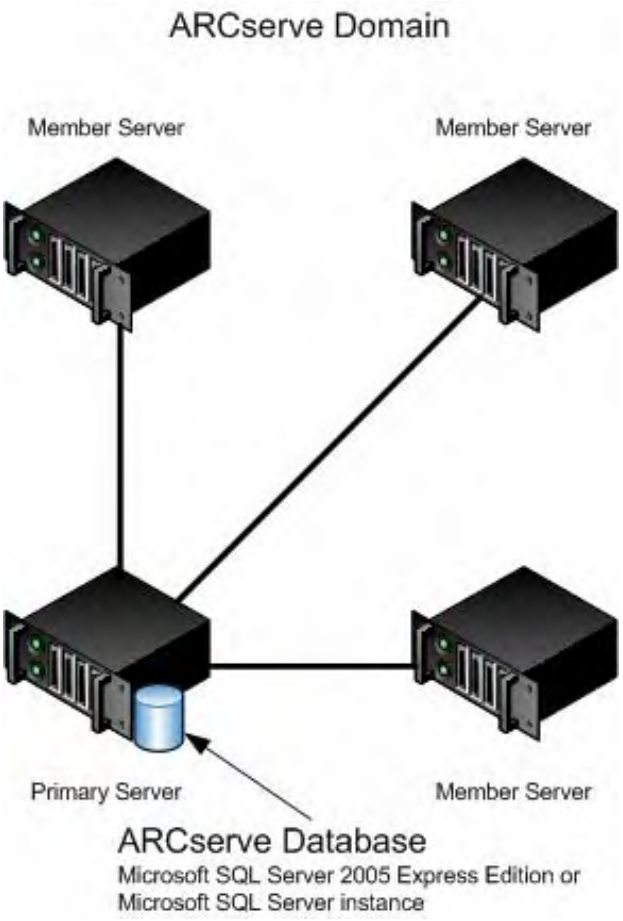
When you require multiple backup servers that reside in the same domain to protect your environment, the best practice is to install CA ARCserve Backup using the Primary Server and Member Server installation options. With this configuration, you can create a centralized management environment.

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 ARCserve servers in your environment. You can then use the Manager Console to manage the primary server.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 Express Edition, the installation wizard installs the database application and the ARCserve database instance on the primary server. To host the ARCserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the topology of a centralized management environment. The environment consists of a primary server and one or more member servers. The ARCserve database is hosted by Microsoft SQL Server 2005 Express Edition and the database instance resides on the primary server.

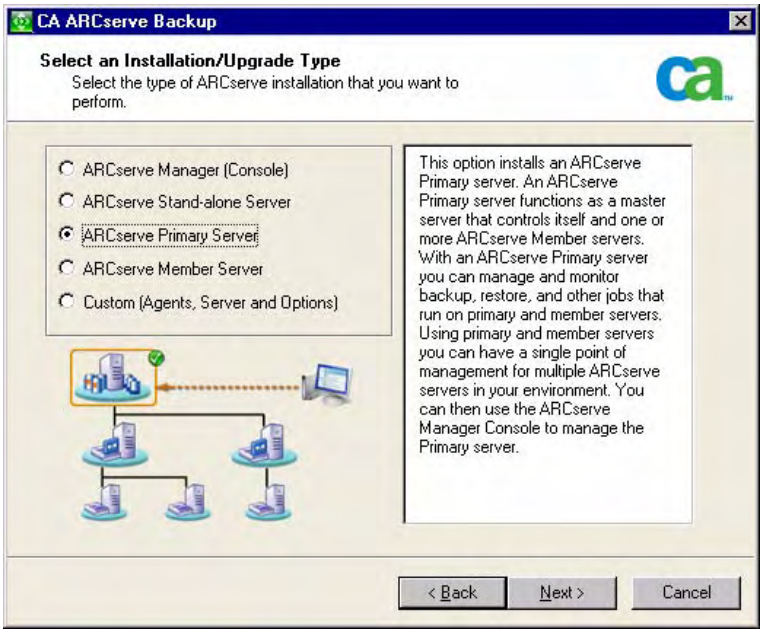


Components You Must Install

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

CA ARCserve Backup Primary Server

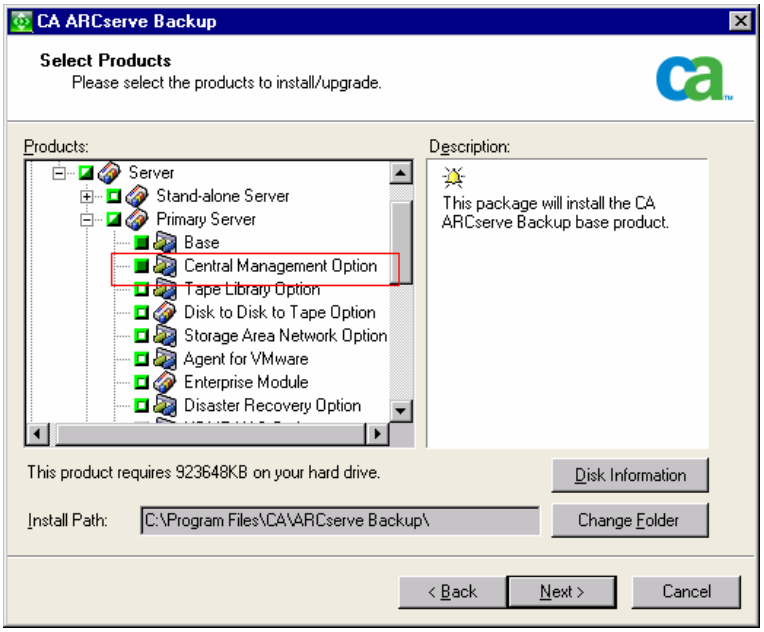
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

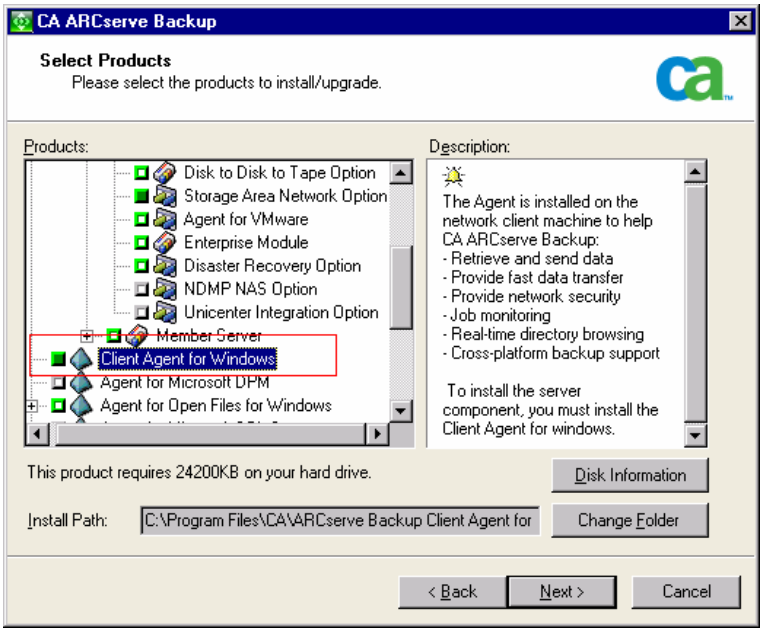
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

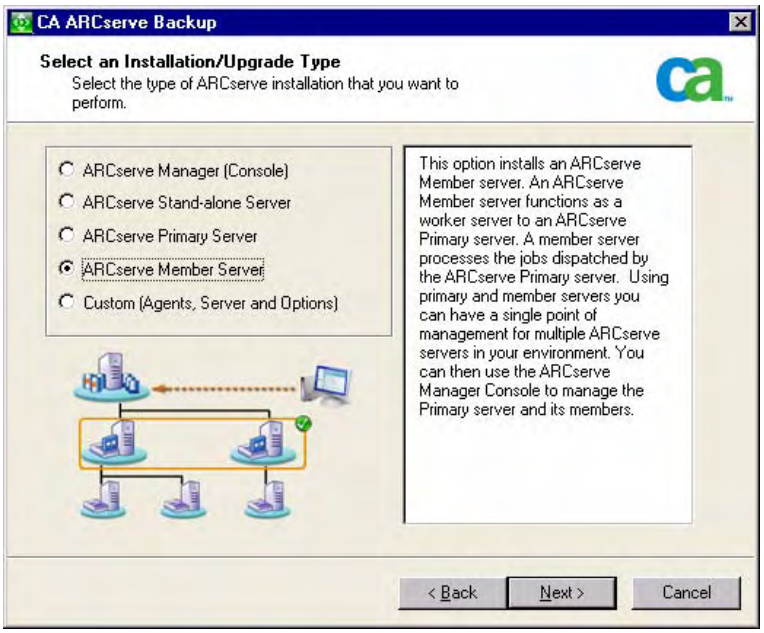
CA ARCserve Backup Client Agent for Windows

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.



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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database.

   If your ARCserve environment will consist of more than ten member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

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

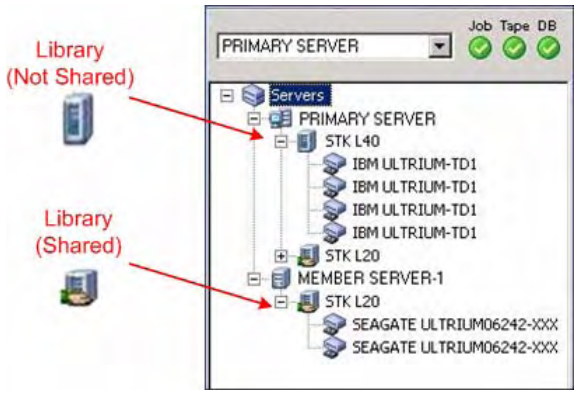
3. Open the Database Manager and the Job Status Manager.

   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.

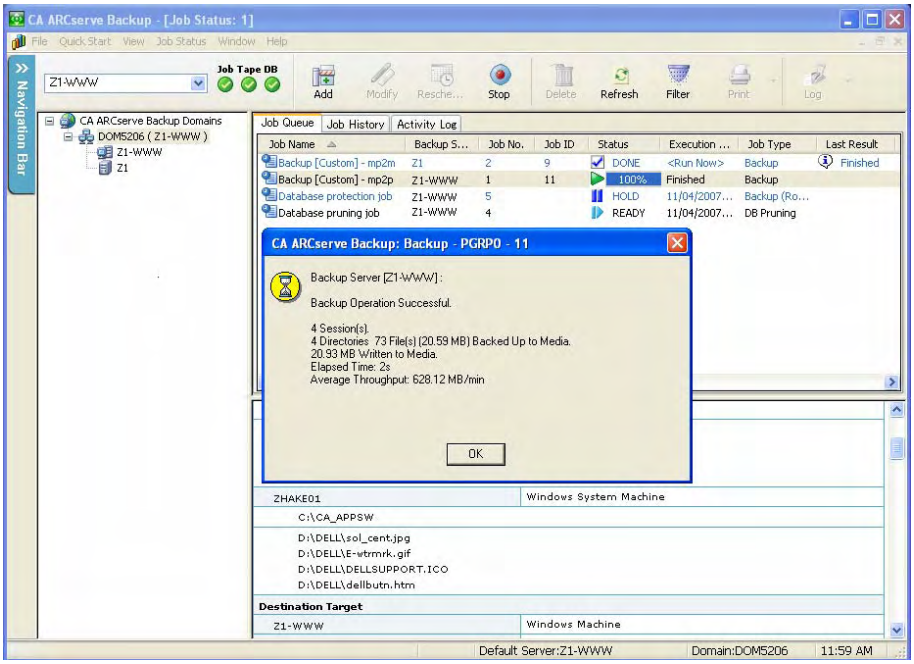
   Note: For information about configuring devices, see the online help or the *Administration Guide*.

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.

   The following screen illustrates a successful backup job on a primary server:



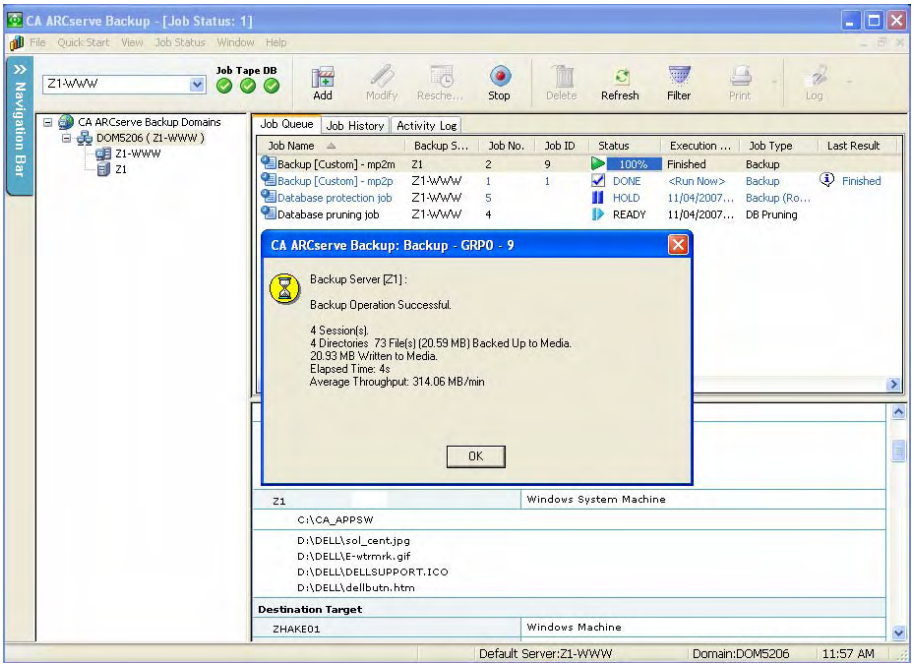
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



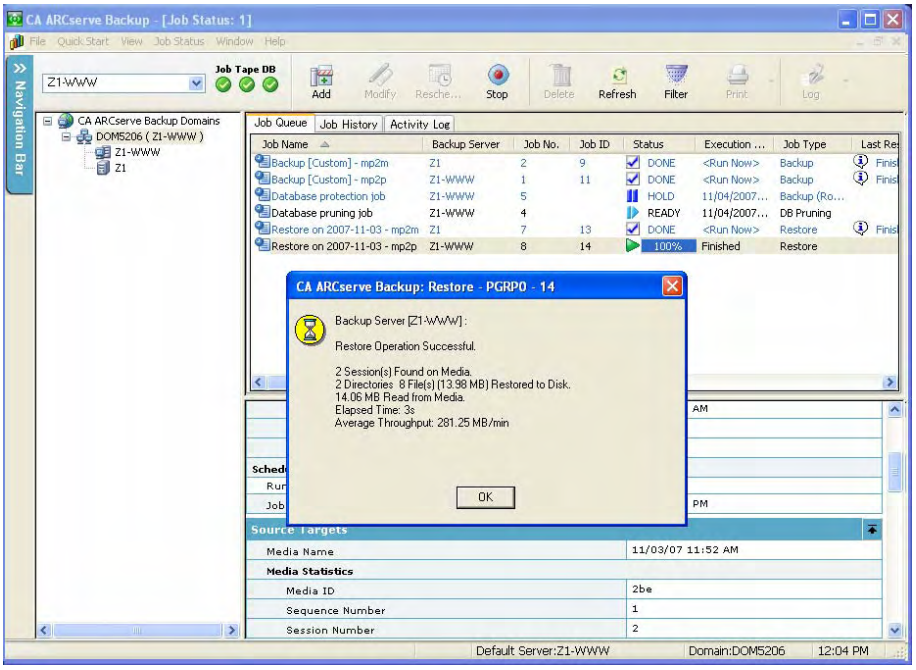
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



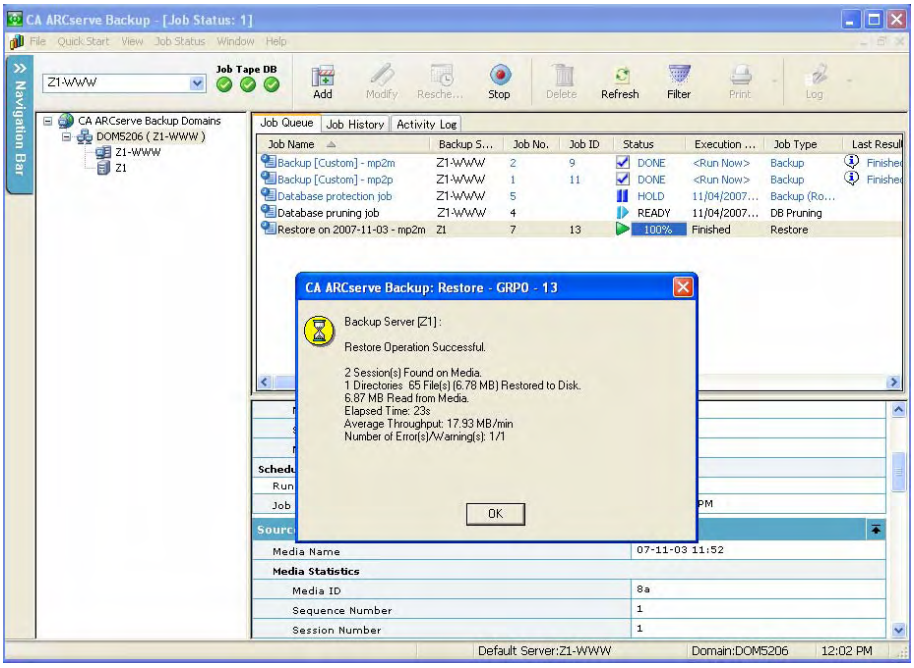
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   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.

Recommended Configuration

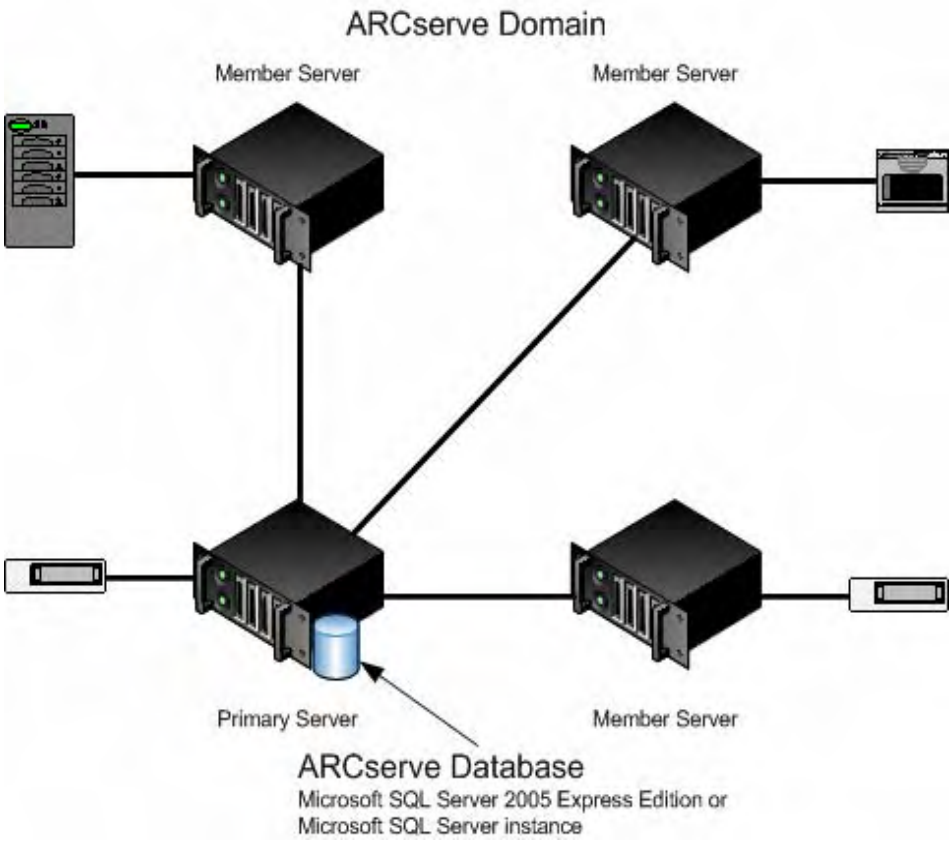
When you require multiple backup servers that reside in the same domain and devices, such as libraries, to protect your environment, the best practice is to install CA ARCserve Backup using the Primary Server and Member Server installation options. With this configuration, you can create a centralized 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 ARCserve servers in your environment. You can then use the Manager Console to manage the primary server.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 with attached devices. The environment consists of a primary server and one or more member servers. The ARCserve database is hosted by Microsoft SQL Server 2005 Express Edition and the database instance resides on the primary server.

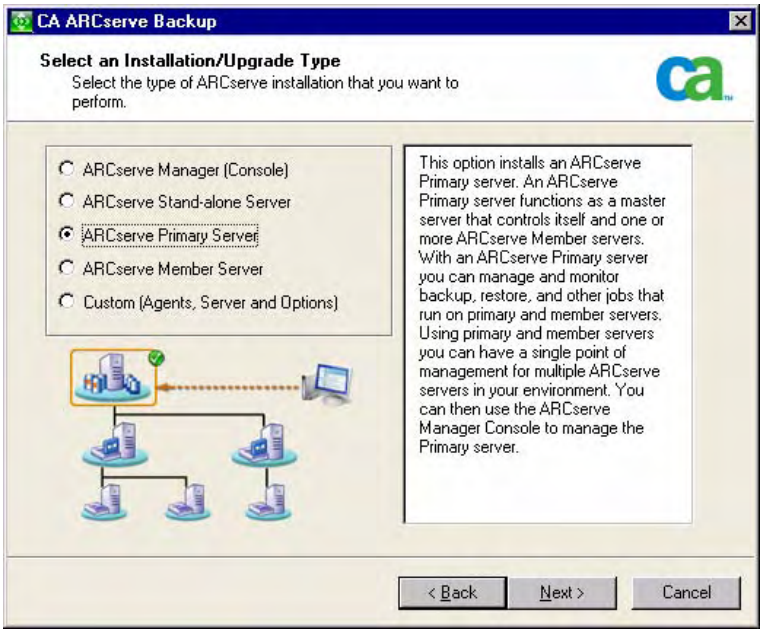


Components You Must Install

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

CA ARCserve Backup Primary Server

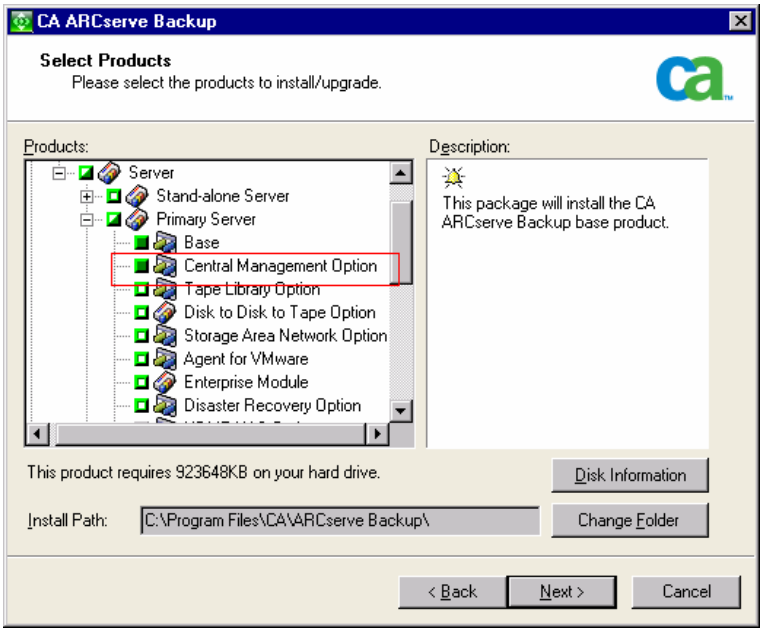
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

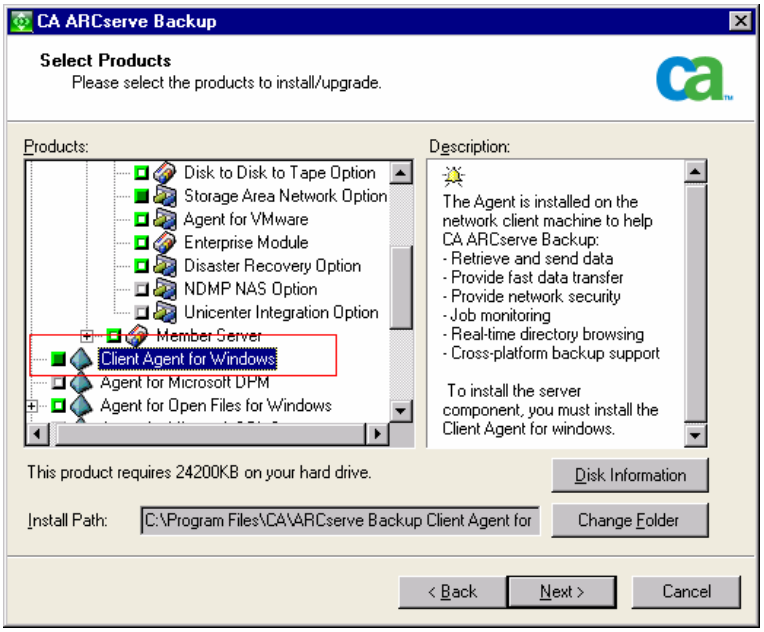
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

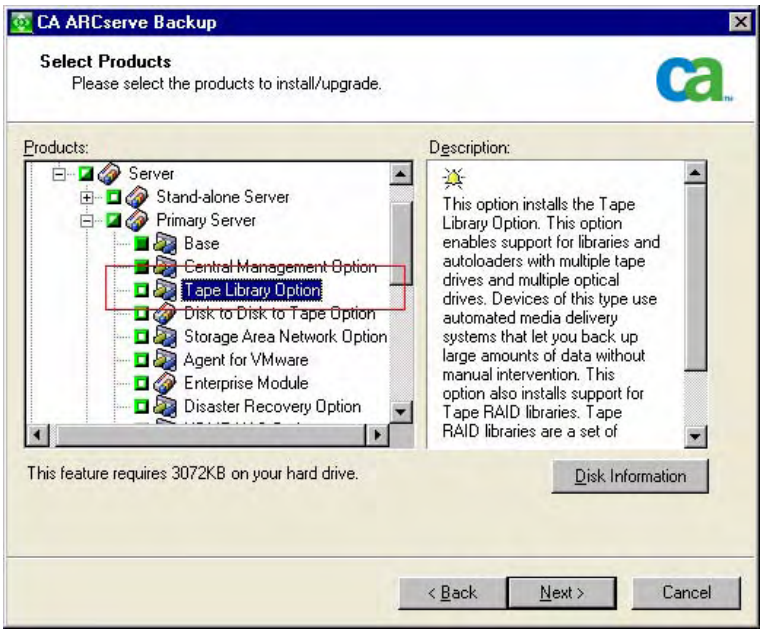
CA ARCserve Backup Client Agent for Windows

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



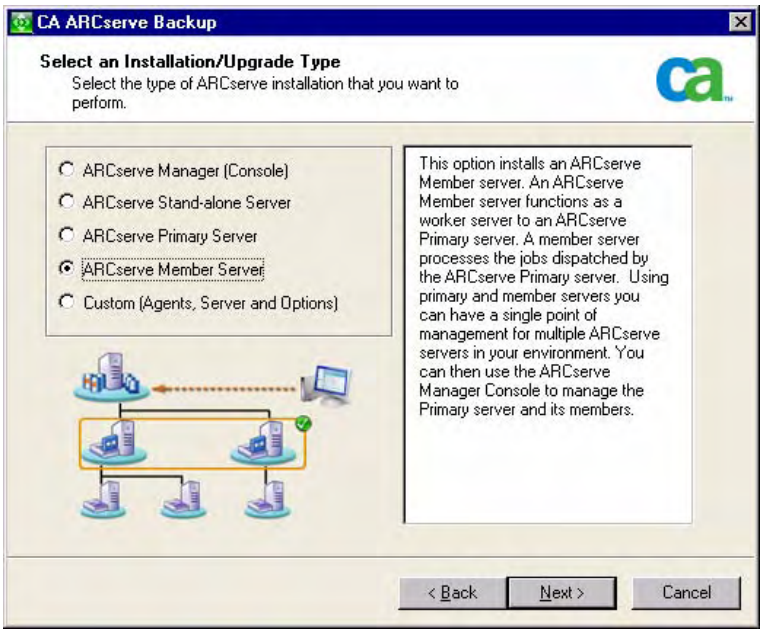
CA ARCserve Backup Tape Library Option

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 an ARCserve 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 members 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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database.

   If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

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 ARCserve 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.

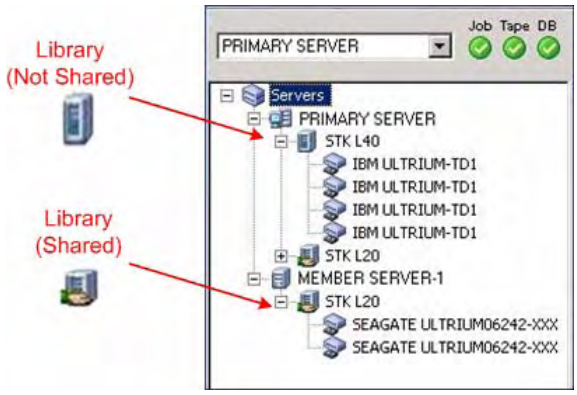
   Ensure that the domain directory tree displays the names of the primary server and all of the member servers in your ARCserve domain.
3. Open the Database Manager and the Job Status Manager.

   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.

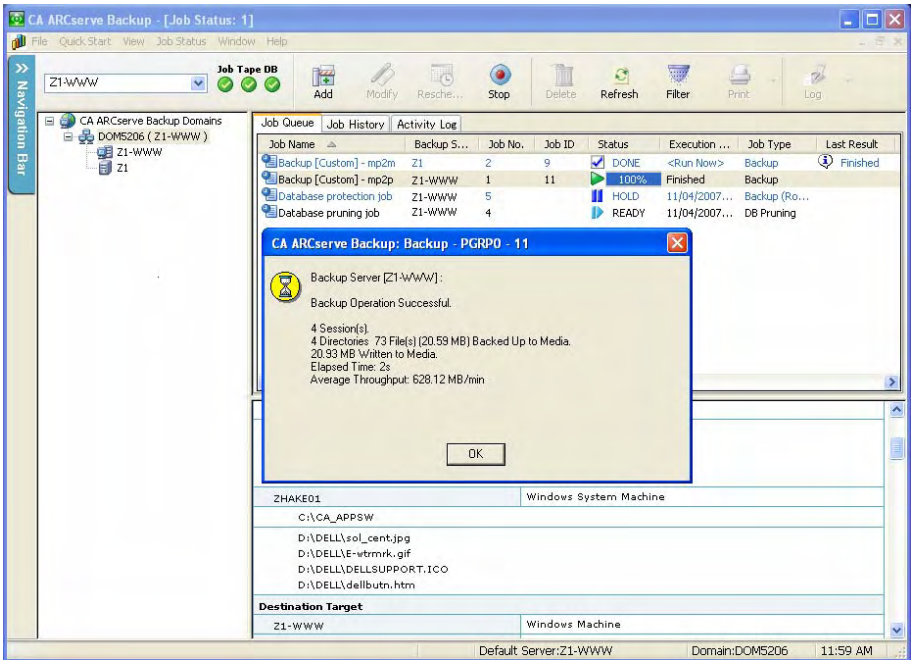
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



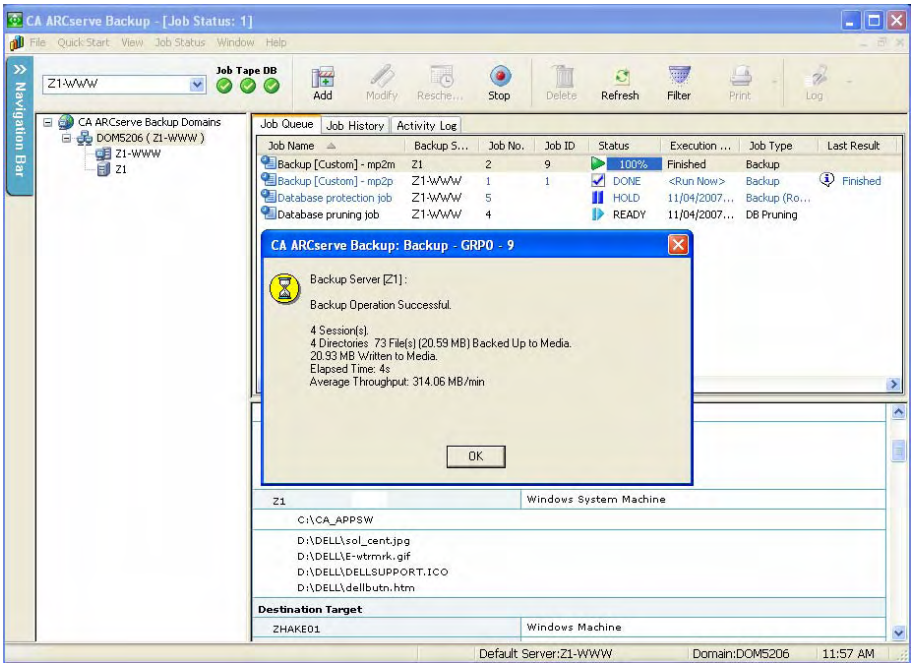
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



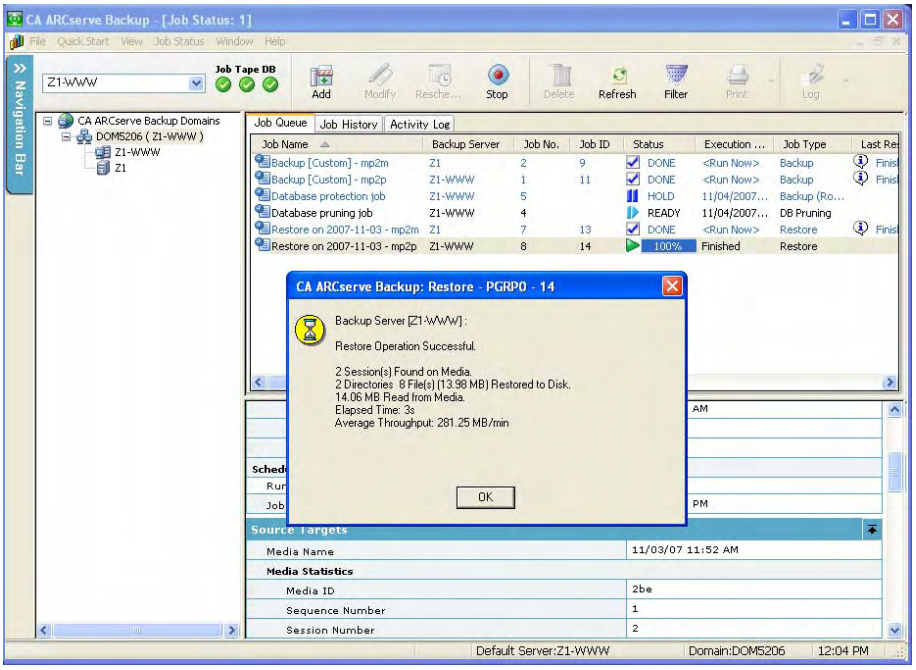
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



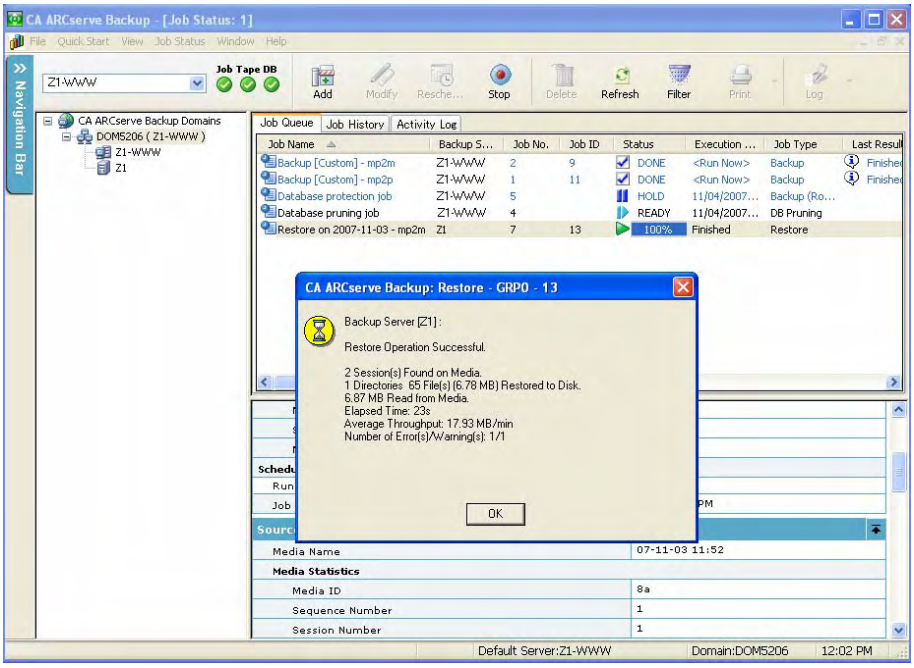
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   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).

Recommended Configuration

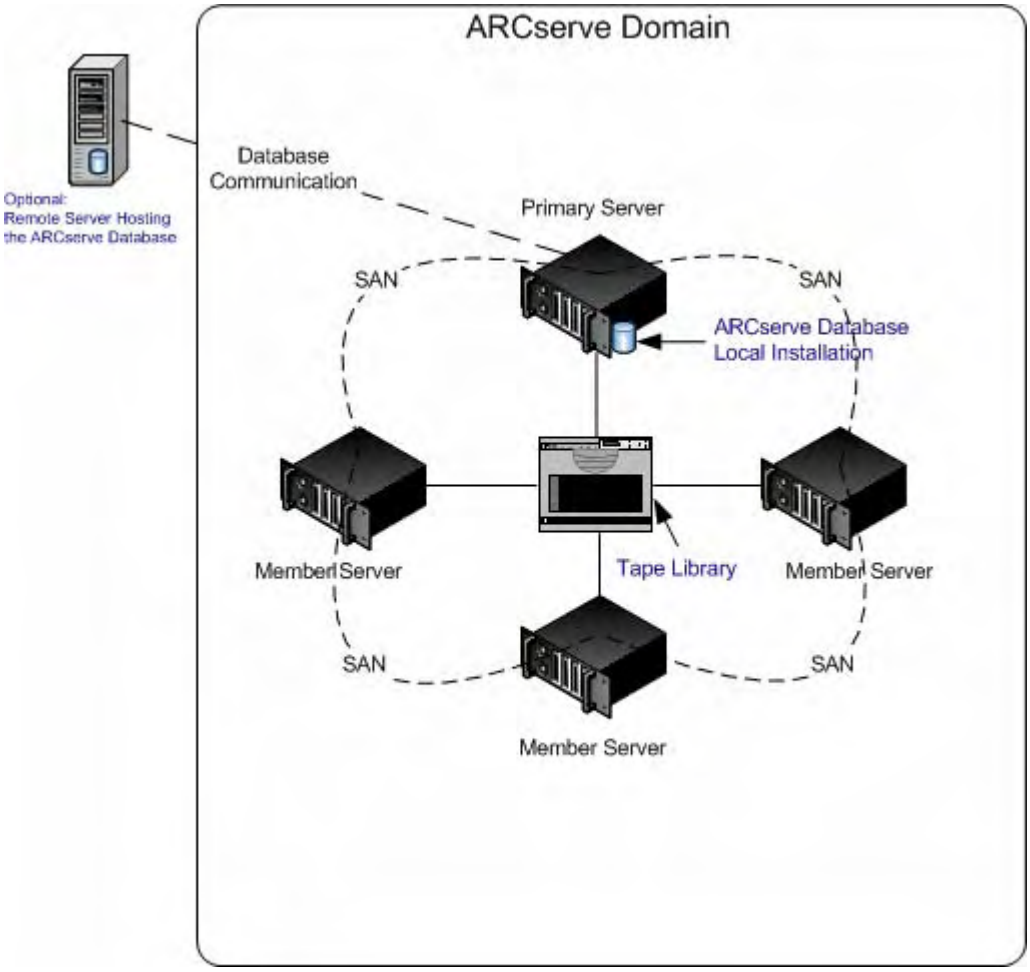
When you require multiple backup servers that reside in the same domain and devices, such as libraries, that are shared in your SAN to protect your environment, the best practice is to install CA ARCserve Backup using the Primary Server and Member Server installation options. With this configuration, 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 ARCserve servers in your environment. You can then use the Manager Console to manage the primary server.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 in a storage area network with shared devices. The environment consists of a primary server and one or more member servers. The ARCserve database is hosted by Microsoft SQL Server 2005 Express Edition and the database instance resides on the primary server.

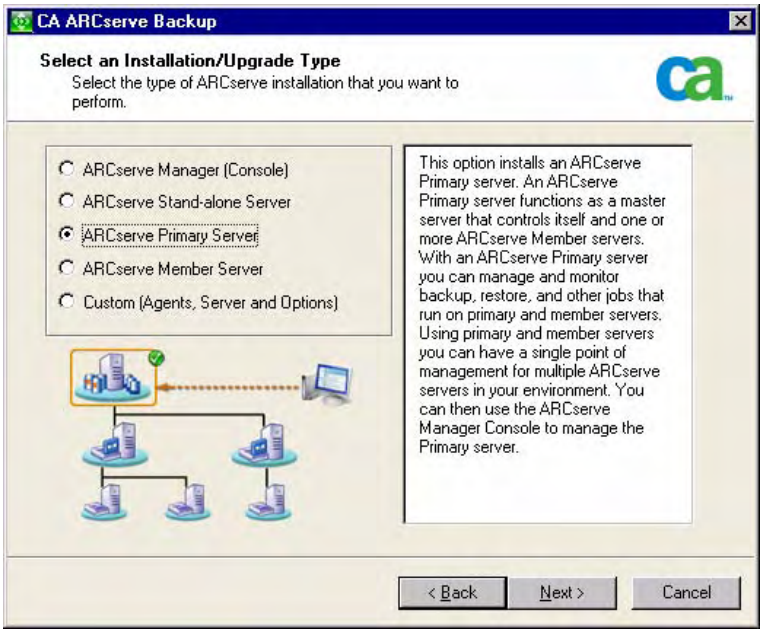


Components You Must Install

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

CA ARCserve Backup Primary Server

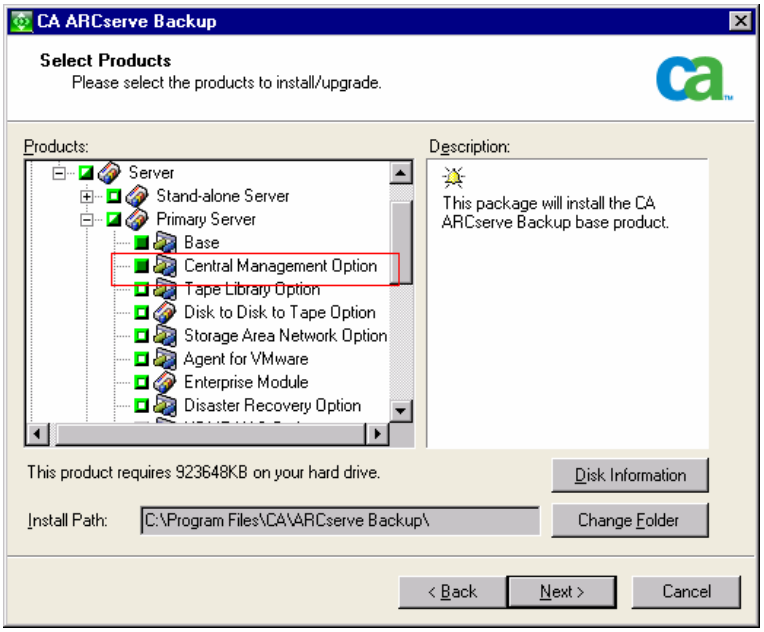
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

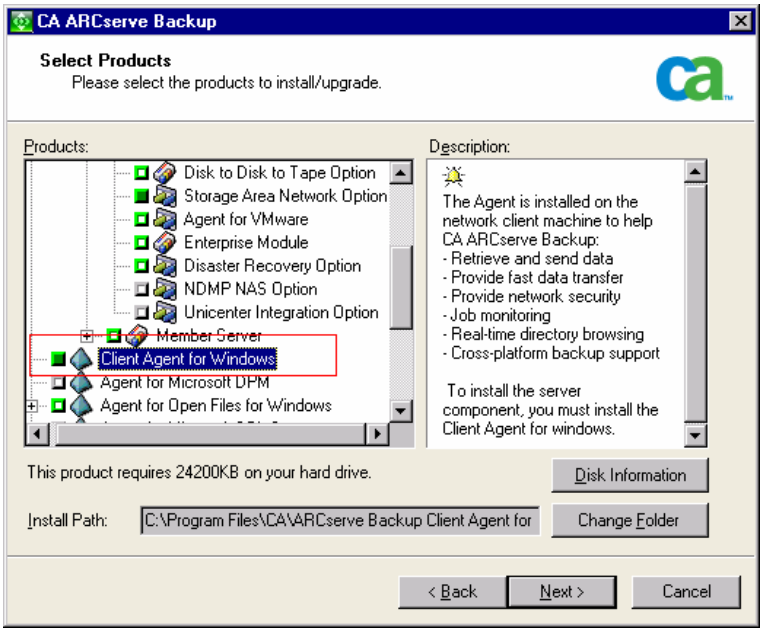
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

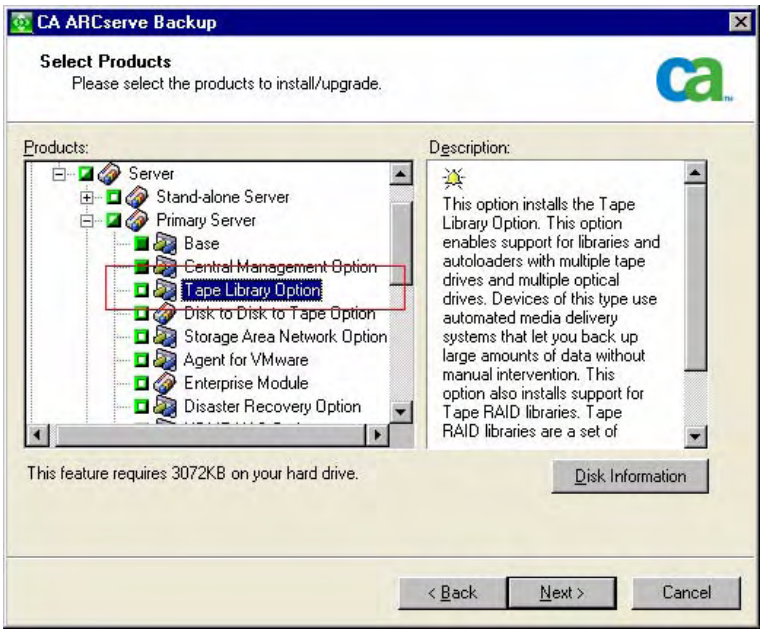
CA ARCserve Backup Client Agent for Windows

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



CA ARCserve Backup Tape Library Option

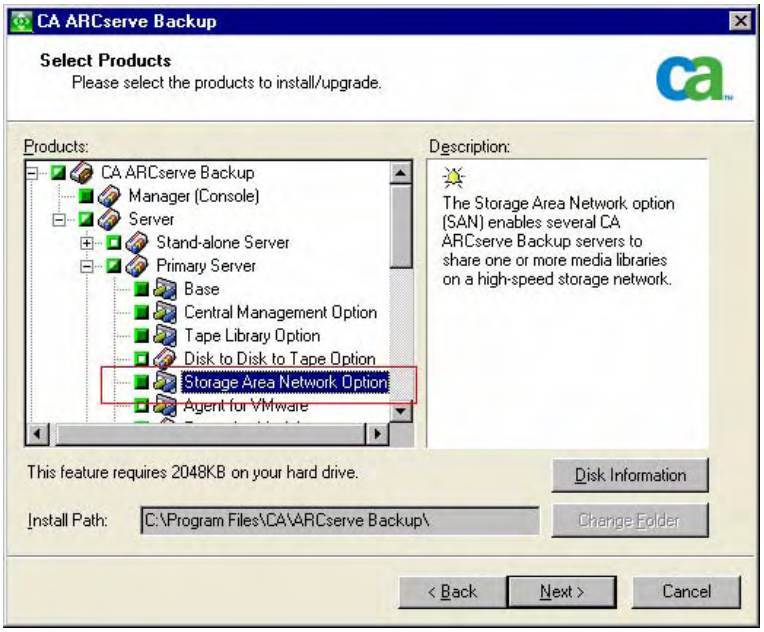
Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.



CA ARCserve Backup Storage Area Network (SAN) Option

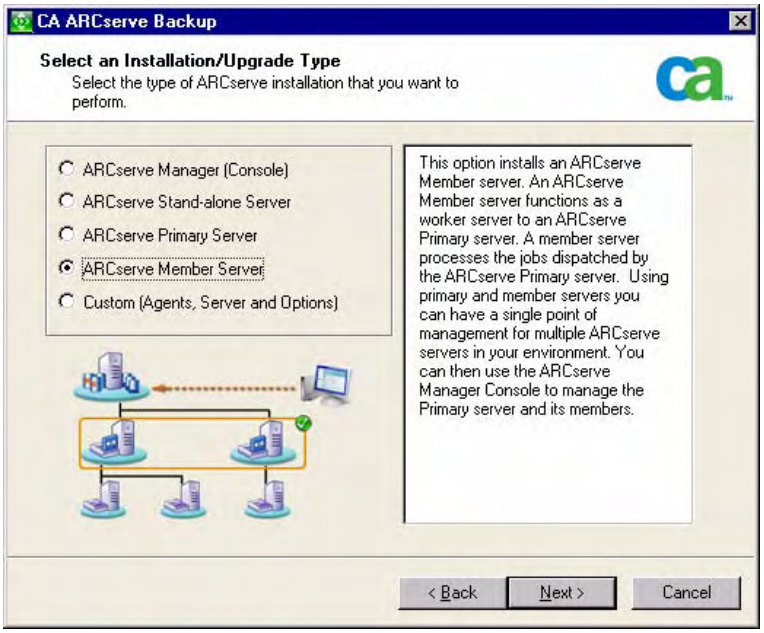
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Note: The Tape Library Option is a prerequisite component for 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.

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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database.

   If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

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 ARCserve 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.

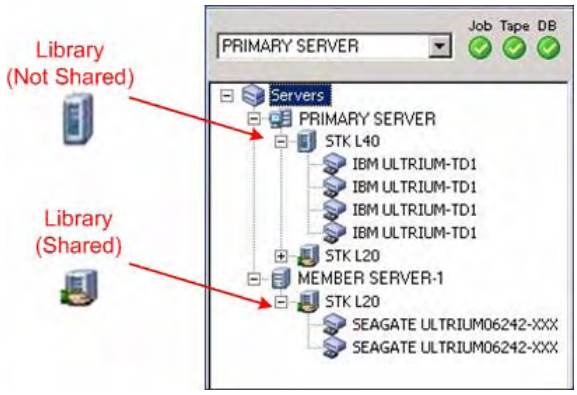
3. Open the Database Manager and the Job Status Manager.

   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.

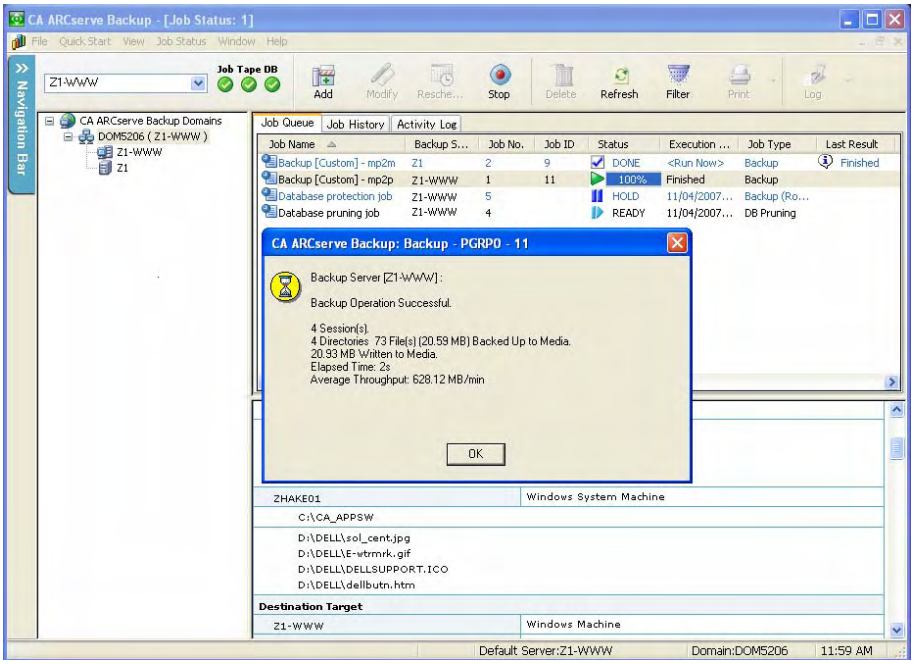
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



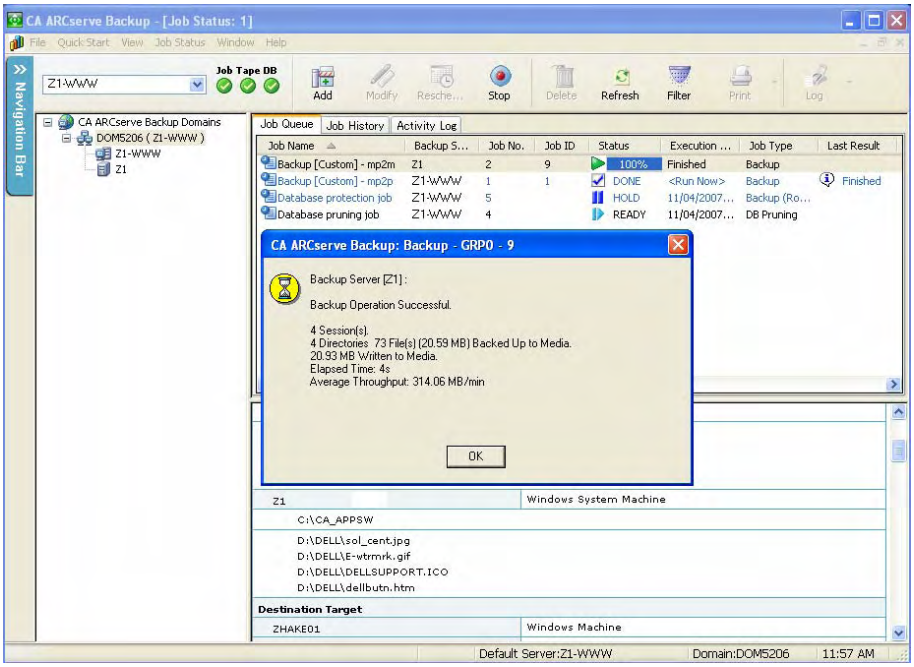
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



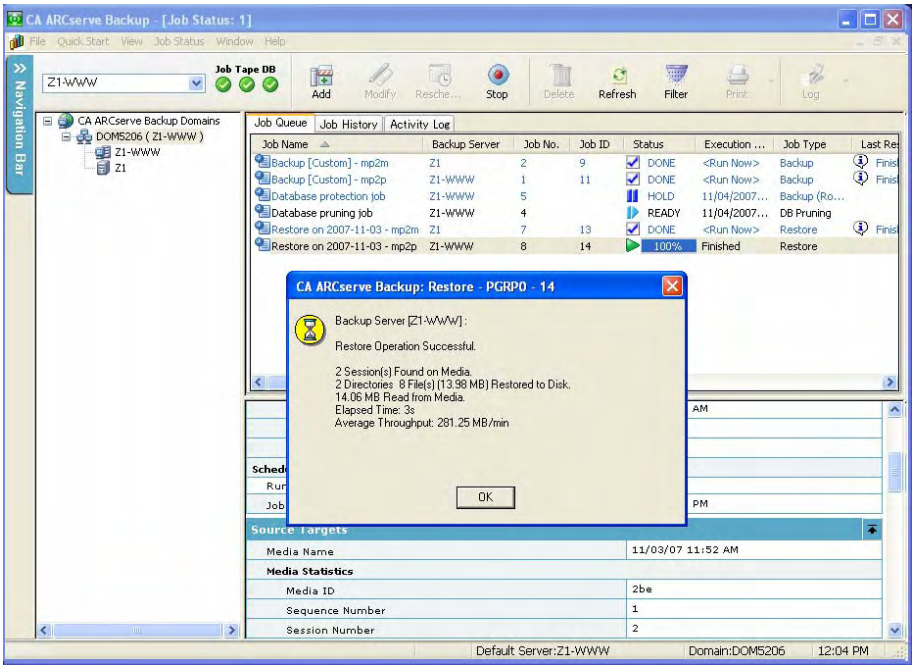
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



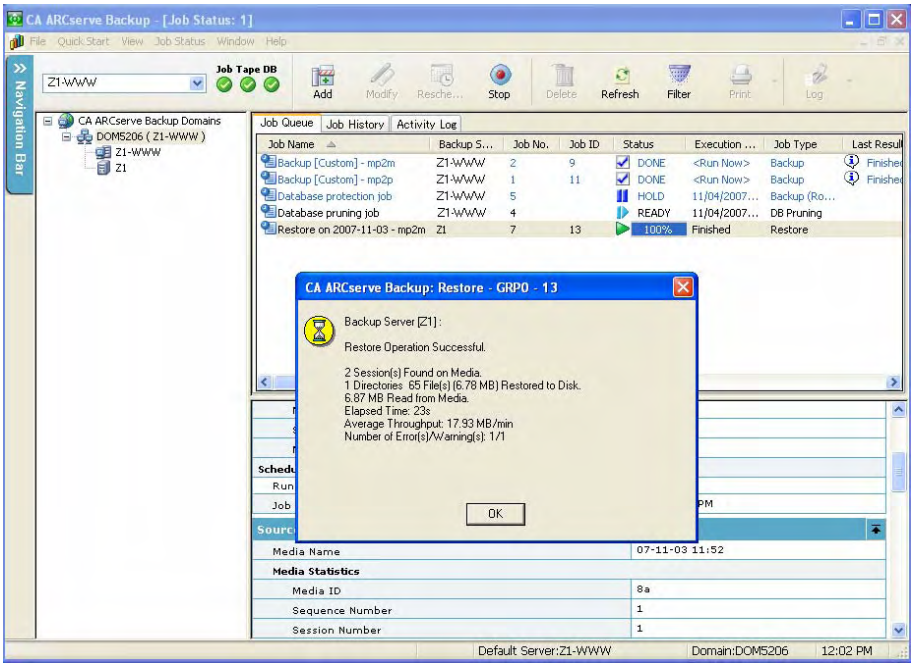
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   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).

Recommended Configuration

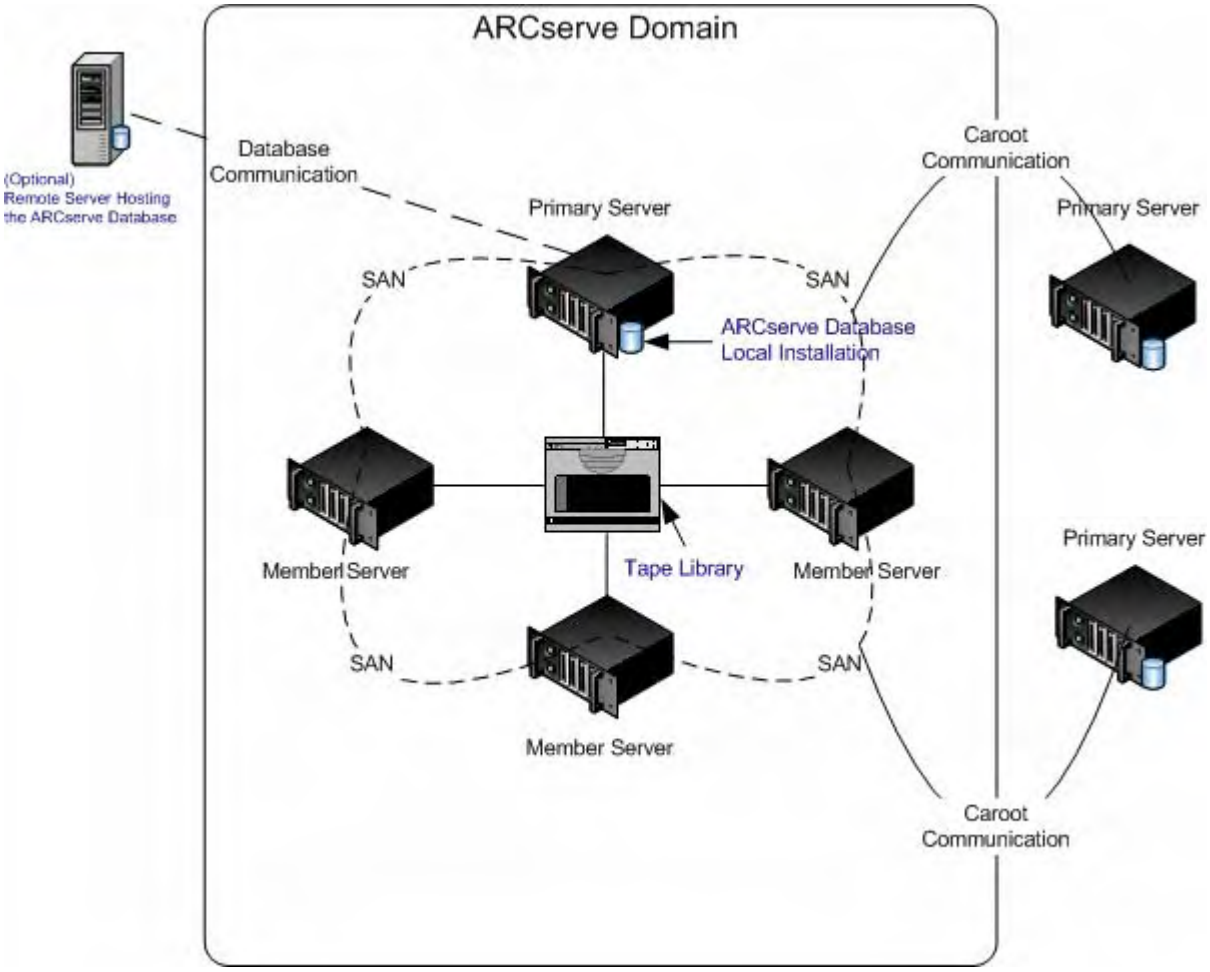
When you require multiple backup servers that reside in the same domain and devices, such as libraries, that are shared in your SAN to protect your environment, the best practice is to install CA ARCserve Backup using the Primary Server and Member Server installation options. With this configuration, 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 ARCserve servers in your environment. You can then use the Manager Console to manage the primary server.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 in a storage area network with shared devices. The environment consists of a primary server and one or more member servers. The ARCserve database is hosted by Microsoft SQL Server 2005 Express Edition and the database instance resides on the primary server.

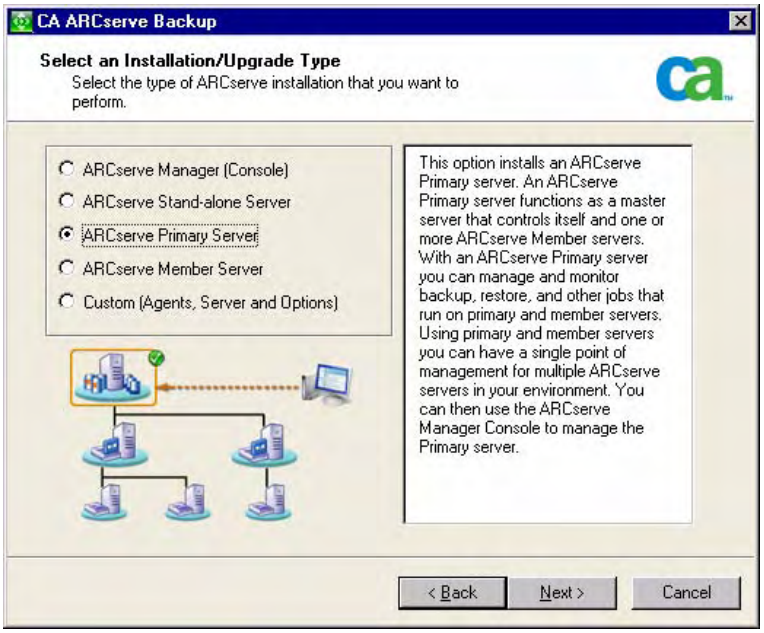


Components You Must Install

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

CA ARCserve Backup Primary Server

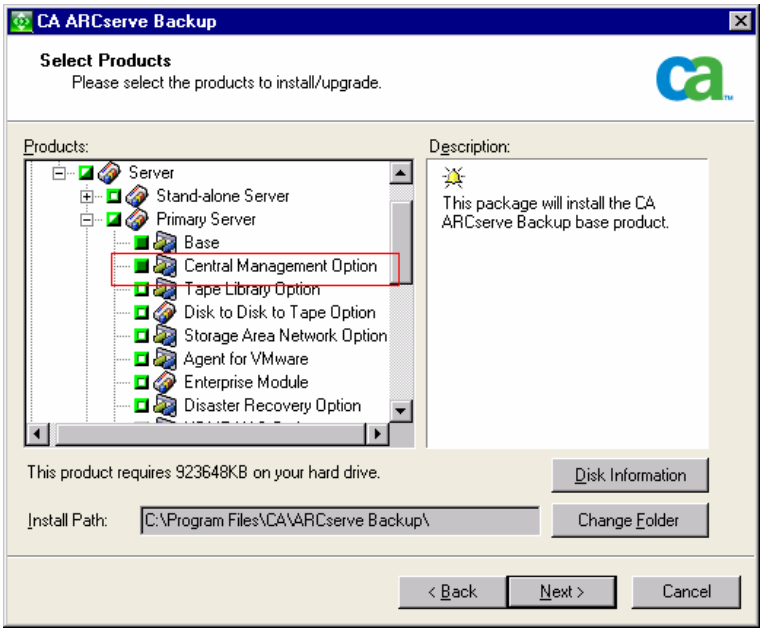
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

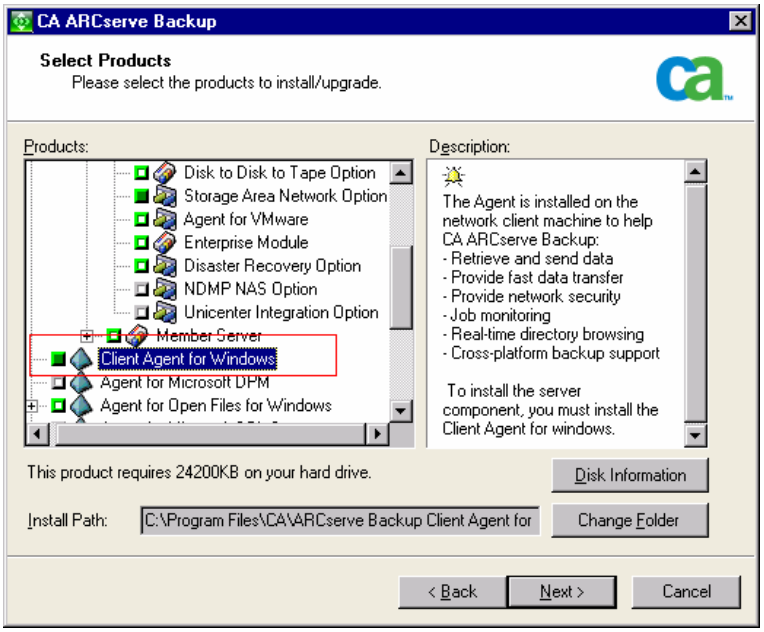
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

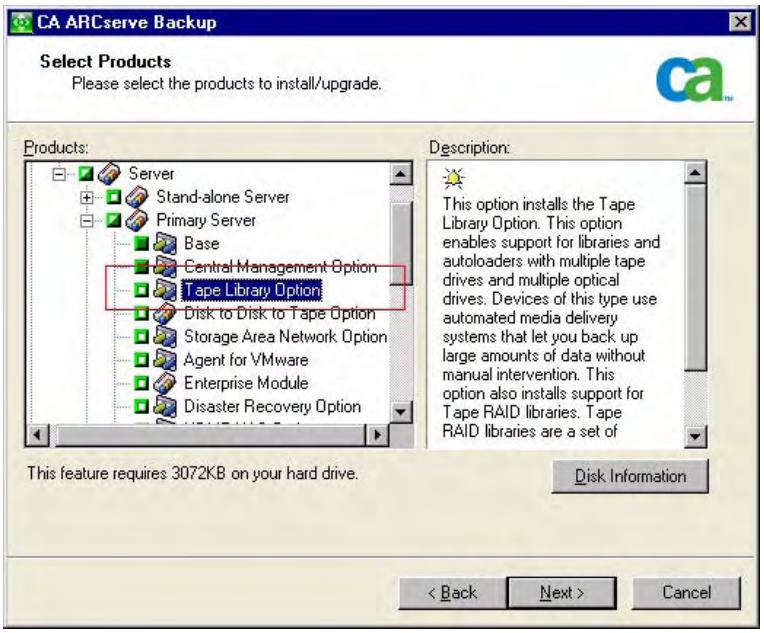
CA ARCserve Backup Client Agent for Windows

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



CA ARCserve Backup Tape Library Option

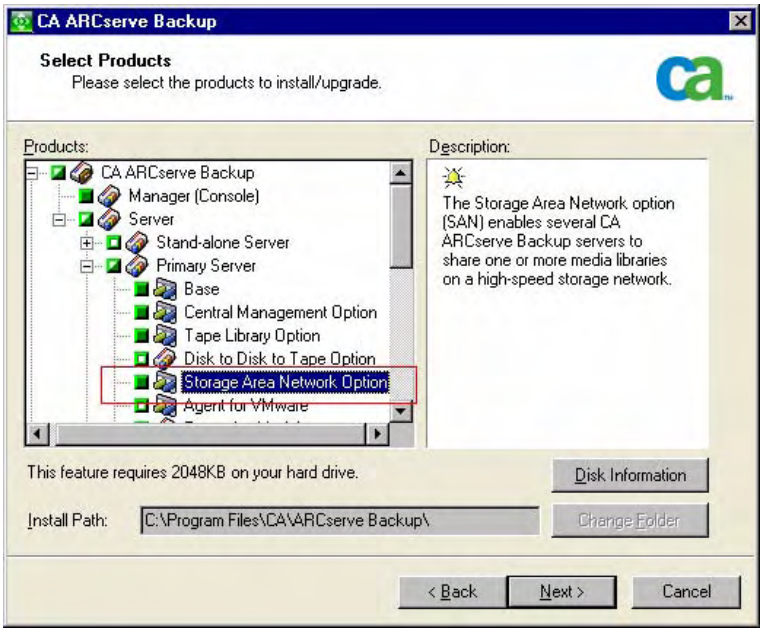
Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.



CA ARCserve Backup Storage Area Network (SAN) Option

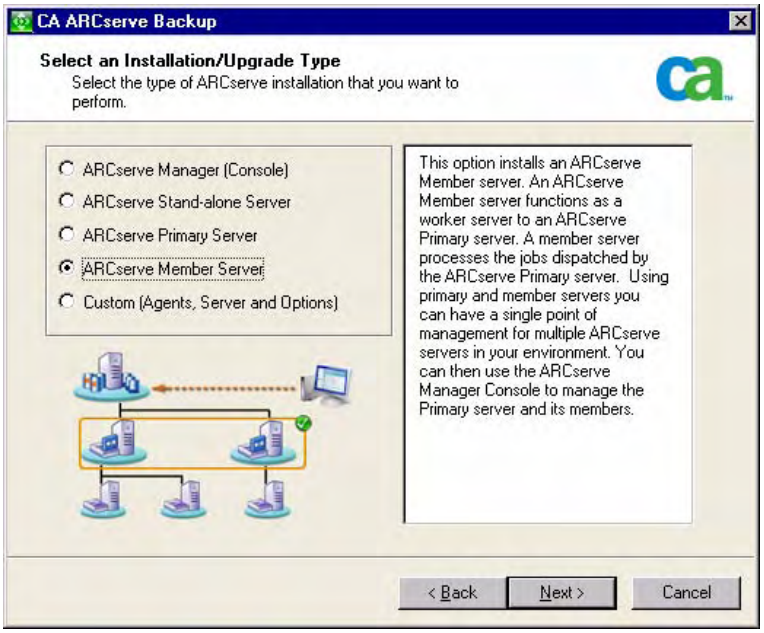
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Note: The Tape Library Option is a prerequisite component for 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.

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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database.

   If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

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:

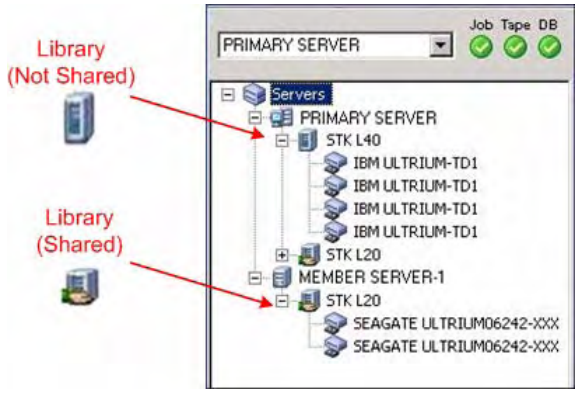
1. Open the CA ARCserve Backup Manager Console on the primary server.
2. Open the Server Admin.

   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.

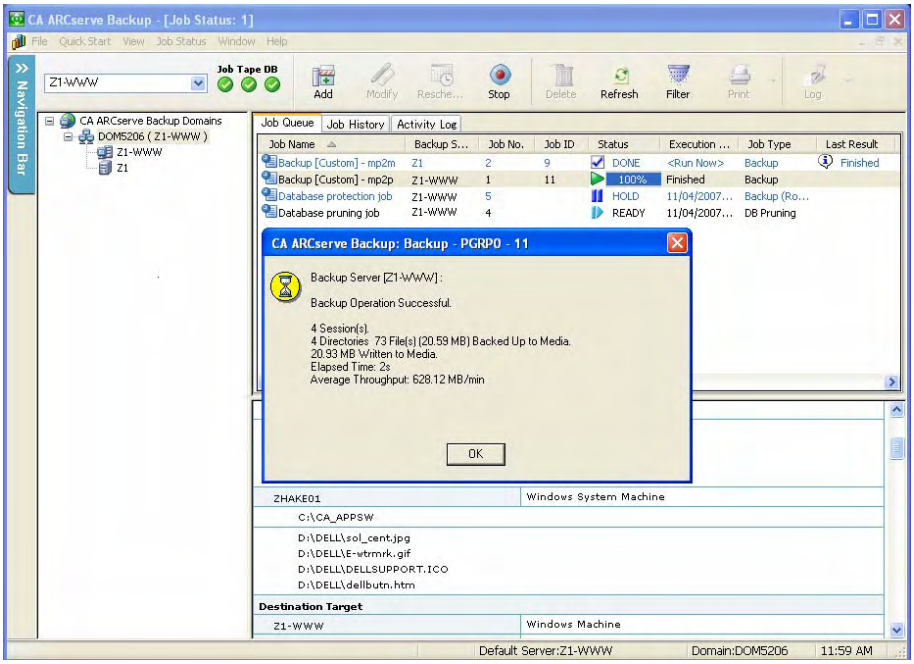
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



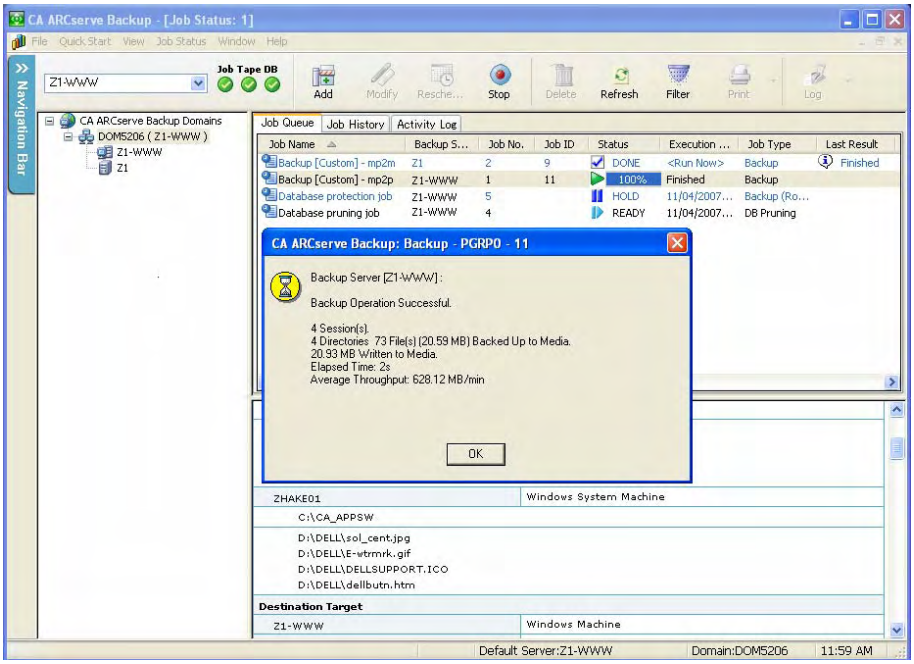
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a primary server:



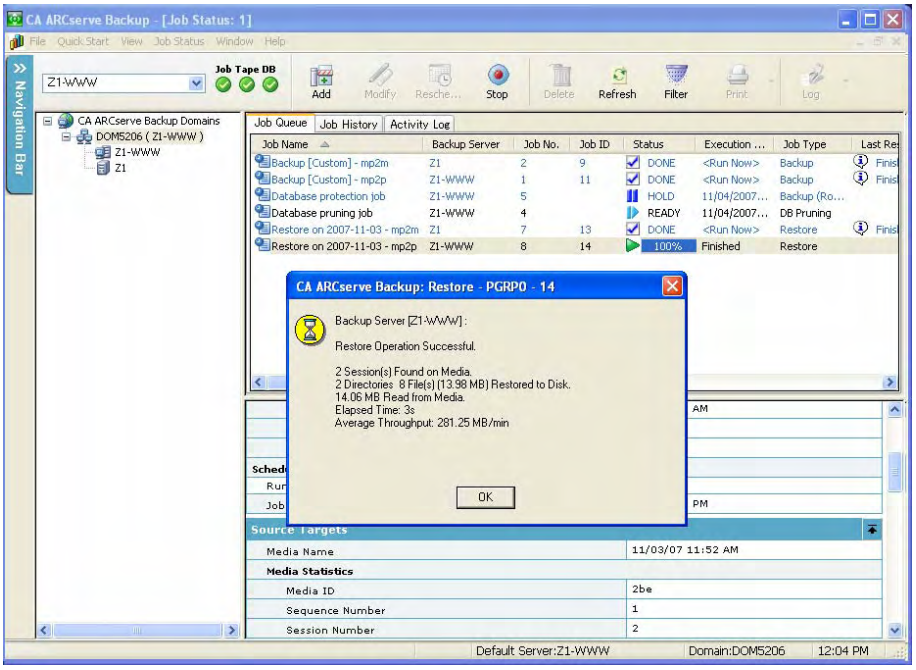
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



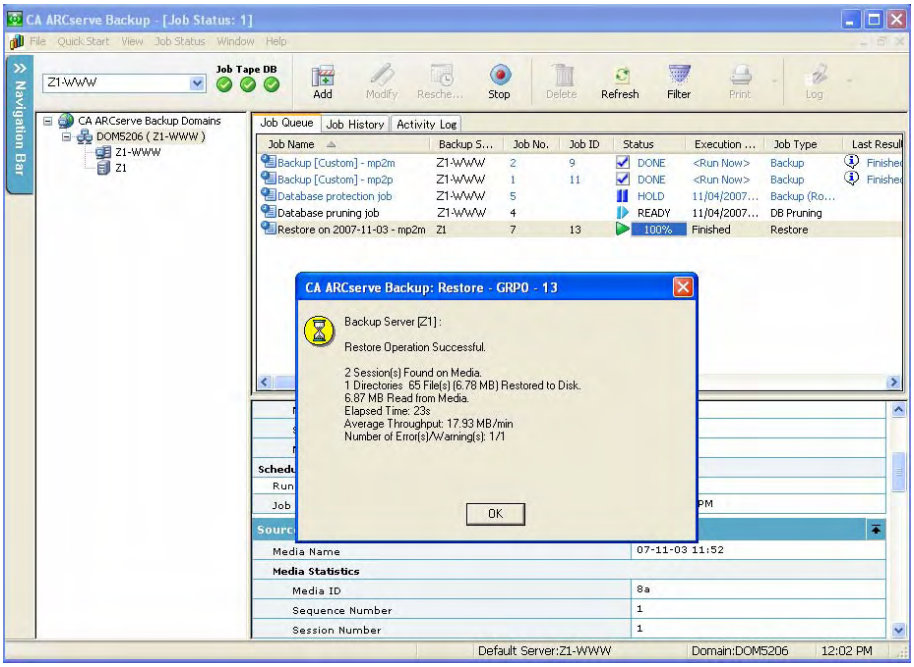
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   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.

Recommended Configuration

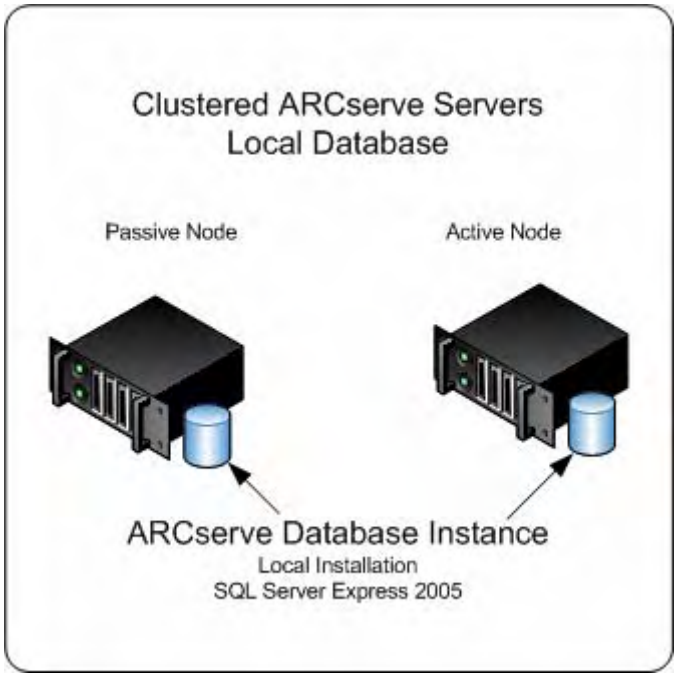
When you require multiple backup servers that reside in the same domain to protect your environment, and the high-availability of a cluster-aware environment, the best practice is to install CA ARCserve Backup using the Primary Server and Member Server installation options into your cluster aware environment. This architecture lets you centrally manage your ARCserve 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 ARCserve servers in your environment. You can then use the Manager Console to manage the primary server.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 2005 Express Edition and the database instance resides on the primary server.

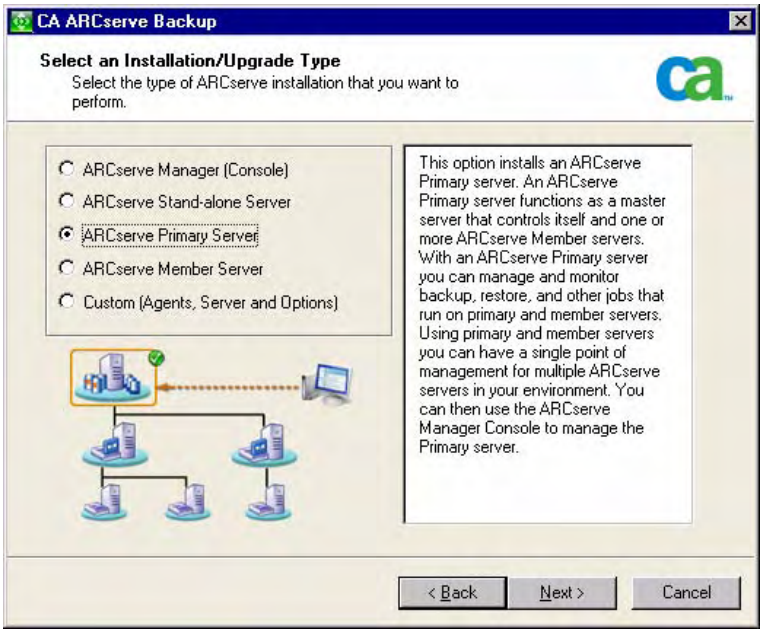


Components You Must Install

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

CA ARCserve Backup Primary Server

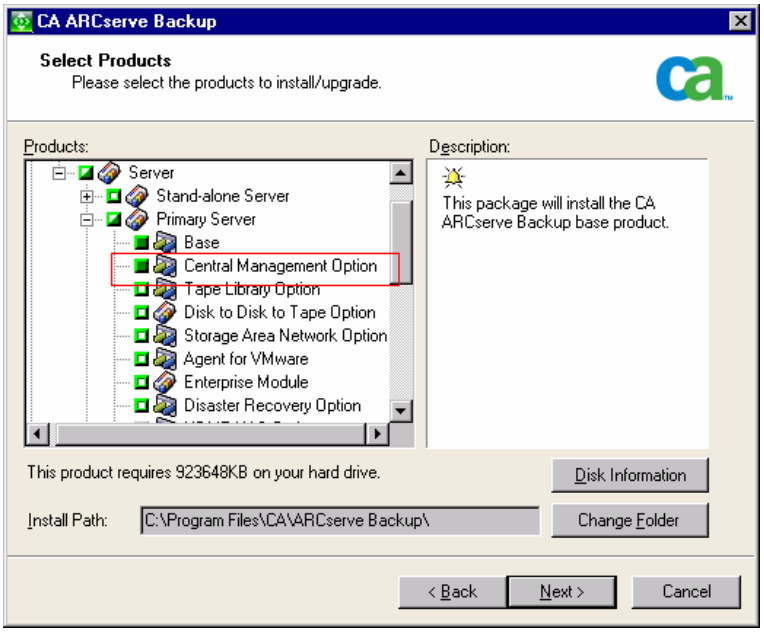
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

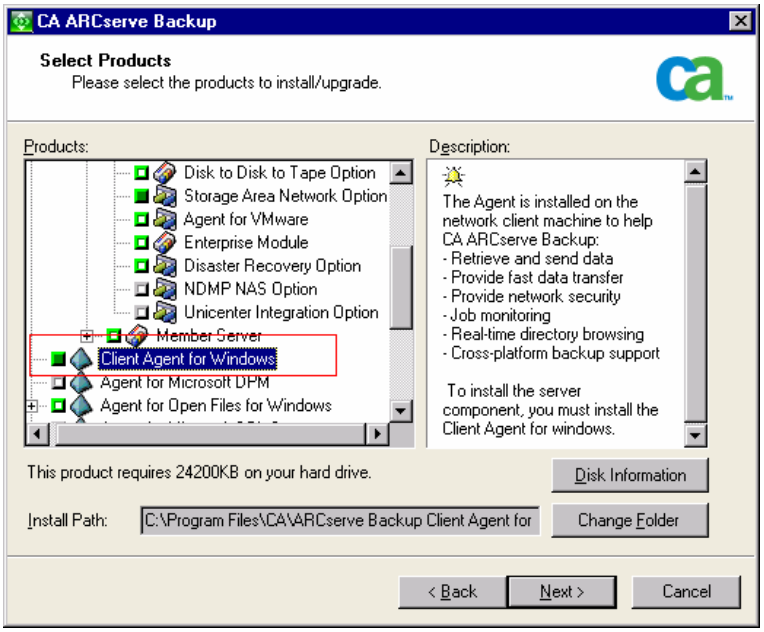
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

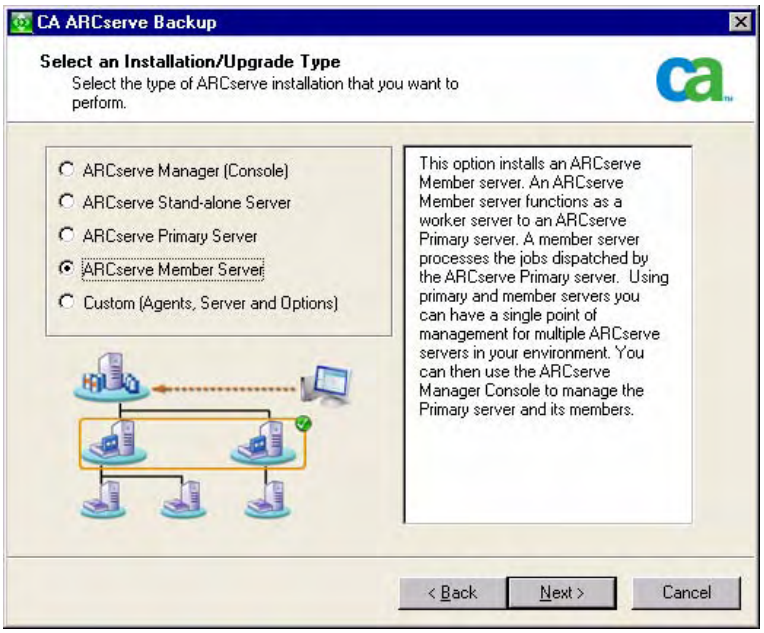
CA ARCserve Backup Client Agent for Windows

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.



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 and NEC ClusterPro/ExpressCluster X 1.0 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 86).
   - For NEC ClusterPro, see Deploy CA ARCserve Backup Server on NEC Cluster (see page 103).
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.

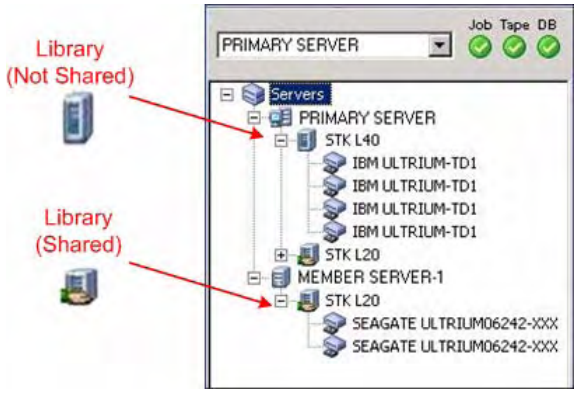
2. Open the Database Manager and the Job Status Manager.

   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.

More information:

Supported Platforms (see page 37)
Supported Devices (see page 37)
Types of CA ARCserve Backup Server Installations (see page 40)
Database Requirements (see page 43)
Post-Installation Tasks (see page 82)

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 50) and Backward Compatibility (see page 51).

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 2005 Express Edition or Microsoft SQL Server. The recommended database application is Microsoft SQL Server 2005 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 2005 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.
- If your new ARCserve environment will consist of an ARCserve domain with a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.
- Microsoft SQL Server 2005 Express Edition is not supported on IA-64 (Intel Itanium) operating systems.
- Microsoft SQL Server 2005 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 43).

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 and Microsoft SQL Server 2005 Express Edition, you can centrally manage up to ten member servers. If you require more than ten member servers, you should host the ARCserve database using Microsoft SQL Server. Additionally, a primary server lets you centrally manage multiple CA ARCserve Backup servers.

  To enable central management capabilities, you must license and install the ARCserve Primary Server option 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 40).

Attached devices

Ensure that all devices, such as libraries, are attached to the ARCserve servers before you start the upgrade process. After the upgrade is complete, the first time the Tape Engine starts, CA ARCserve Backup automatically detects and configures the attached devices; manual configuration is not required.

In-progress jobs

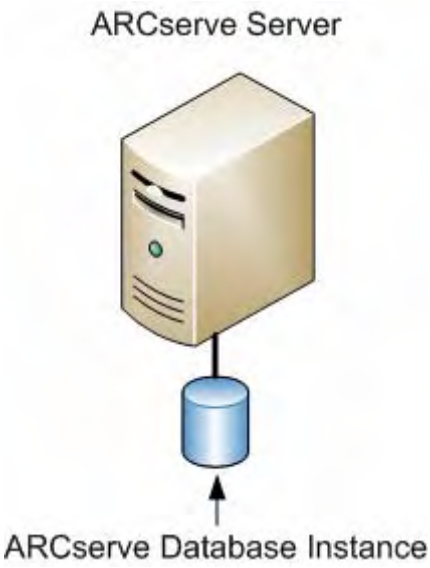
Ensure that all jobs are stopped before you start the upgrade process. CA ARCserve Backup detects all jobs with a Ready Status and places them in a Hold status for you. If there are jobs in progress, CA ARCserve Backup displays a message and the upgrade process pauses until all jobs in progress are complete.

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.

Current Configuration - ARCserve Stand-alone Server

The following diagram illustrates an ARCserve 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.

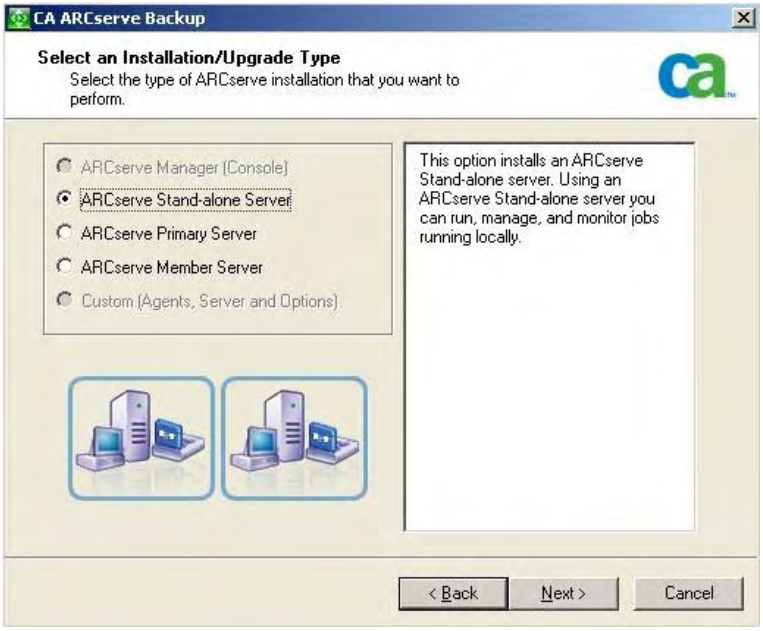
The following diagram illustrates a CA ARCserve Backup Primary Server or a CA ARCserve Backup Stand-alone Server.

New Components You Must Install

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

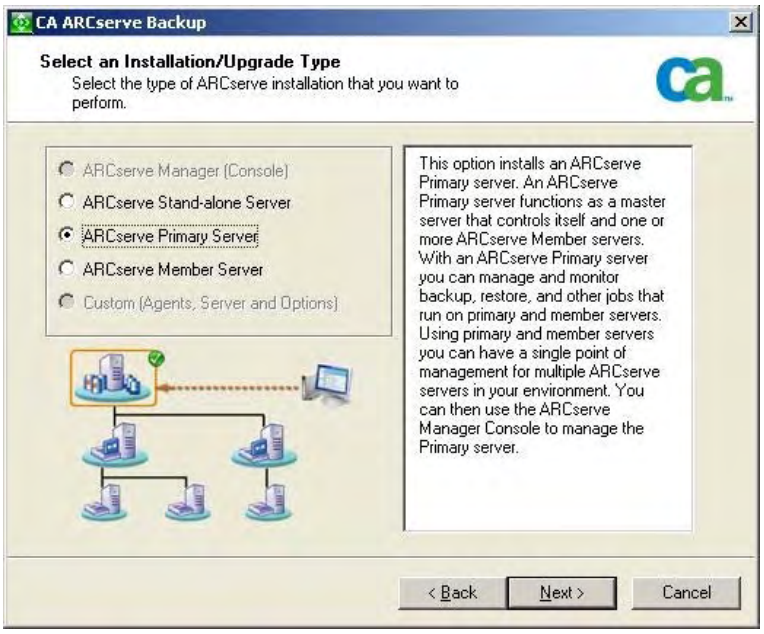
CA ARCserve Backup Stand-alone Server

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.



CA ARCserve Backup Agent for Microsoft SQL Server

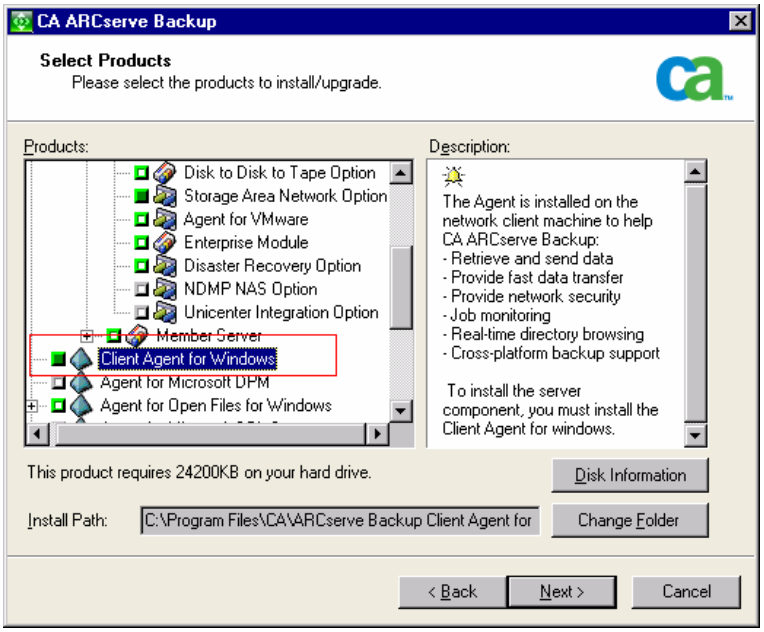
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard 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.

More information:

Upgrade Considerations (see page 50)
Upgrade CA ARCserve Backup from a Previous Release (see page 66)

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.

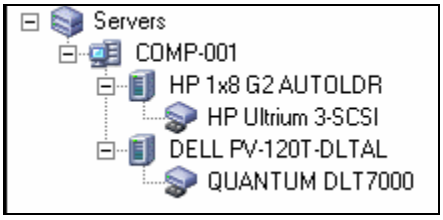
   Ensure that all previous backup data migrated successfully.

   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.

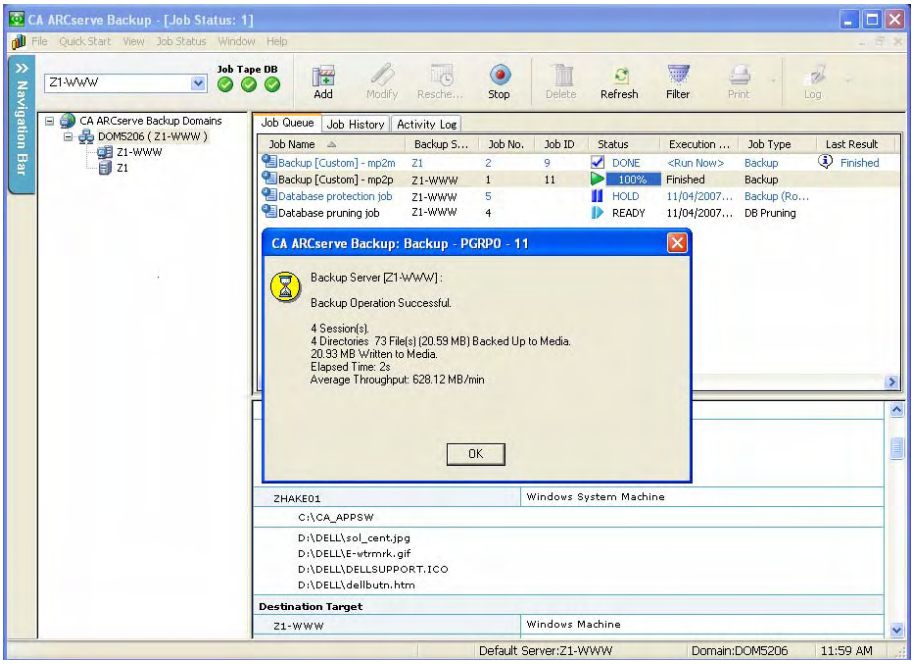
   Note: For information about configuring devices, see the online help or the *Administration Guide*.

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.

   The following diagram illustrates a successful backup job:



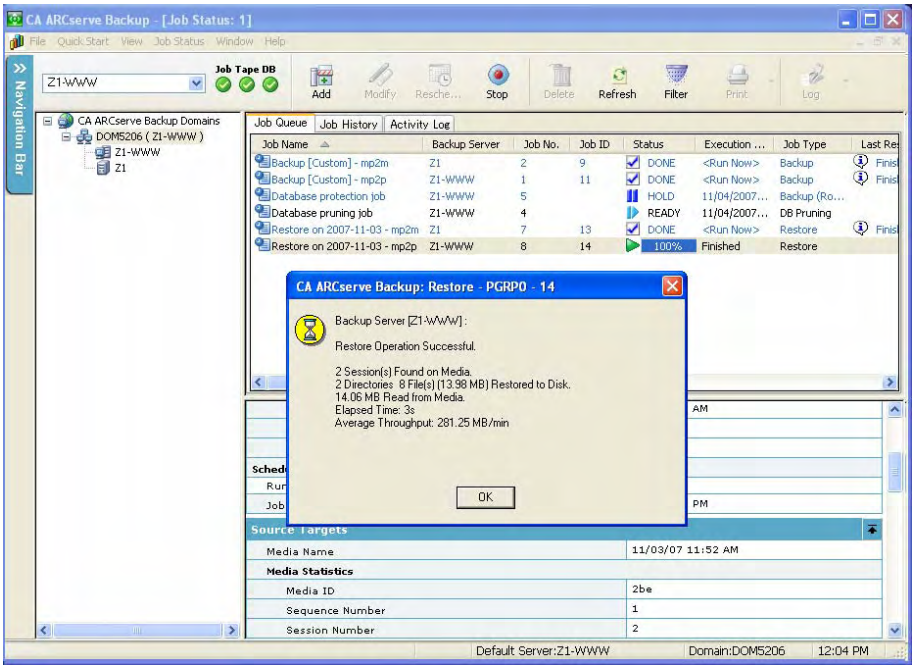
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following diagram illustrates a successful restore job:



   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.

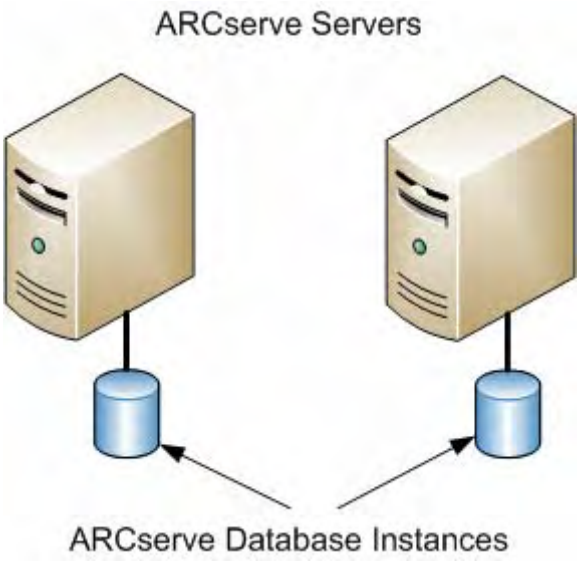
   Ensure the Job Queue tab and Activity Log display information about the jobs.

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.

Current Configuration - Multiple ARCserve Servers in a Domain

The following diagram illustrates multiple ARCserve 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 ARCserve servers in a domain, the best practice is to upgrade to a centralized management environment that consists of a primary server and one or more member servers.

To upgrade to a centralized management environment, you must upgrade one of your existing ARCserve 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.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 a centralized management environment:

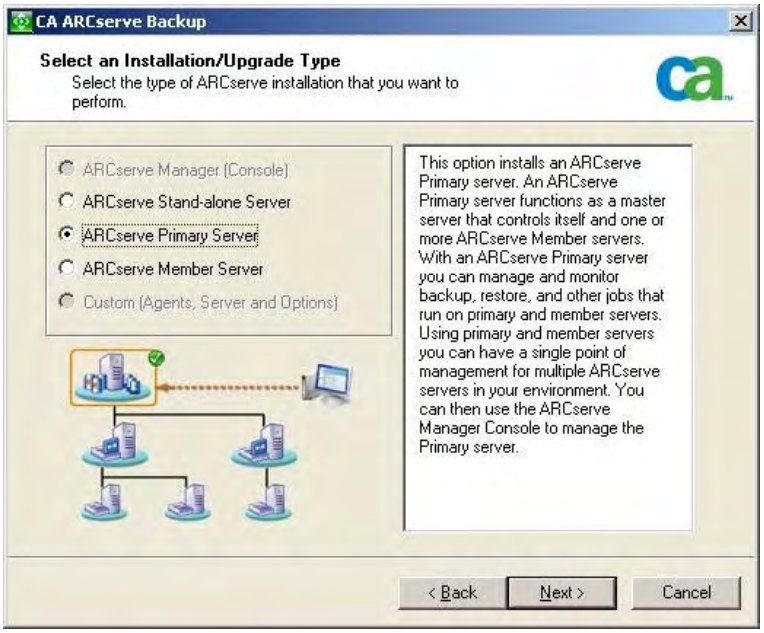
Note: To enable CA ARCserve Backup to communicate with a remote database, you must use Microsoft SQL Server to host the ARCserve database.

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

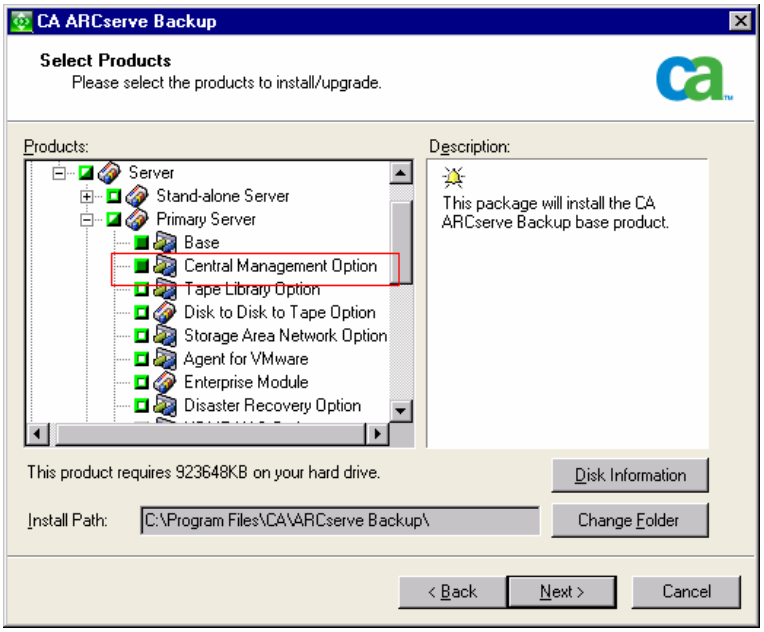
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

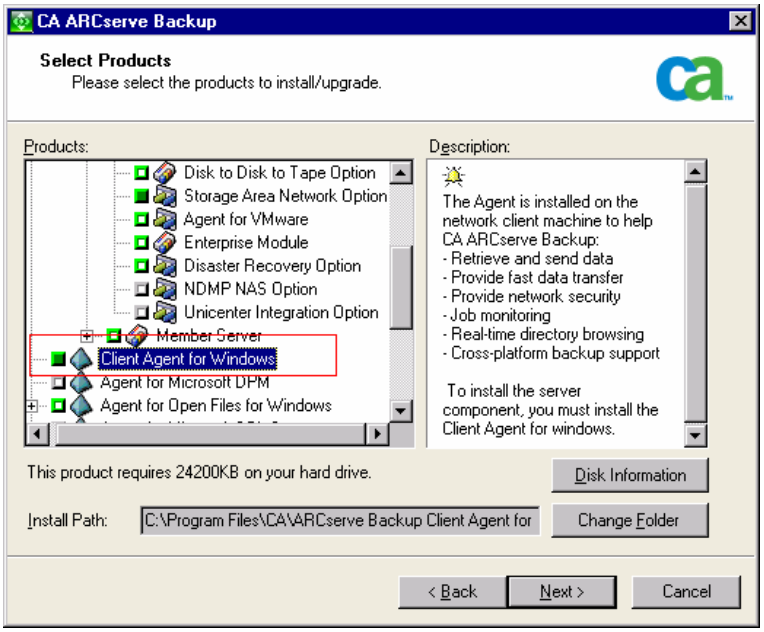
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

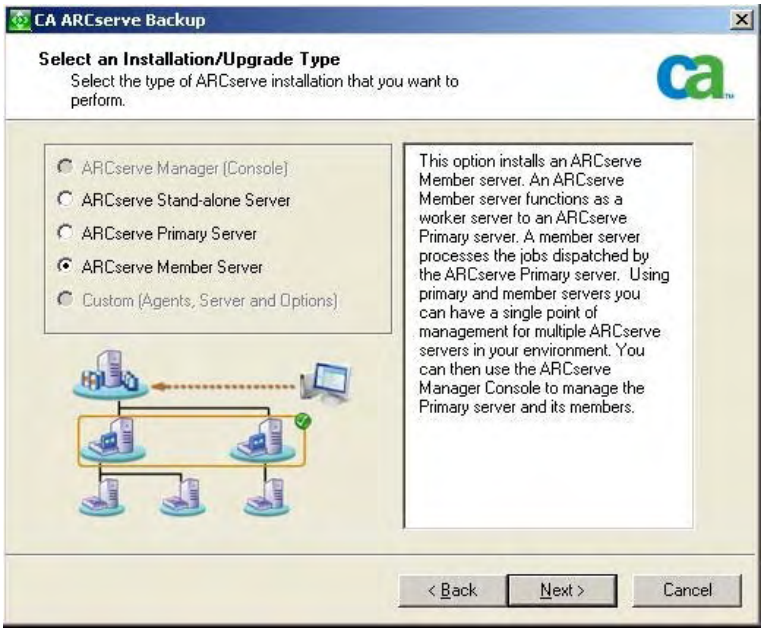
CA ARCserve Backup Client Agent for Windows

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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database. If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

   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.

More information:

Upgrade Considerations (see page 50)
Upgrade CA ARCserve Backup from a Previous Release (see page 66)

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.

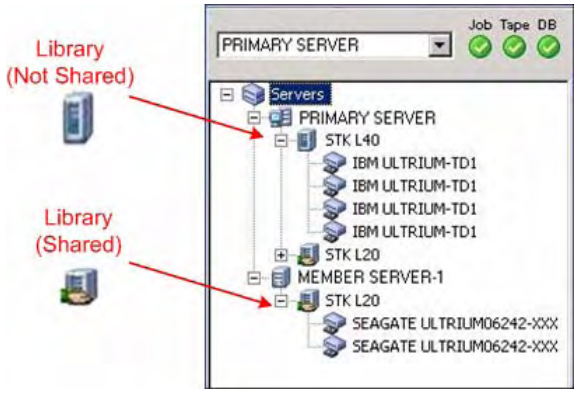
   Ensure that all previous backup data migrated successfully.

   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.

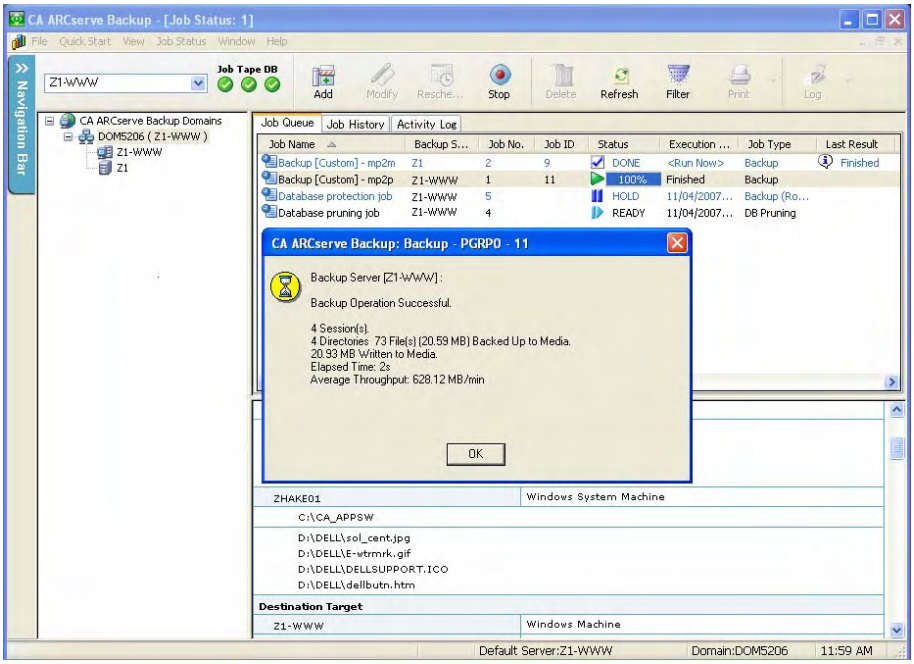
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



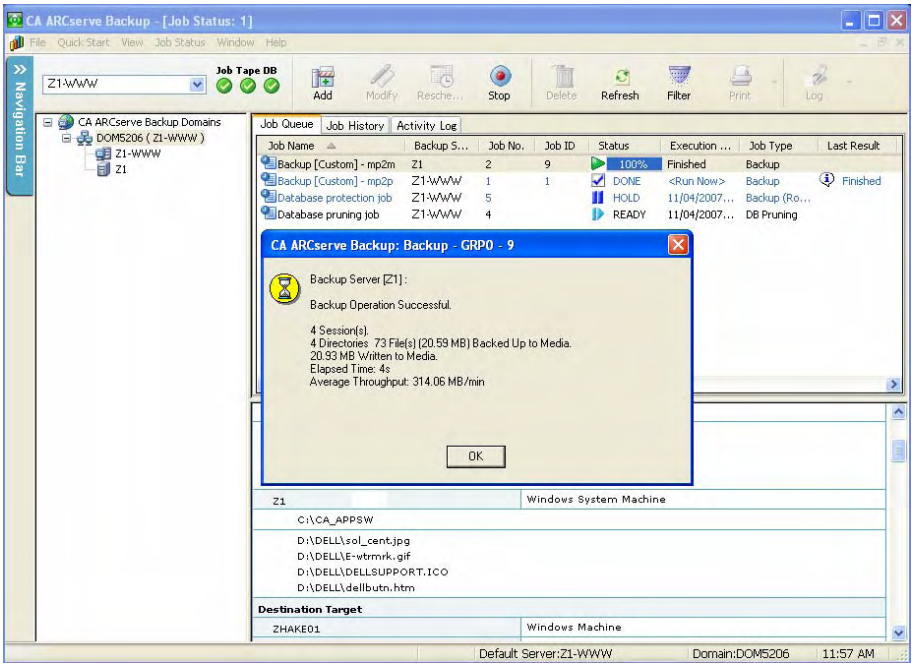
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



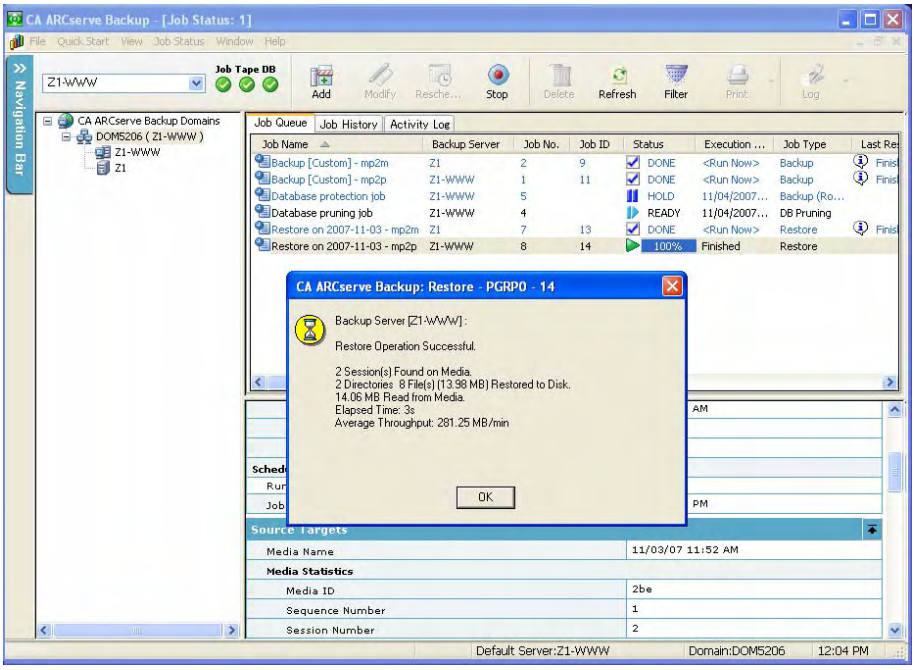
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



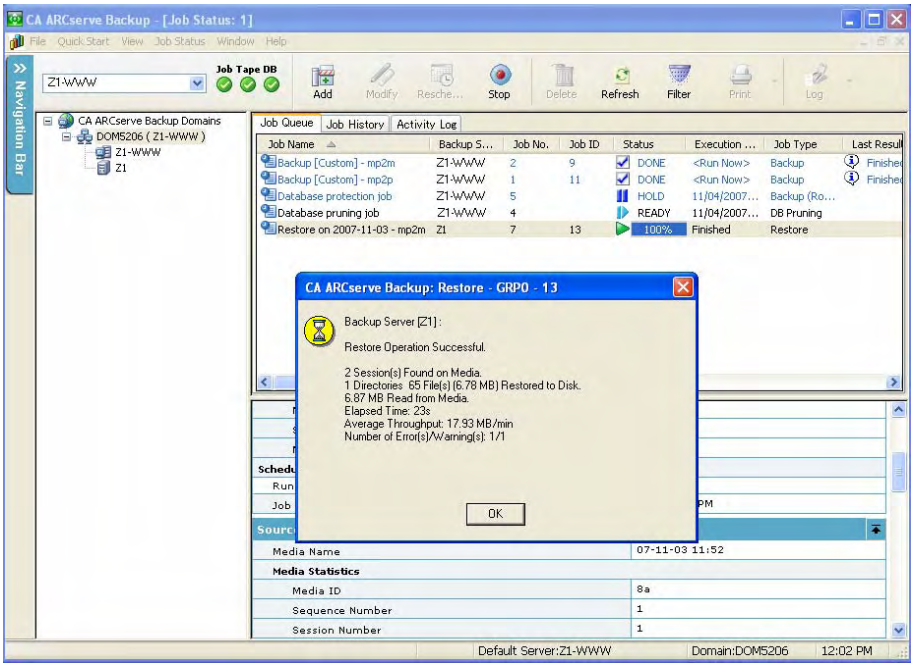
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   If the job fails, perform the following troubleshooting tasks:

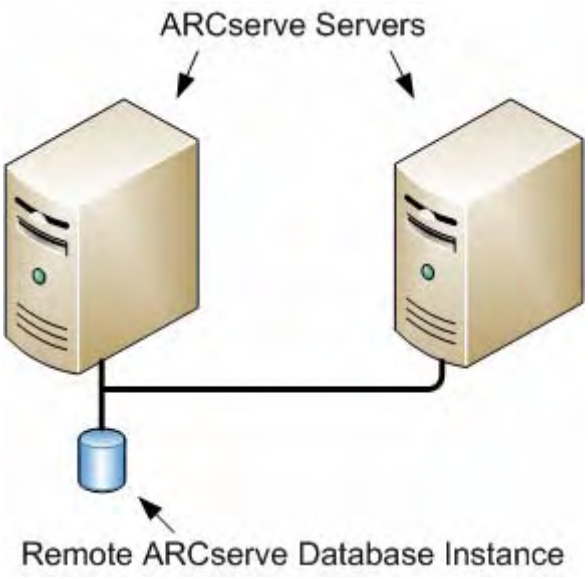
   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit 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.

Current Configuration - Multiple ARCserve Servers Sharing a Remote Database

The following diagram illustrates multiple ARCserve 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 ARCserve 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 an ARCserve 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.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 a centralized management environment:

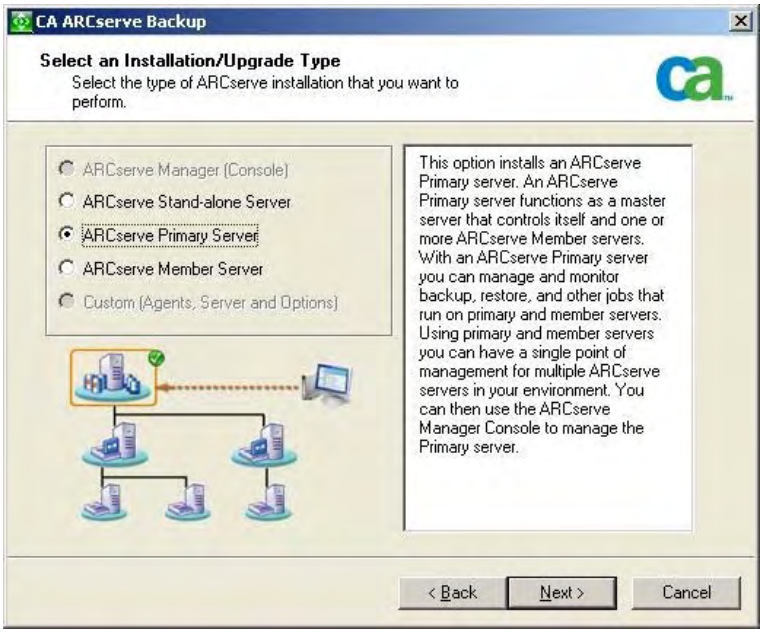
Note: To enable CA ARCserve Backup to communicate with a remote database, you must use Microsoft SQL Server to host the CA ARCserve Backup database instance.

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

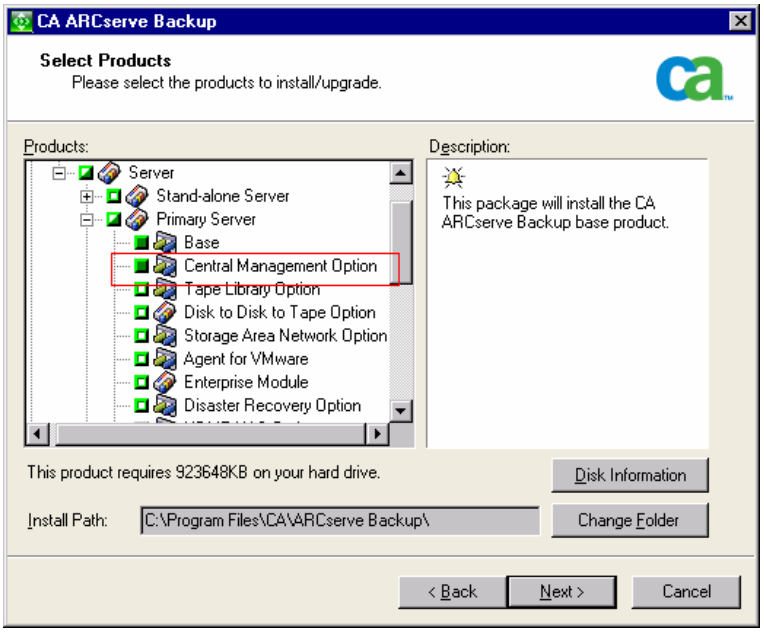
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

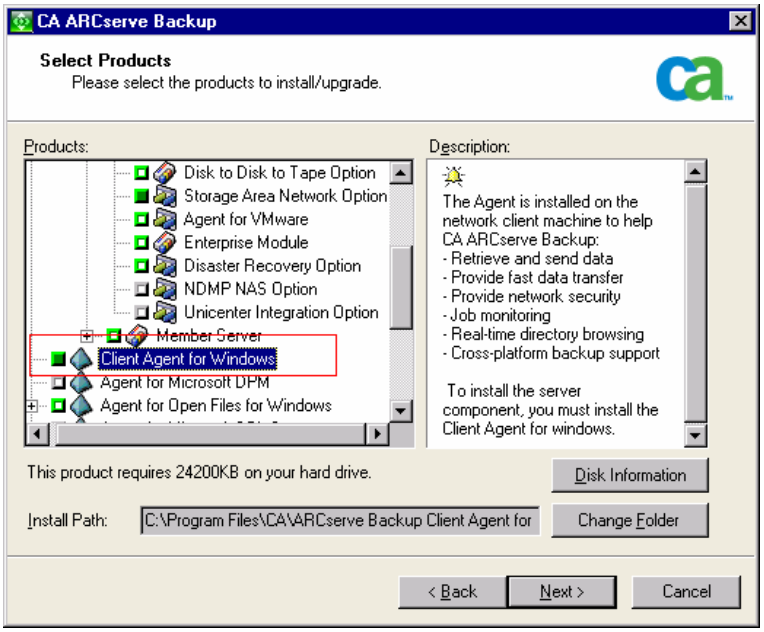
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

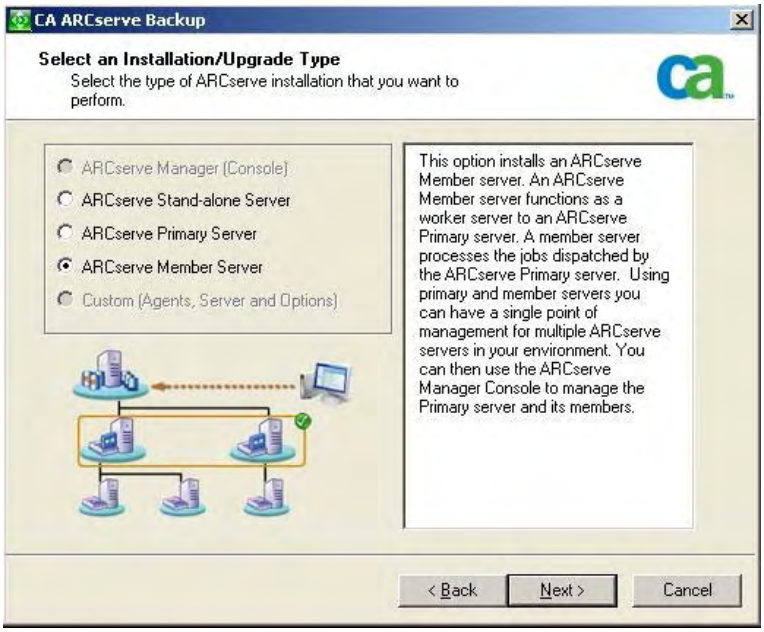
CA ARCserve Backup Client Agent for Windows

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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database. If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

   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.

More information:

Upgrade Considerations (see page 50)
Upgrade CA ARCserve Backup from a Previous Release (see page 66)

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.

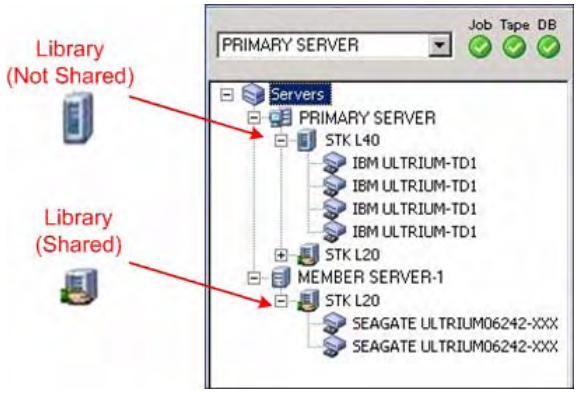
   Ensure that all previous backup data migrated successfully.

   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.

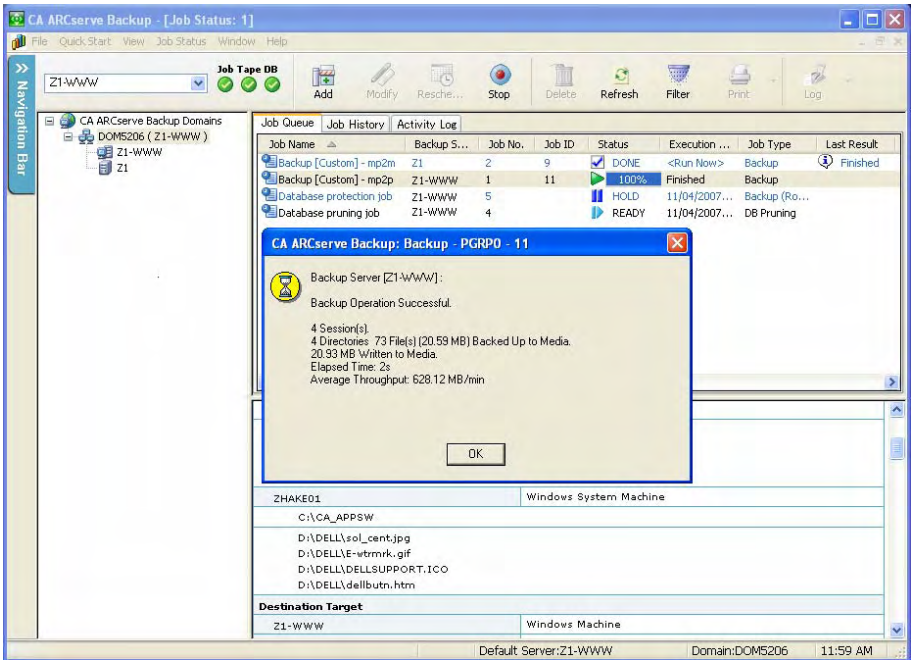
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



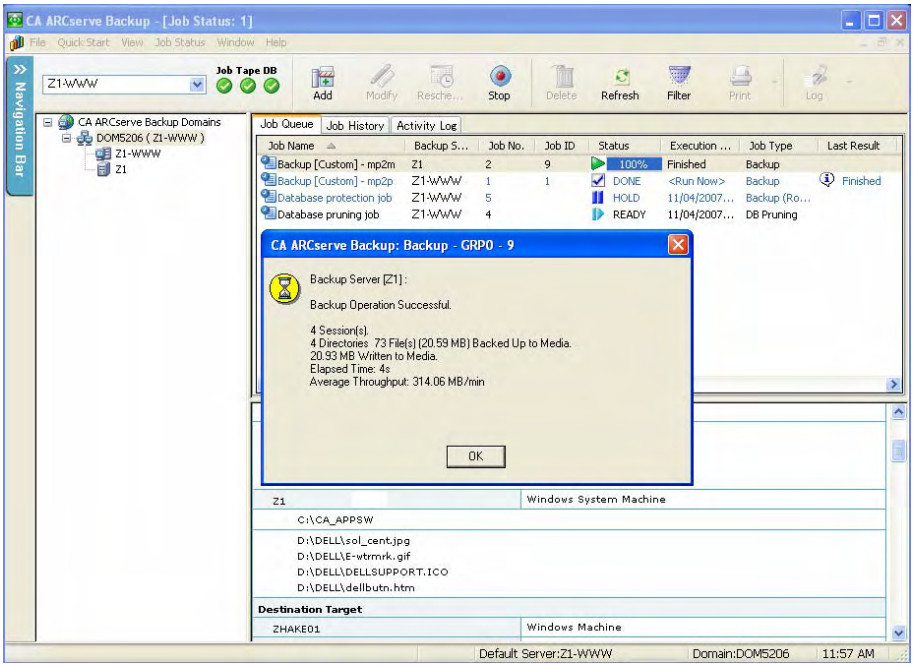
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



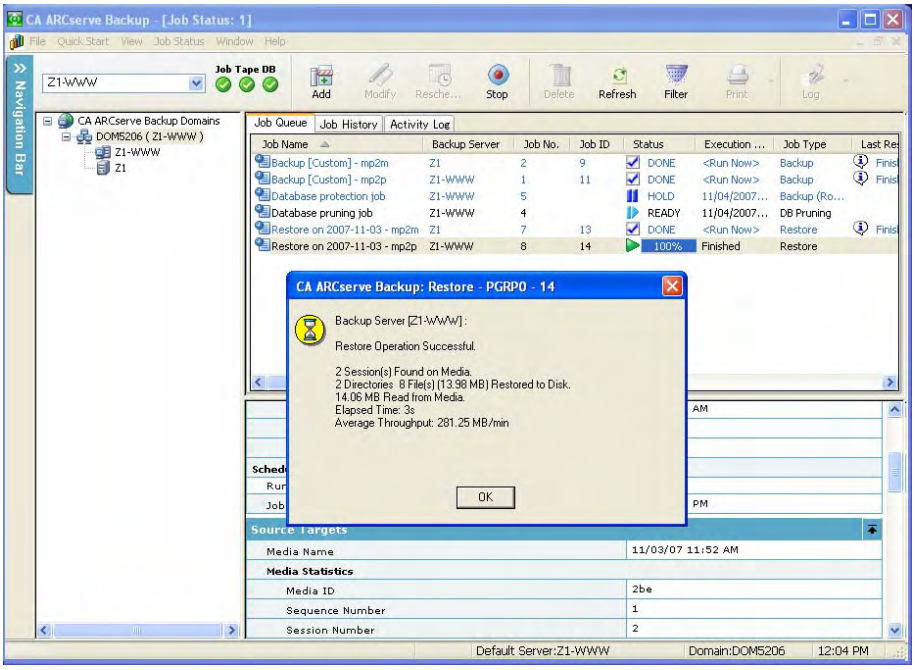
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



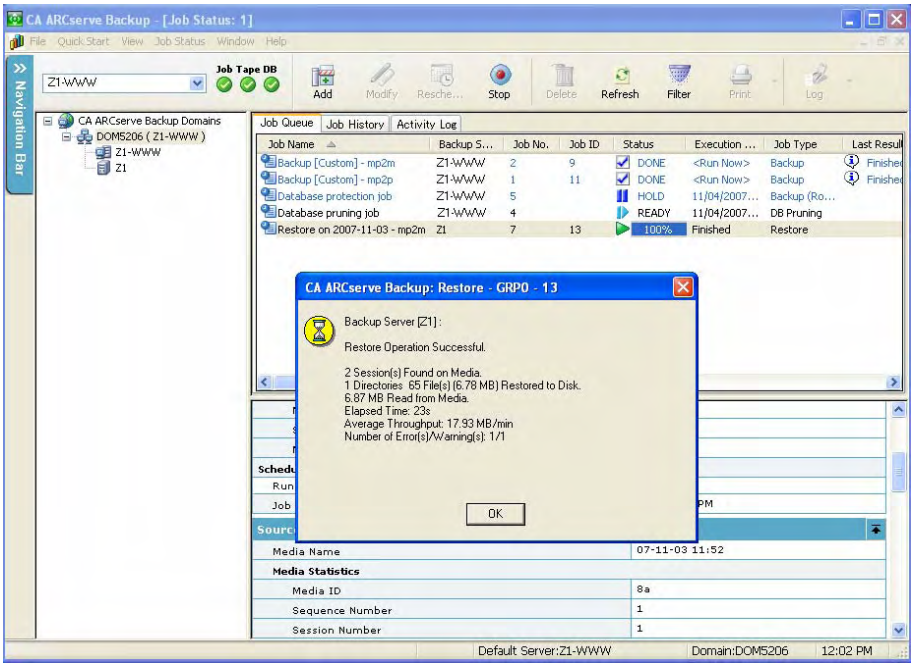
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   If the job fails, perform the following troubleshooting tasks:

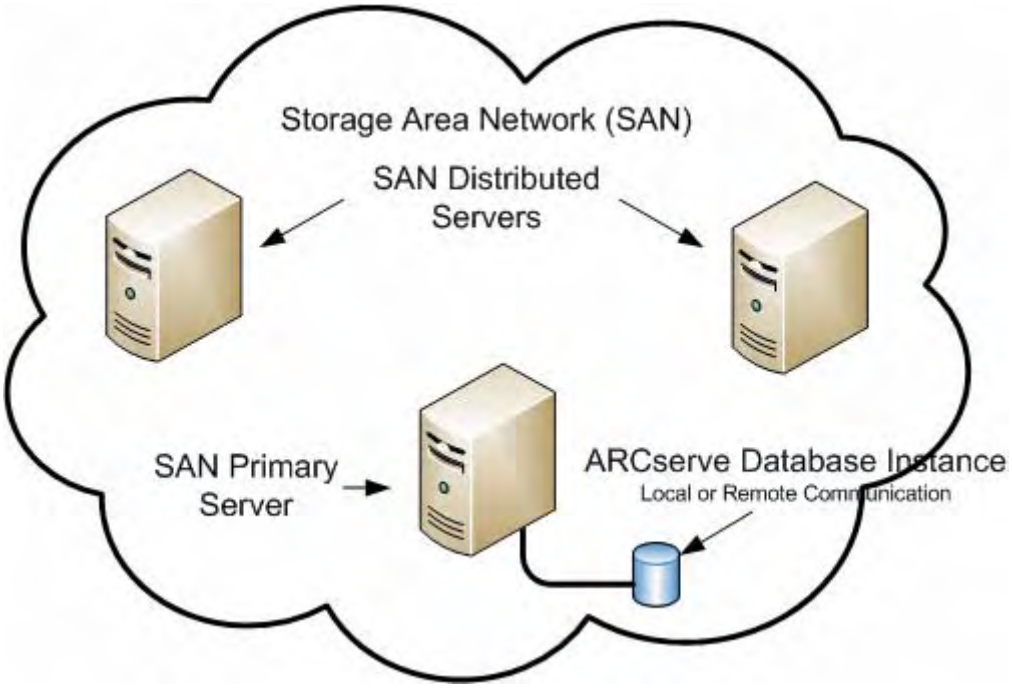
   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit 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.

Current Configuration - Multiple ARCserve Servers in a SAN Using a Local or Remote Database

The following diagram illustrates multiple ARCserve 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 ARCserve environment consists of multiple ARCserve servers that reside on a SAN and share a local or remote ARCserve 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.

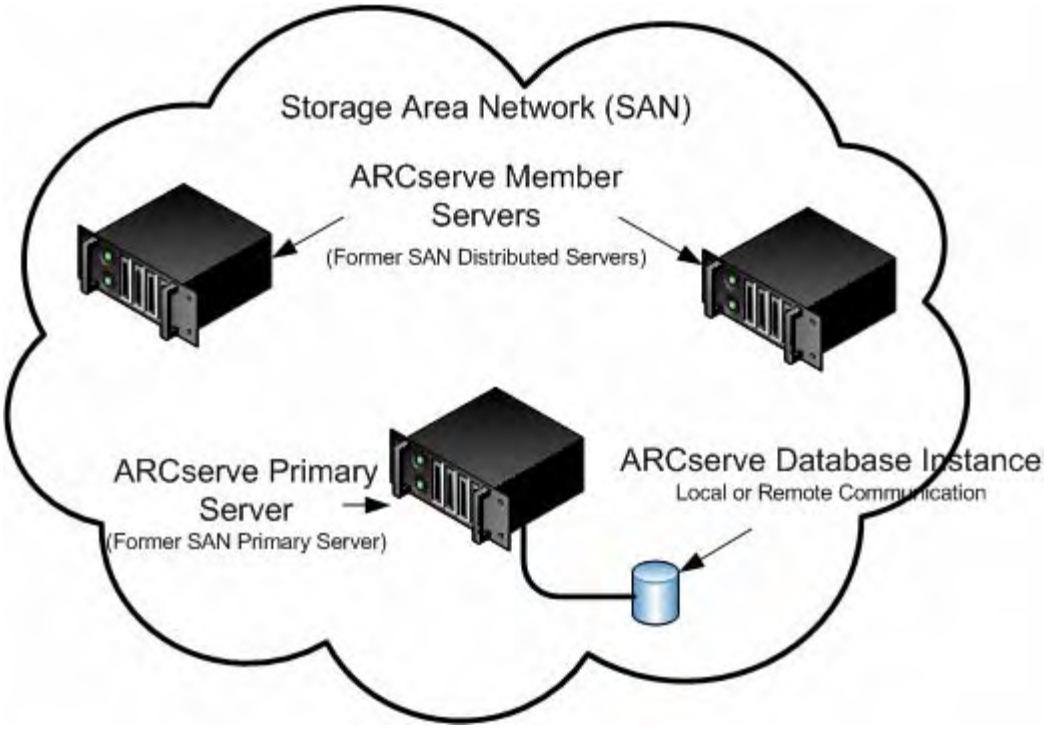
To upgrade your current SAN environment to a centralized management environment, you must upgrade your current SAN primary server to a CA ARCserve Backup Primary Server, and then upgrade your SAN distributed servers to CA ARCserve Backup Member Servers of that particular primary server.

To install member servers, the installation wizard must be able to detect the ARCserve 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.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 a centralized management environment integrated with a SAN and a local or remote ARCserve database.

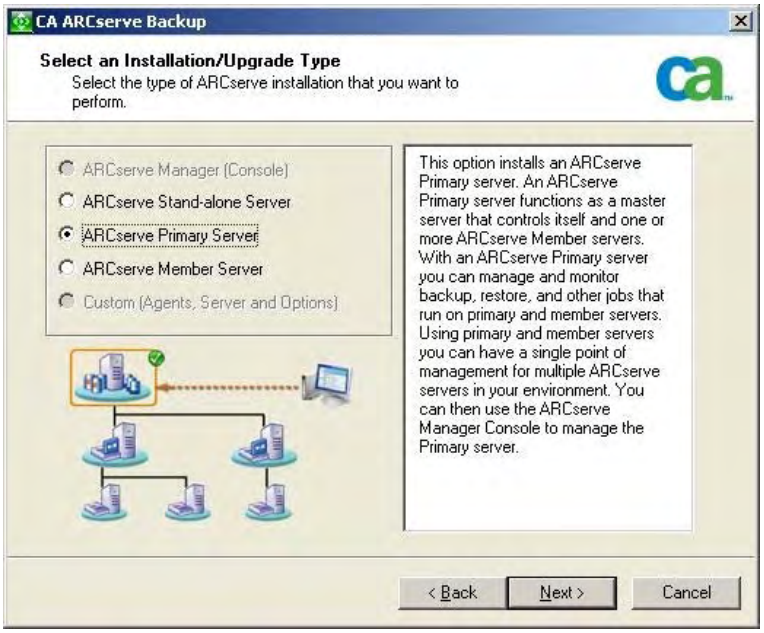


New Components You Must Install

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

CA ARCserve Backup Primary Server

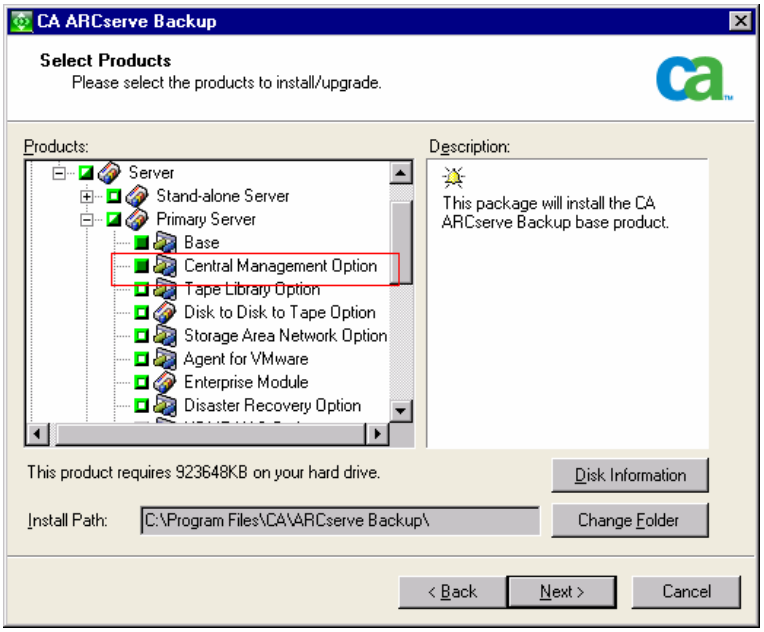
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

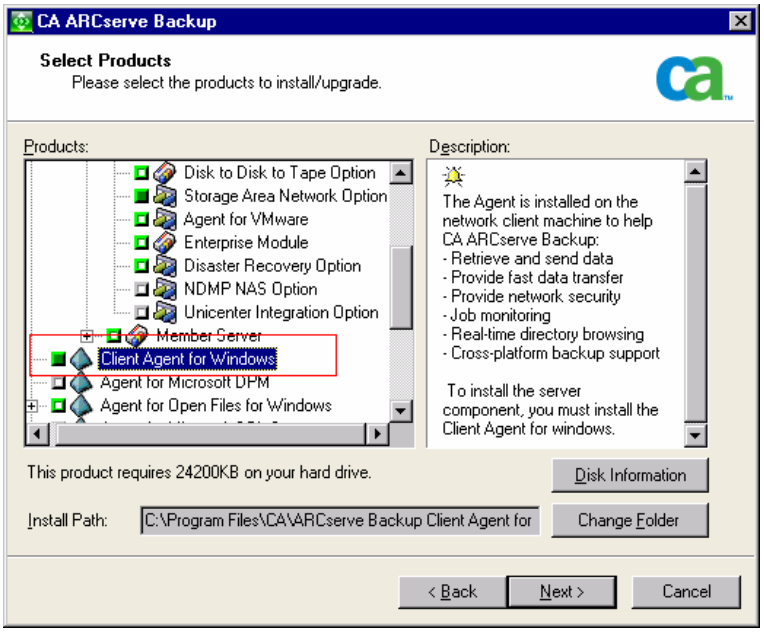
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

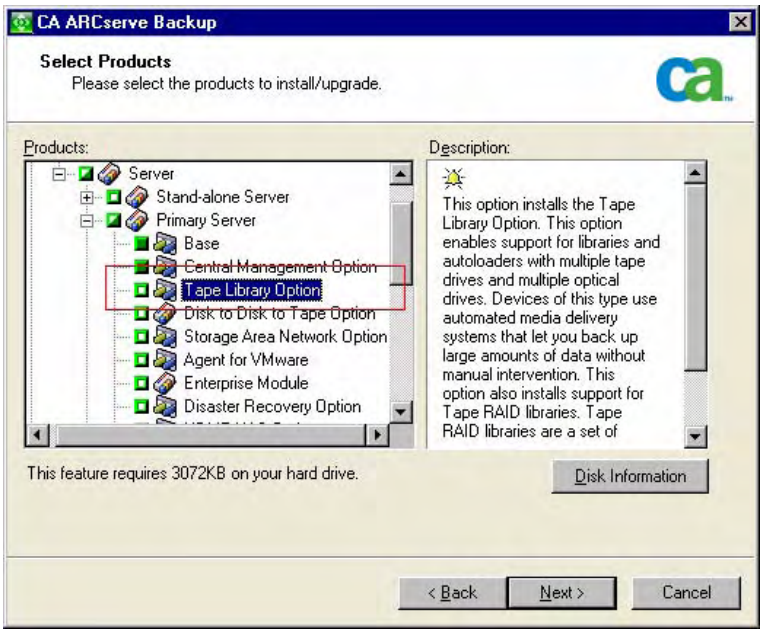
CA ARCserve Backup Client Agent for Windows

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



CA ARCserve Backup Tape Library Option

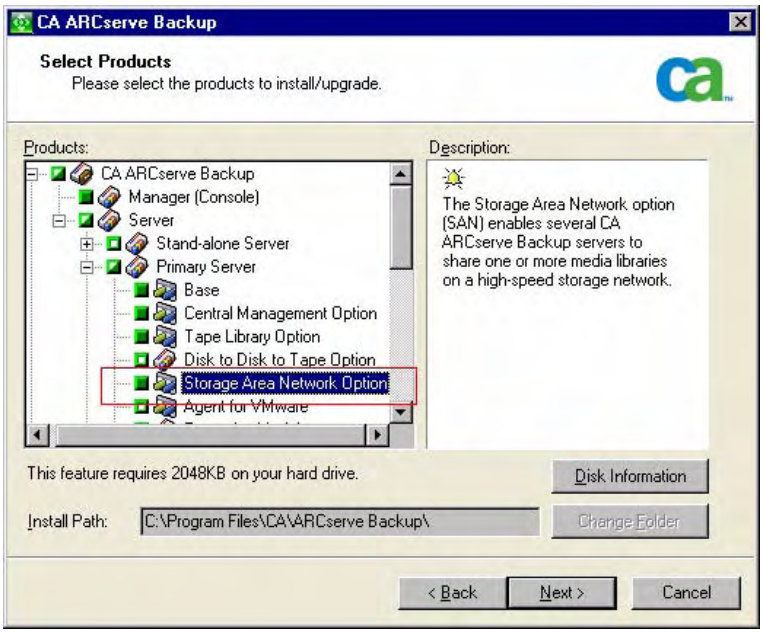
Lets you perform backup, restore, and media management capabilities using libraries with multiple tape drives and multiple optical drives, and tape RAID libraries.



CA ARCserve Backup Storage Area Network (SAN) Option

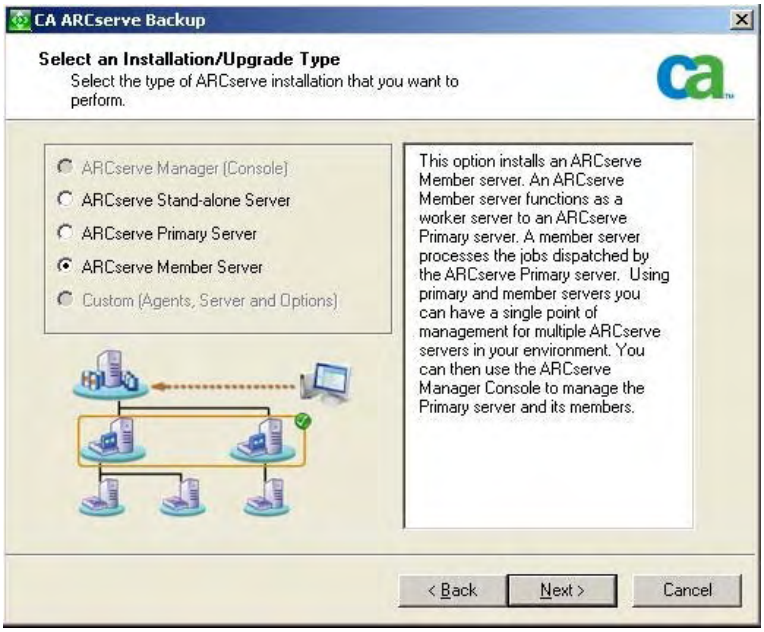
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Note: The Tape Library Option is a prerequisite component for 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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database. If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

   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.

More information:

Upgrade Considerations (see page 50)
Upgrade CA ARCserve Backup from a Previous Release (see page 66)

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.

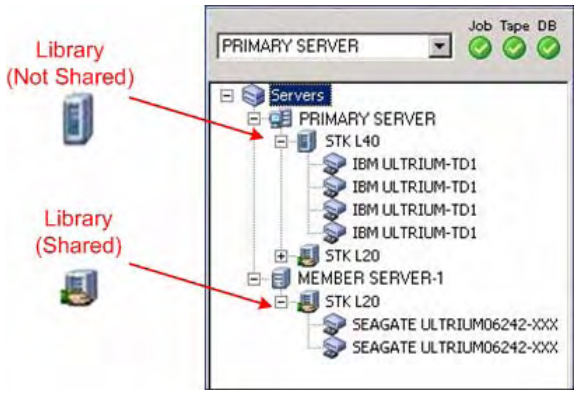
   Ensure that all previous backup data migrated successfully.

   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.

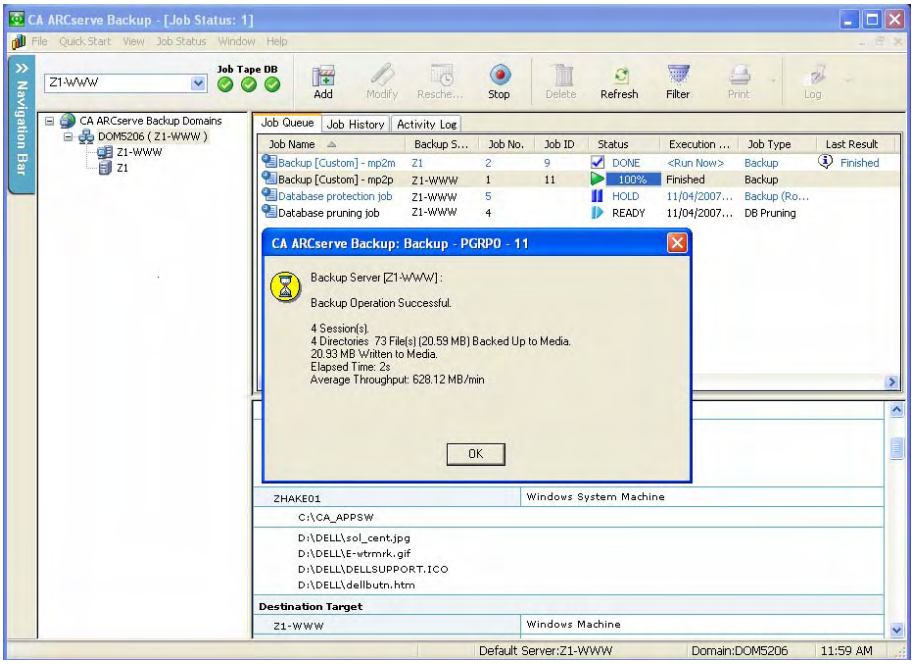
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



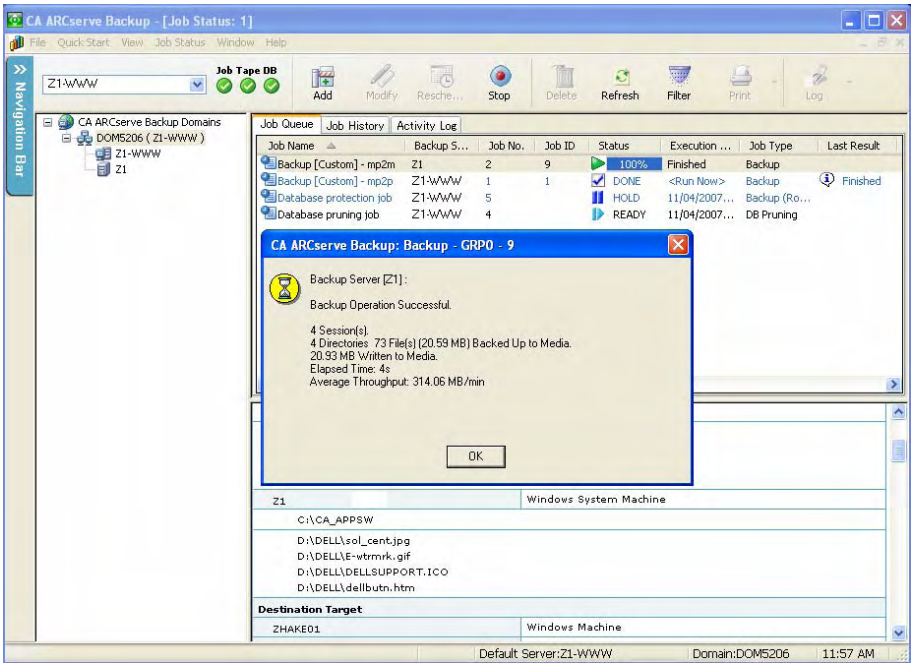
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



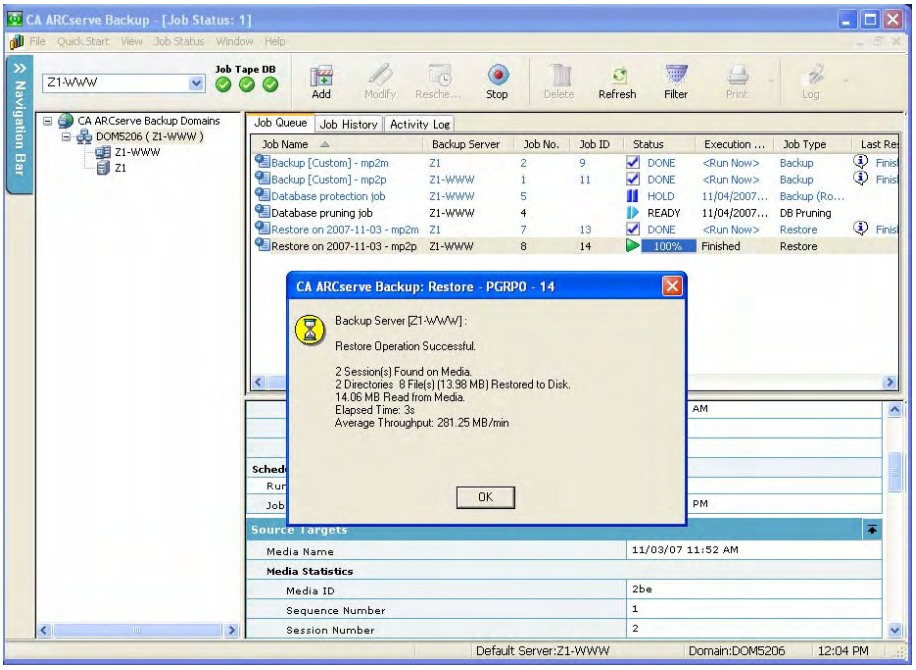
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



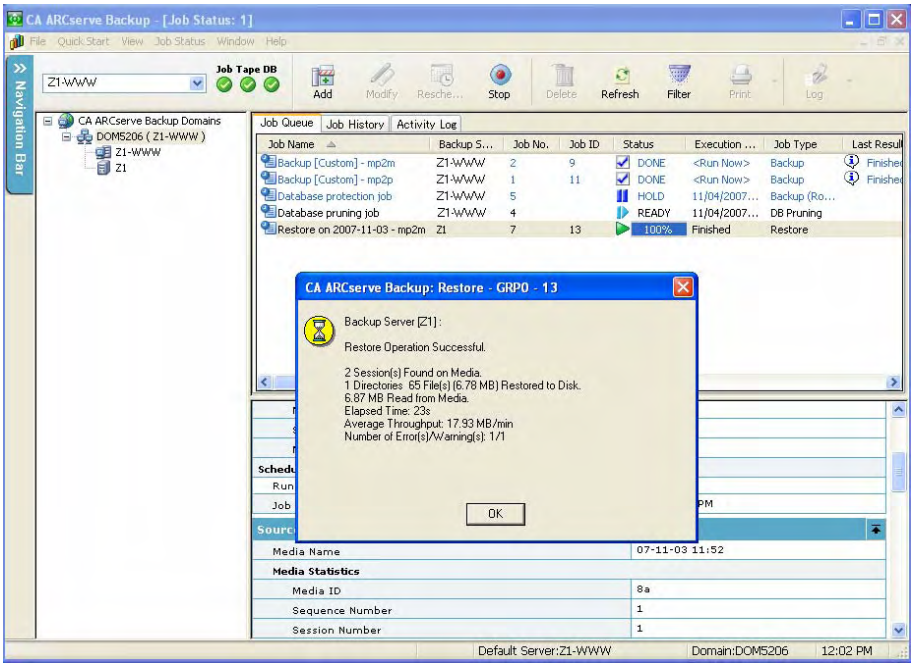
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   If the job fails, perform the following troubleshooting tasks:

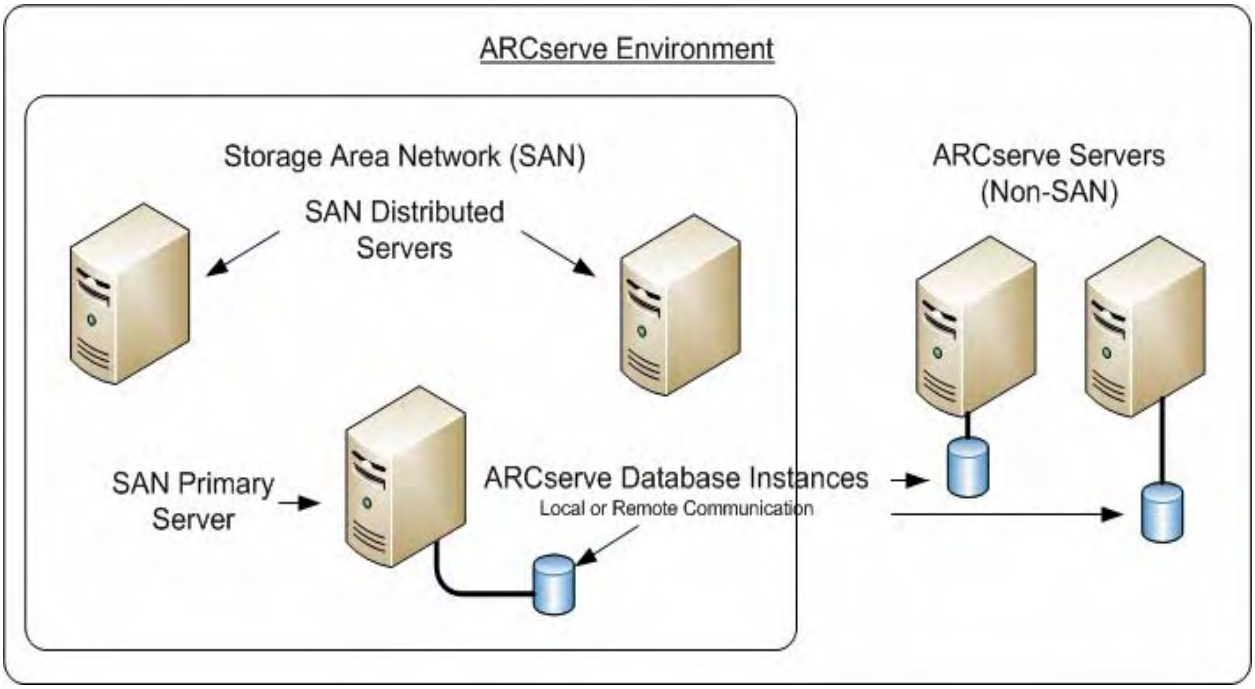
   - From the Job Status Manager, review the Activity Log details for the job.
   - If a job contains warning messages, error messages, or both, double-click the message to view a description of the problem and the steps that you can take to correct the problem.
   - After you correct the problem, resubmit 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.

Current Configuration - Multiple ARCserve Servers in a SAN and Non-SAN Environment

The following diagram illustrates multiple ARCserve 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 ARCserve servers reside on the SAN while other ARCserve servers do not reside on the SAN, the best practice is to install CA ARCserve Backup in a centrally managed environment.

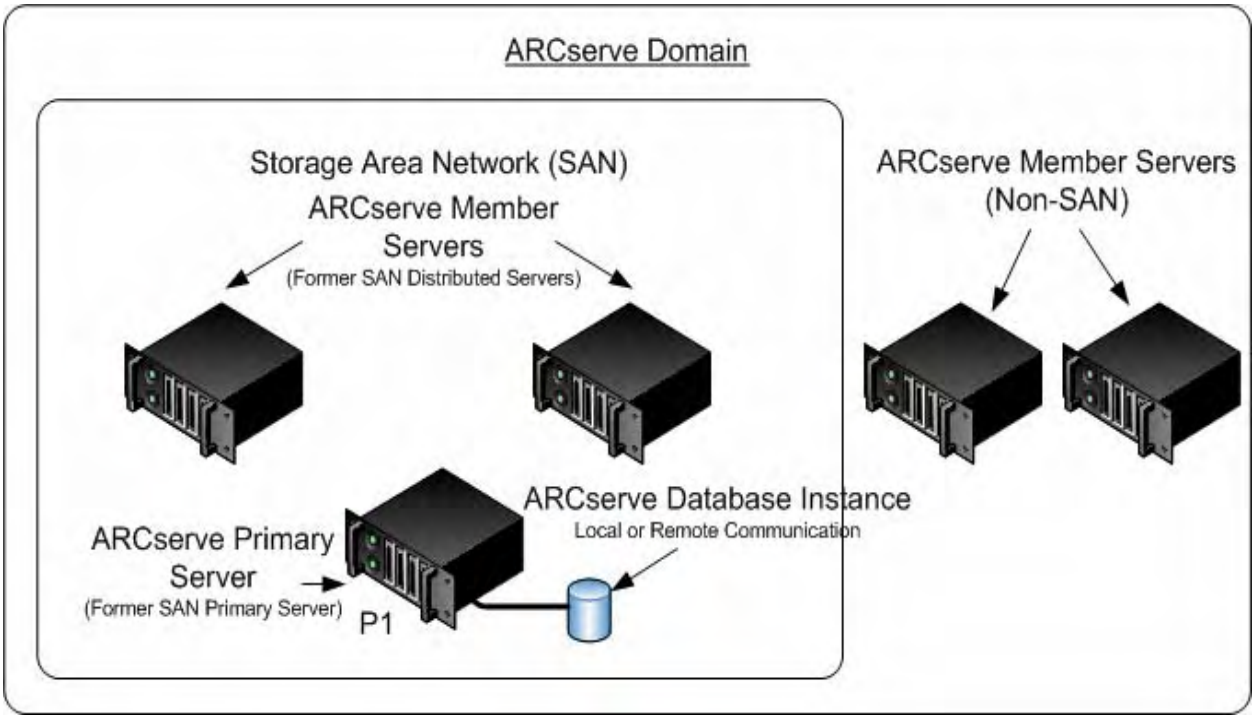
To upgrade your current SAN environment to a centralized management environment, you must upgrade your current SAN primary server to a CA ARCserve Backup Primary Server, and then upgrade your SAN distributed servers to CA ARCserve Backup Member Servers.

To install member servers, the installation must be able to detect the ARCserve 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.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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 a centralized management environment consisting of an ARCserve primary server and ARCserve member servers that reside on a SAN, and ARCserve member servers that do not reside on the SAN.

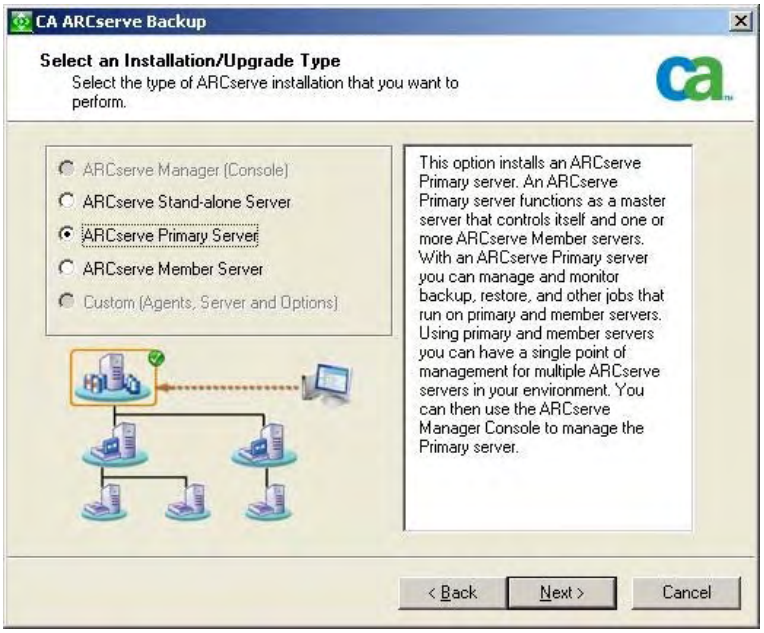


New Components You Must Install

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

CA ARCserve Backup Primary Server

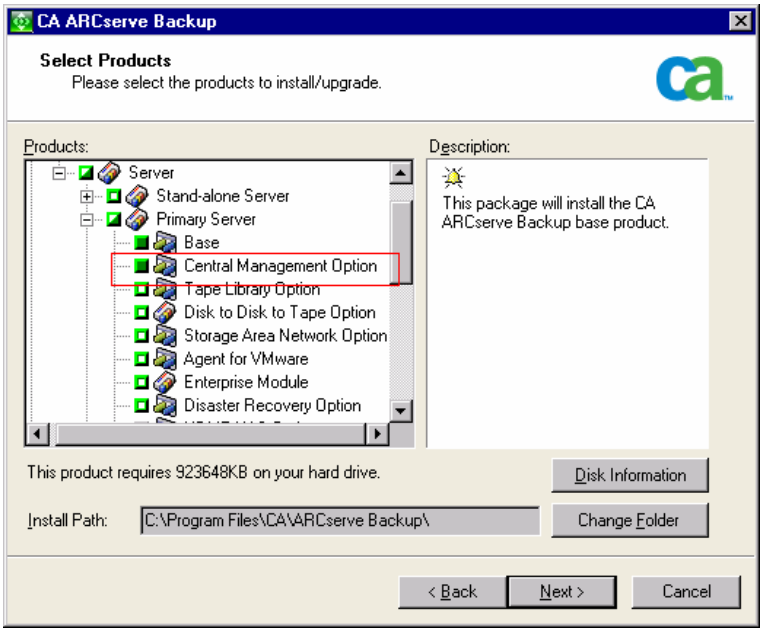
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

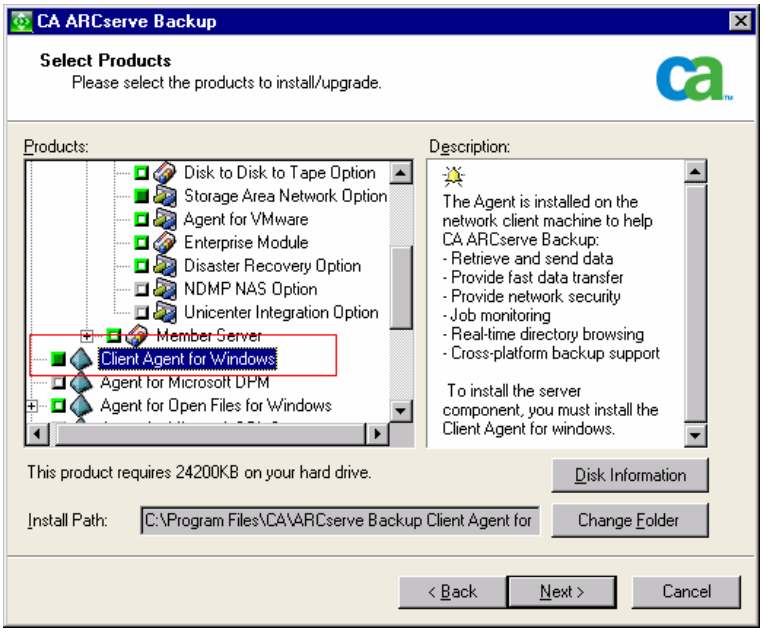
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

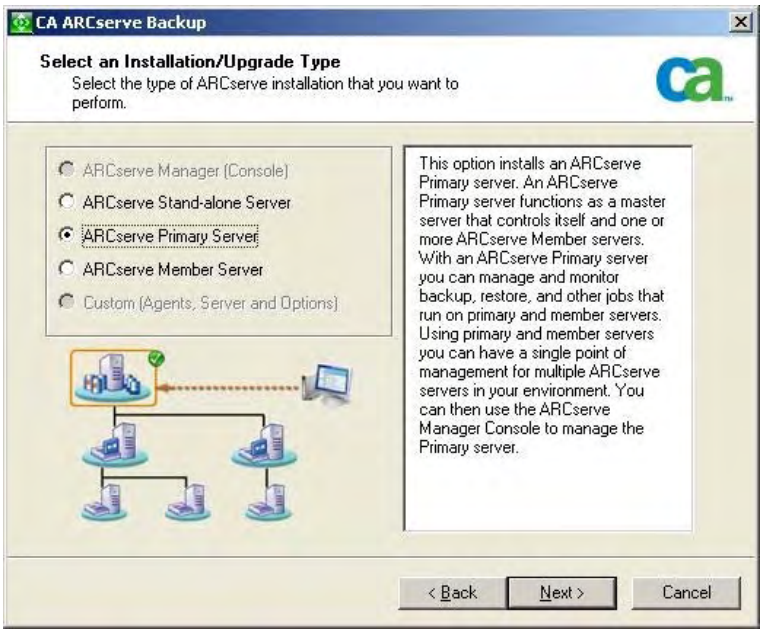
CA ARCserve Backup Client Agent for Windows

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



CA ARCserve Backup Primary Server

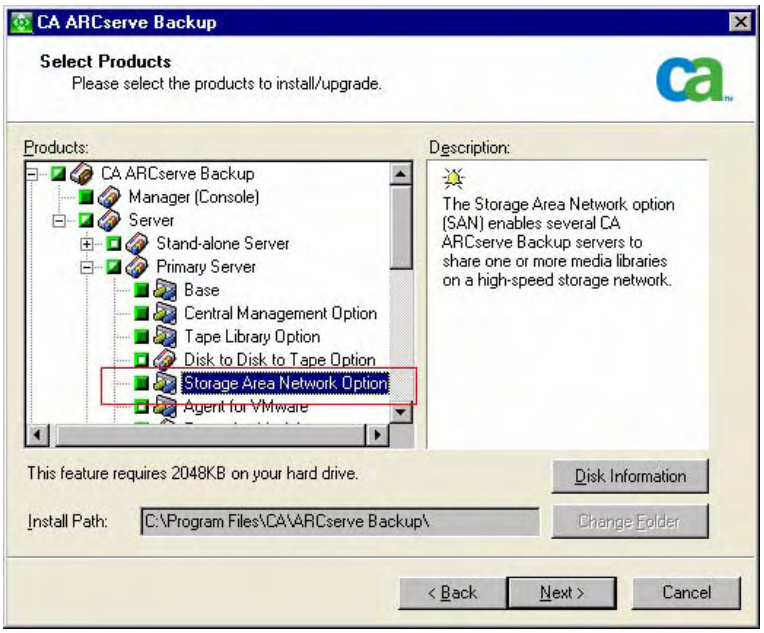
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Storage Area Network (SAN) Option

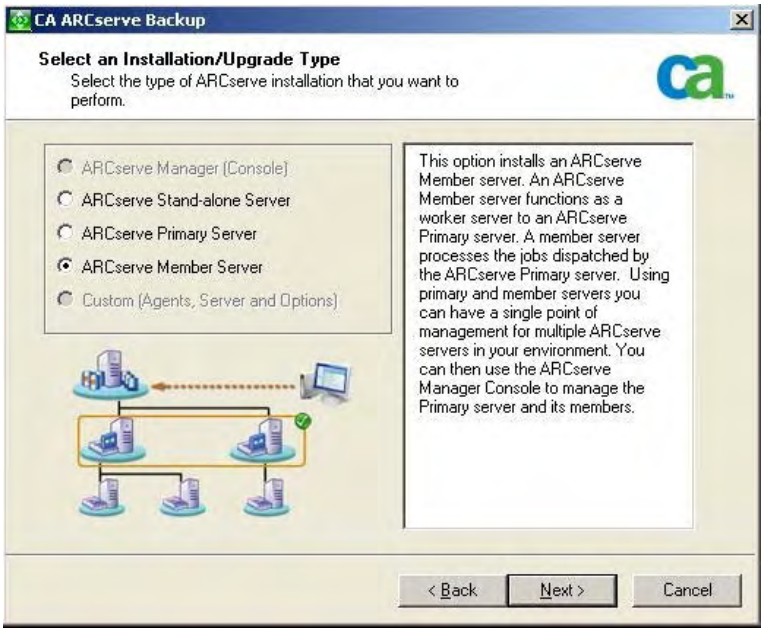
Lets you share one or more media libraries on a high-speed storage network with one or more ARCserve servers.

Note: The Tape Library Option is a prerequisite component for 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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database. If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

   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.

More information:

Upgrade Considerations (see page 50)
Upgrade CA ARCserve Backup from a Previous Release (see page 66)

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.

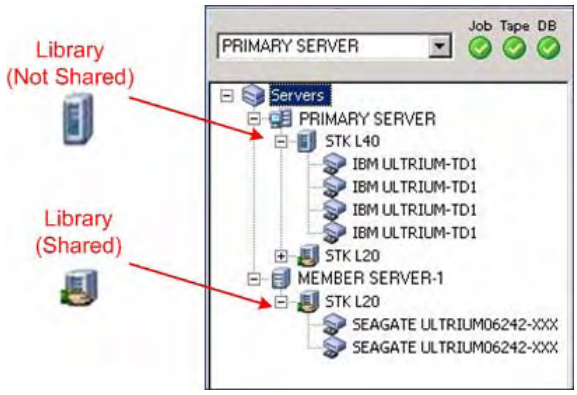
   Ensure that all previous backup data migrated successfully.

   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.

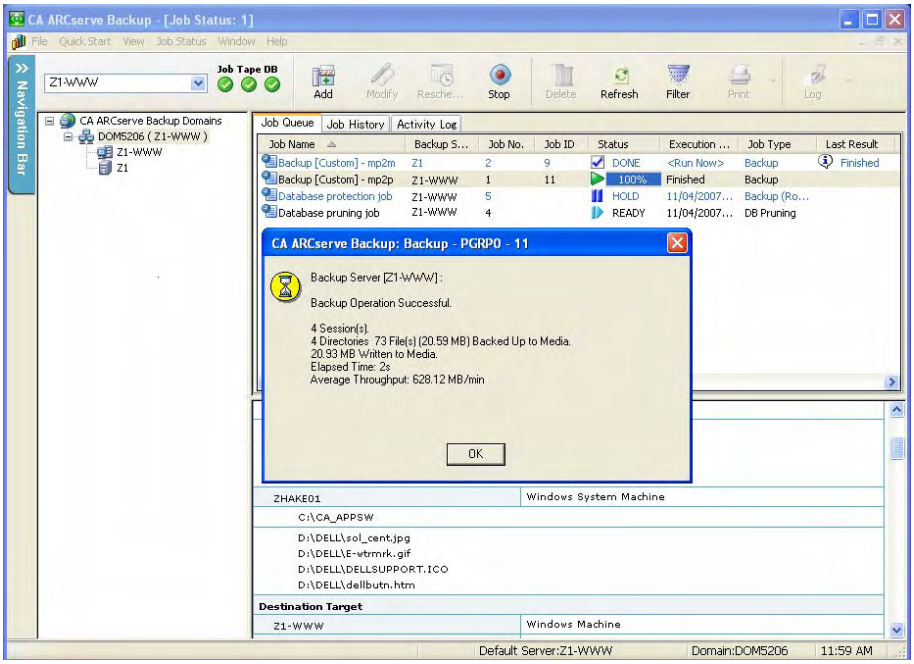
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



   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.

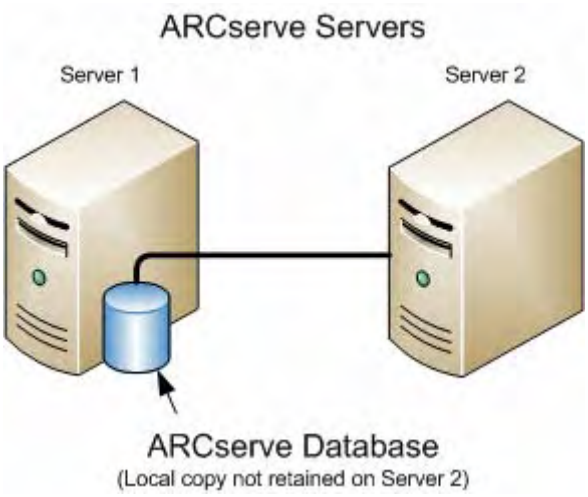
Upgrading Multiple Servers Using a Central Database

The following sections describe best practices that you can use to upgrade multiple ARCserve servers that share a centralized database to this release.

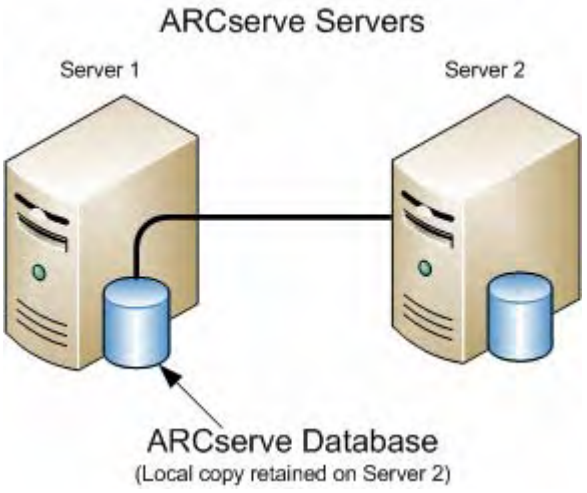
Current Configuration - Multiple ARCserve Servers Using a Central Database

The following diagram illustrates multiple ARCserve servers using a centralized database in previous releases.

In the following diagram, multiple ARCserve servers are sharing a centralized database. A copy of the ARCserve database is not retained on one of the ARCserve servers sharing the database.



In the following diagram, multiple ARCserve servers are sharing a centralized database. A copy of the ARCserve database is retained on one of the ARCserve servers sharing the database.



Recommended Configuration - CA ARCserve Backup Domain with a Primary Server and Member Servers

If your current configuration consists of multiple ARCserve servers sharing a centralized database, the best practice is to upgrade to a centralized management environment containing a primary server and one or more member servers. A centralized management environment lets you host the ARCserve database on the primary server or a remote system. You do not need to install CA ARCserve Backup on the system that hosts the ARCserve database instance.

To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition to host the ARCserve database. However, if your environment will consist of a primary server and more than ten member servers, you should host the ARCserve database using Microsoft SQL Server.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 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.

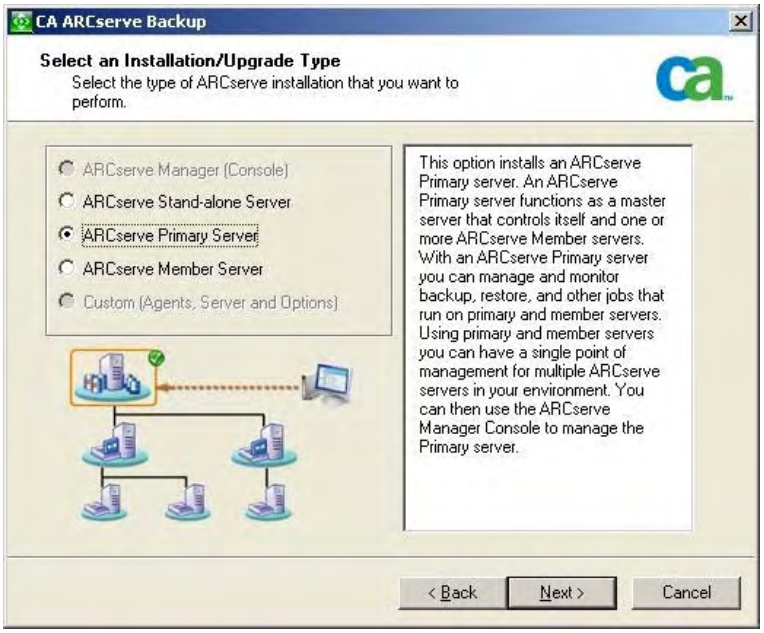
The following diagram illustrates a centralized management environment with a remote system hosting the CA ARCserve Backup database.

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

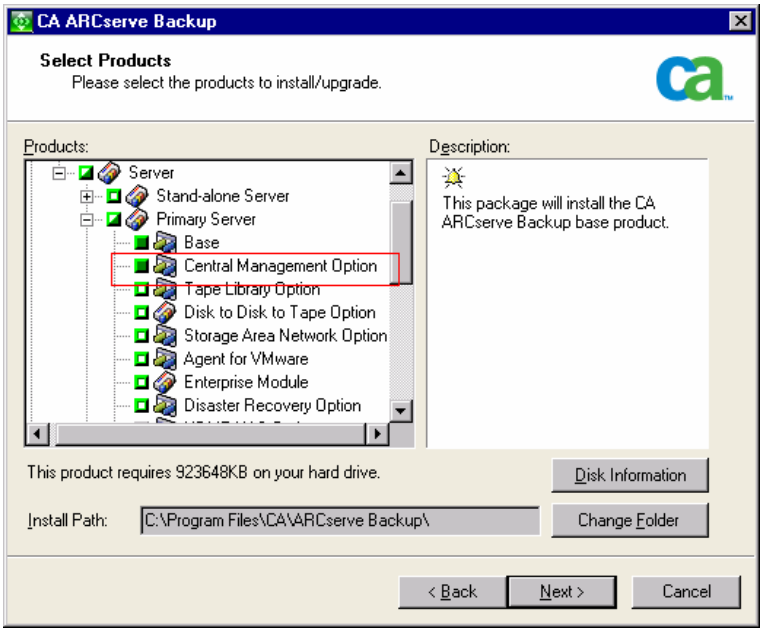
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

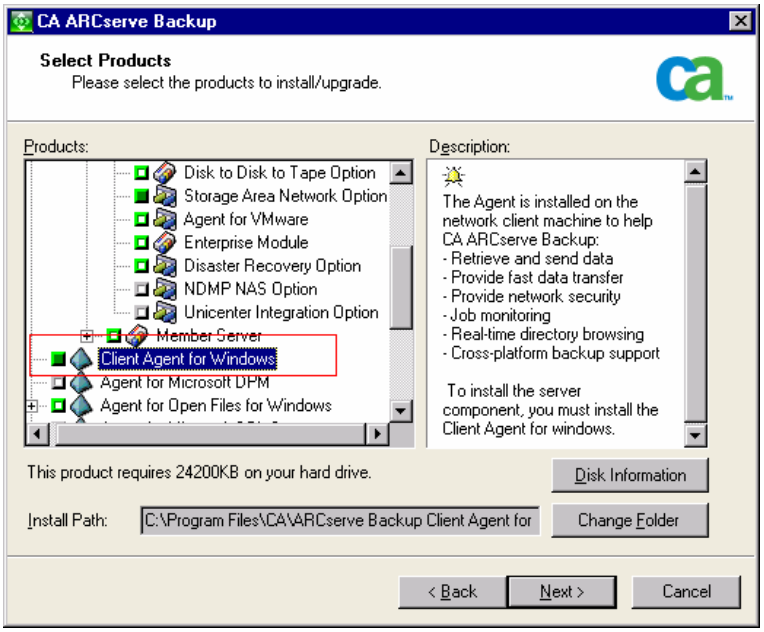
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

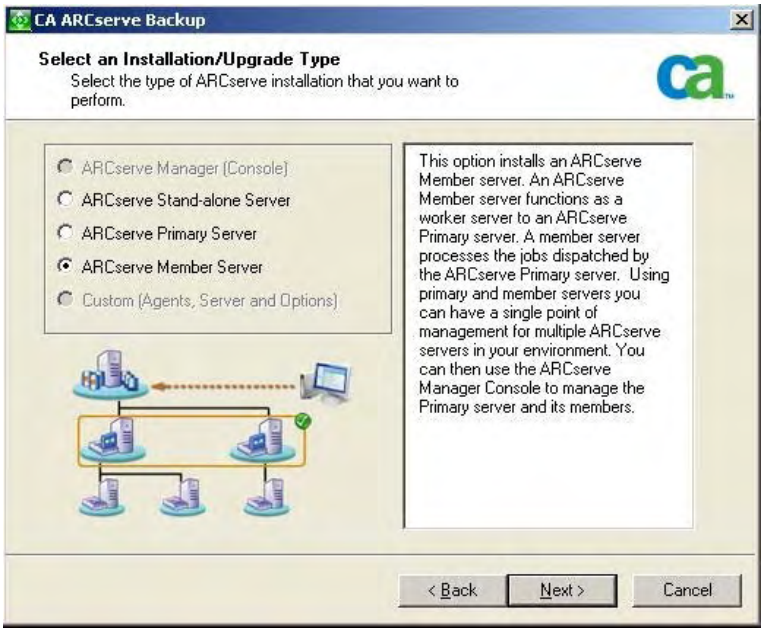
CA ARCserve Backup Client Agent for Windows

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 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 2005 Express or Microsoft SQL Server for the CA ARCserve Backup database. If your ARCserve environment will consist of more than 10 member servers, you should use Microsoft SQL Server to host the CA ARCserve Backup database instance.

   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.

More information:

Upgrade Considerations (see page 50)
Upgrade CA ARCserve Backup from a Previous Release (see page 66)

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.

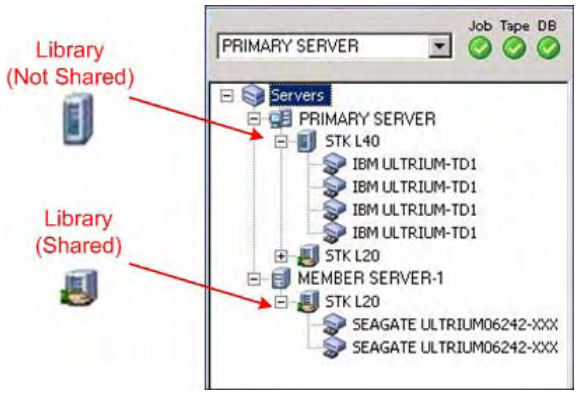
   Ensure that you can view database information and Activity Log data.

   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.

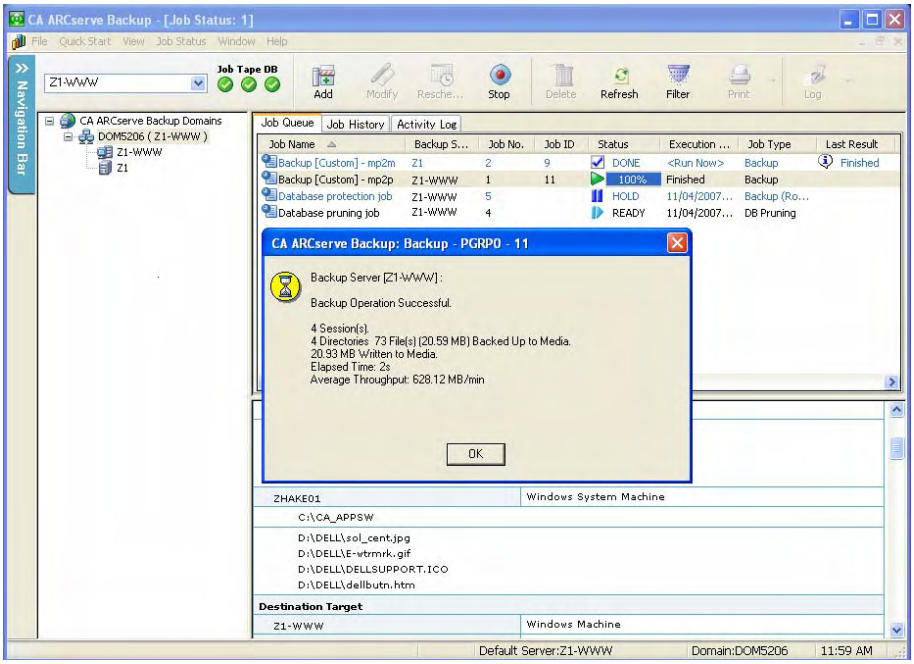
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



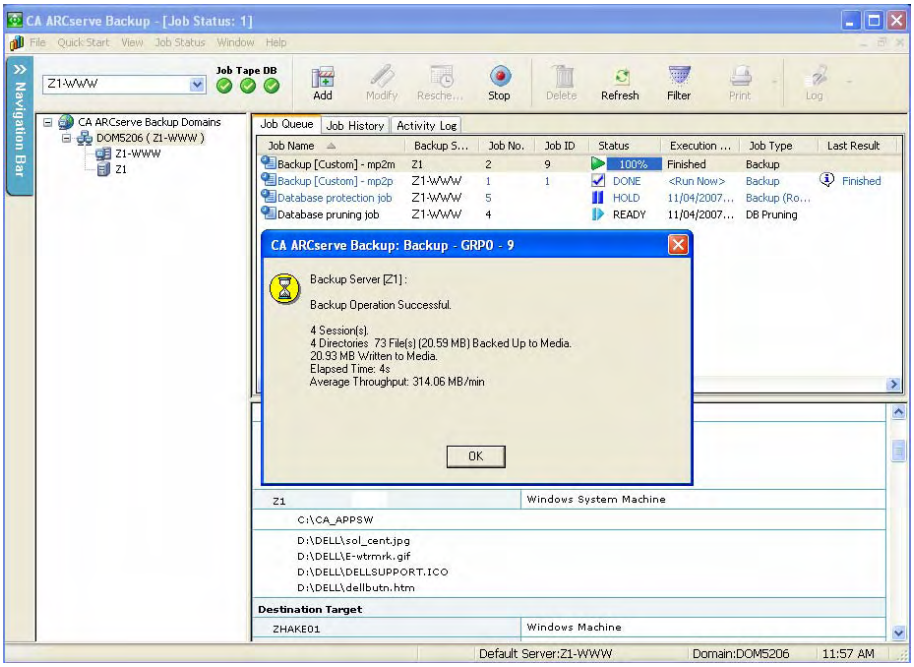
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



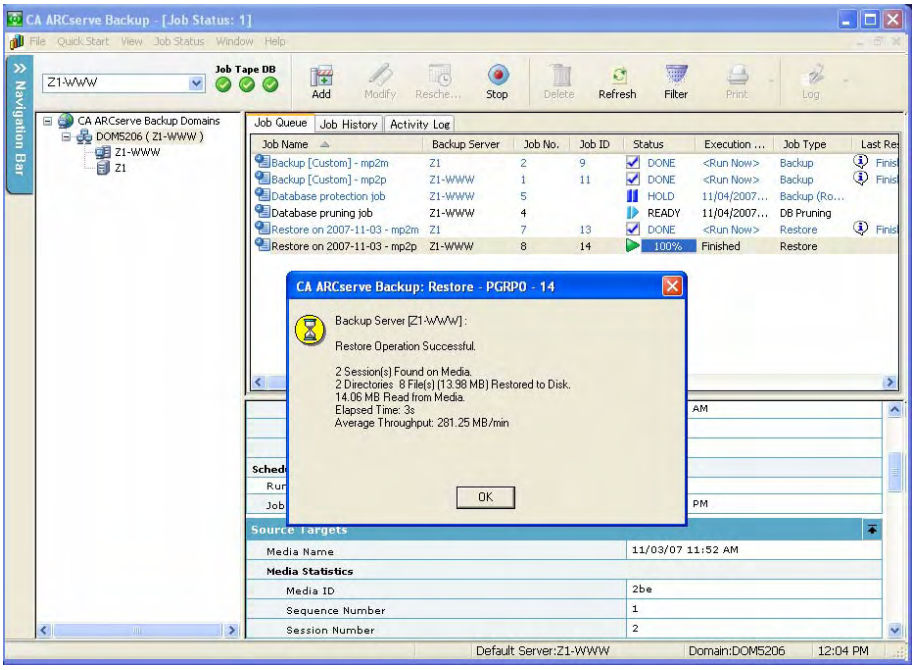
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



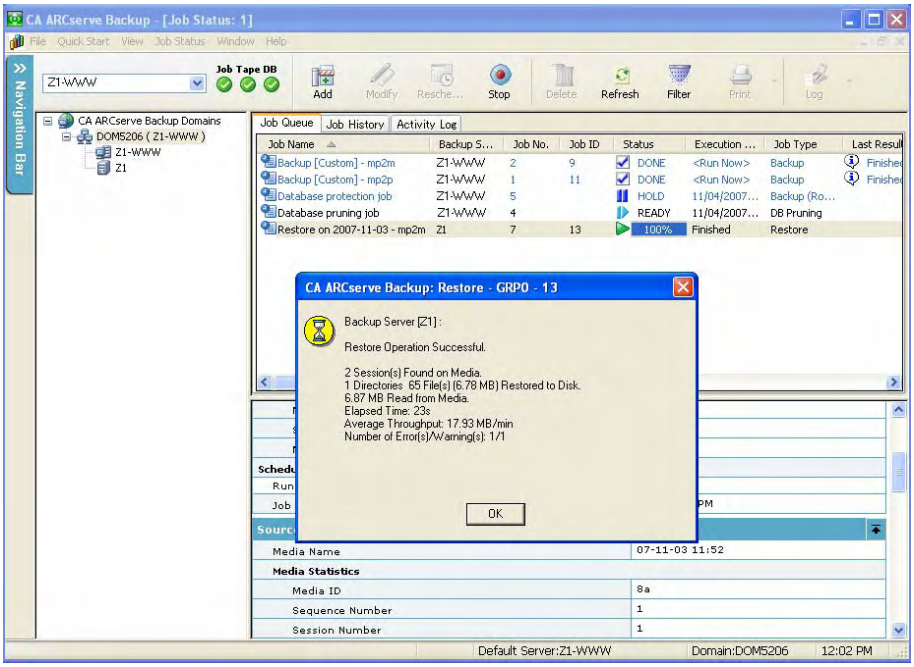
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a member server:



   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.

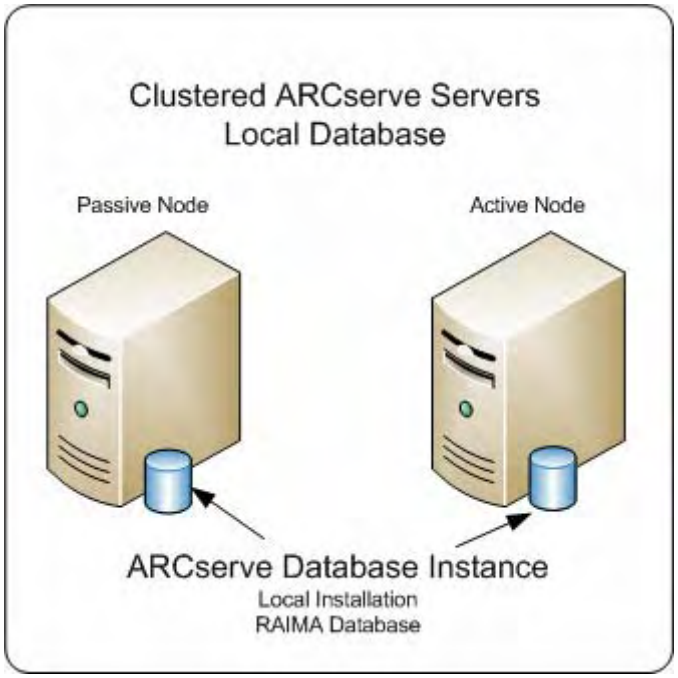
Upgrading Multiple Servers in a Cluster-aware Environment

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.

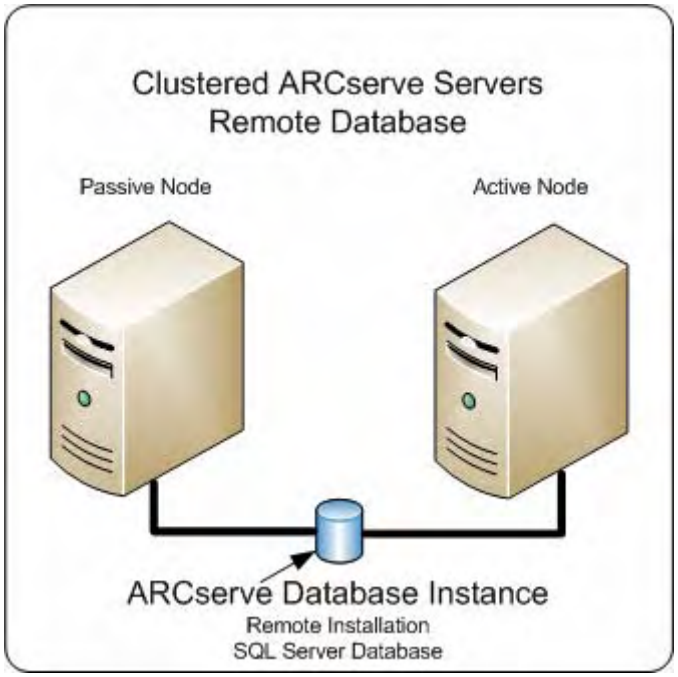
Important! The following best practices only apply to upgrading a BrightStor ARCserve Backup r11.5 cluster-aware environment. For all other releases, you must uninstall the previous release and then install CA ARCserve Backup into the cluster-aware environment.

Current Configuration - Multiple ARCserve Servers in a Cluster

The following diagram illustrates the architecture of multiple ARCserve servers in a cluster-aware environment in previous releases. The ARCserve database is hosted by a RAIMA database and the ARCserve instance resides on the ARCserve backup server.



The following diagram illustrates the architecture of multiple ARCserve servers in a cluster-aware environment in previous releases. The ARCserve database is hosted by Microsoft SQL Server and the ARCserve instance resides on a remote system.



Recommended Configuration - ARCserve Primary and Members Servers Installed in a Cluster-aware Environment

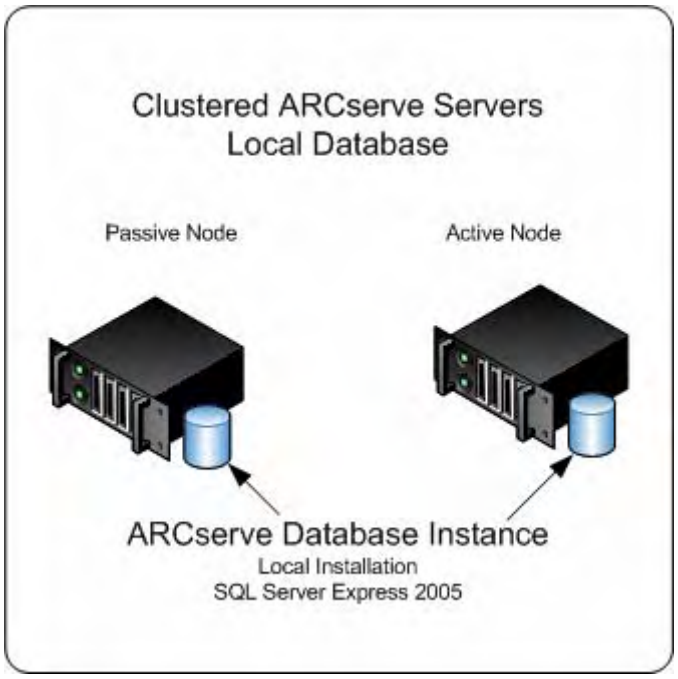
If your current configuration consists of multiple ARCserve servers in a cluster-aware environment, the best practice is to upgrade to multiple CA ARCserve Backup Primary Servers or multiple CA ARCserve Backup Stand-alone Servers.

This architecture lets you centrally manage your ARCserve environment and maintain the high availability capabilities of a cluster-aware environment.

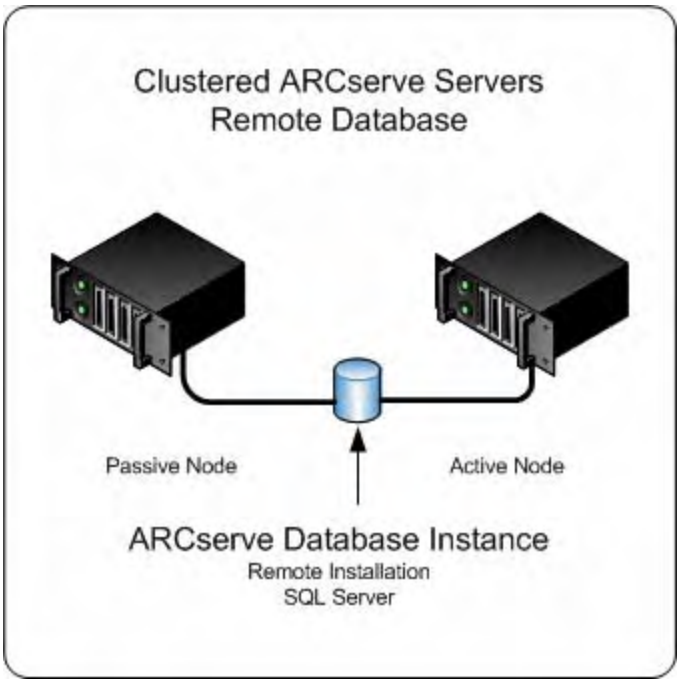
To deploy this configuration in your environment, you can use Microsoft SQL Server 2005 Express Edition or Microsoft SQL Server to host the ARCserve database.

Note: Microsoft SQL Server 2005 Express Edition does not support remote communication. When you install CA ARCserve Backup using Microsoft SQL Server 2005 Express Edition, the installation wizard installs the database application and the ARCserve database instance on the primary server. To host the ARCserve database instance on a remote system, you must use Microsoft SQL Server.

The following diagram illustrates the architecture of multiple ARCserve servers in a cluster-aware environment in this release. The ARCserve database is hosted by Microsoft SQL Server 2005 Express Edition and the ARCserve database instance resides on the ARCserve backup server.



The following diagram illustrates the architecture of multiple ARCserve servers in a cluster-aware environment in this release. The ARCserve database is hosted by Microsoft SQL Server and the ARCserve database instance resides on a remote system.

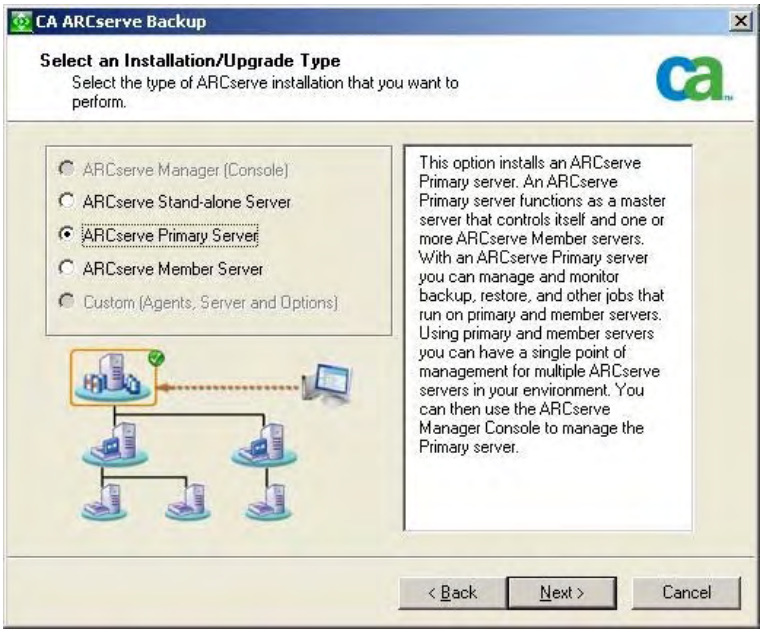


New Components You Must Install

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

CA ARCserve Backup Primary Server

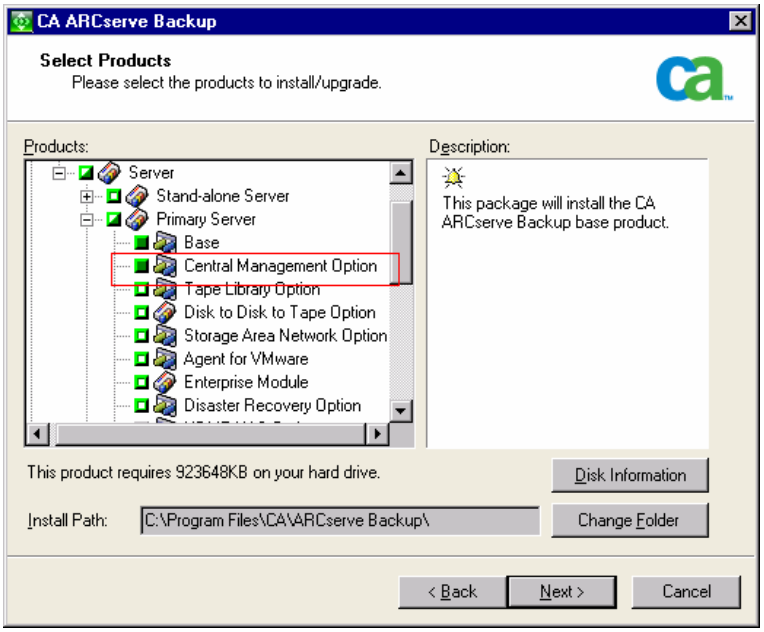
Lets you install CA ARCserve Backup on a server that you will use to centrally submit, manage, and monitor backup and restore jobs that run on member servers and the primary server.



CA ARCserve Backup Central Management Option

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

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



CA ARCserve Backup Agent for Microsoft SQL Server

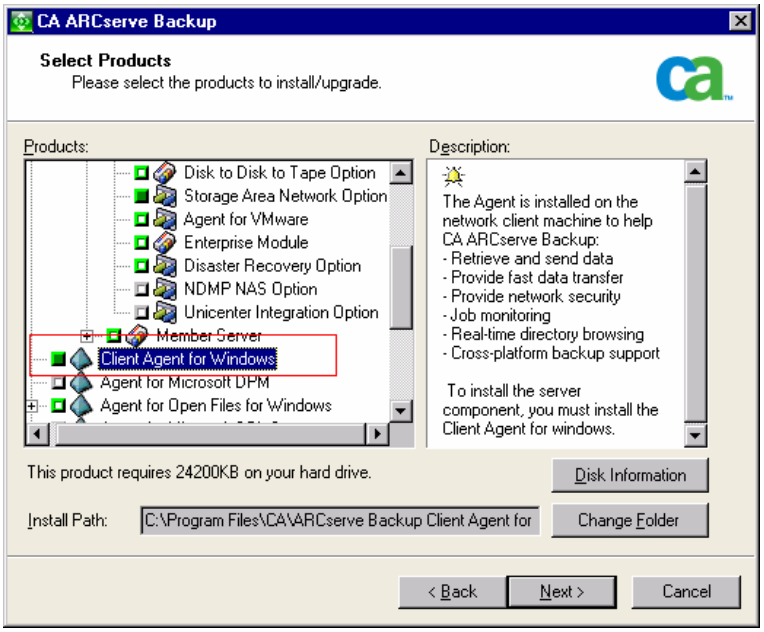
Lets you protect the CA ARCserve Backup database.

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 ARCserve database instance and the Agent for ARCserve Database from your computer. When you reinstall CA ARCserve Backup, the installation wizard detects the presence of a Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition database instance on your system. As a result, the installation wizard selects the CA ARCserve Backup Agent for Microsoft SQL Server component on the Select Product installation dialog.

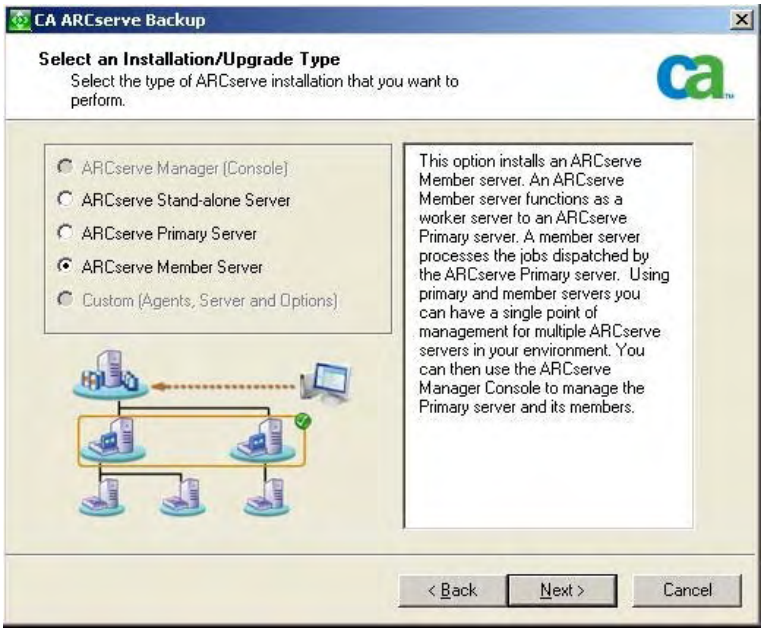
CA ARCserve Backup Client Agent for Windows

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 and NEC ClusterPro/ExpressCluster X 1.0 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 r12 in a MSCS Cluster Environment (see page 96)
   - Upgrade CA ARCserve Backup from r11.5 to r12 in an NEC ClusterPro Environment (see page 116).
2. Verify the upgrade.

More information:

Upgrade CA ARCserve Backup from r11.5 to r12 in a MSCS Cluster Environment (see page 96)
Upgrade CA ARCserve Backup from r11.5 to r12 in an NEC ClusterPro Environment (see page 116)

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.

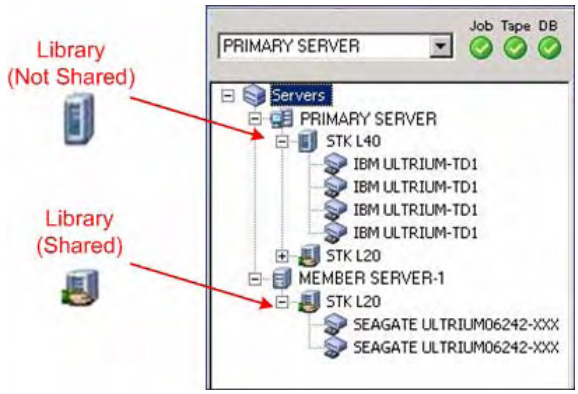
5. Open the Job Status Manager.

   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.

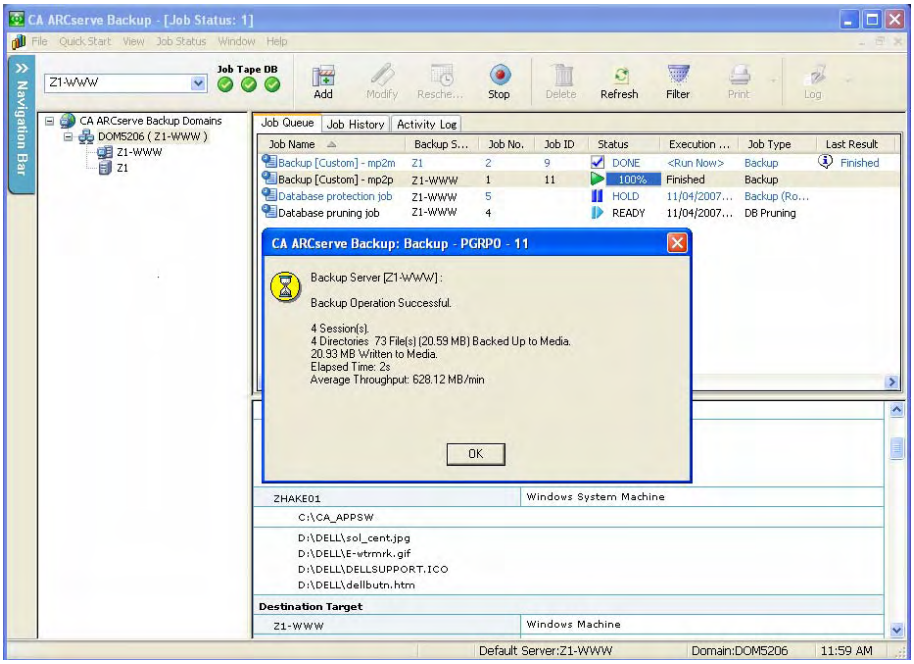
   If CA ARCserve Backup cannot detect the devices after you complete these tasks, contact Technical Support at http://ca.com/support.

   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.

   The following screen illustrates a successful backup job on a primary server:



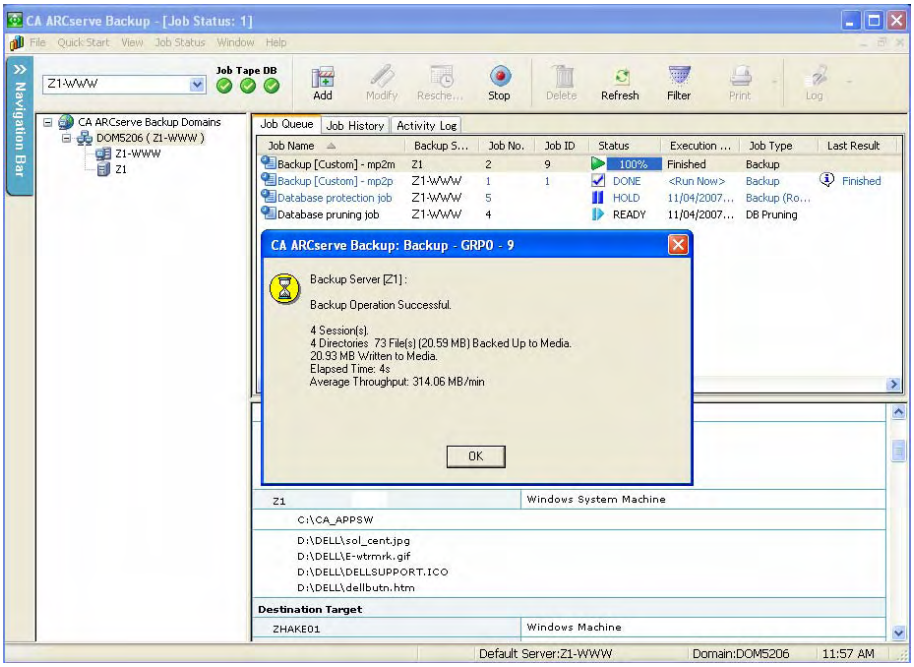
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful backup job on a member server:



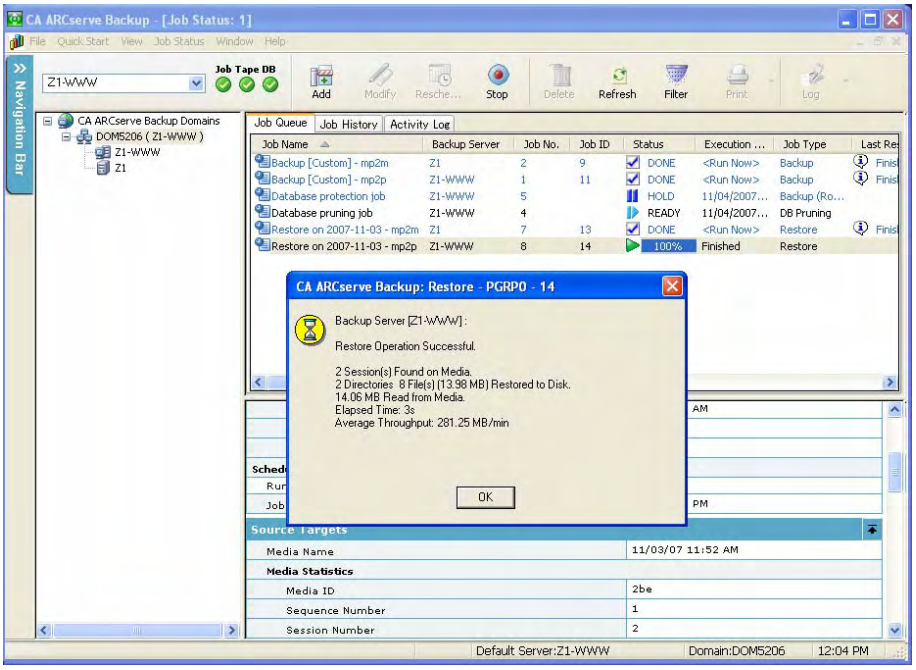
   If the job fails, perform the following troubleshooting tasks:

   - 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.

   The following screen illustrates a successful restore job on a primary server:



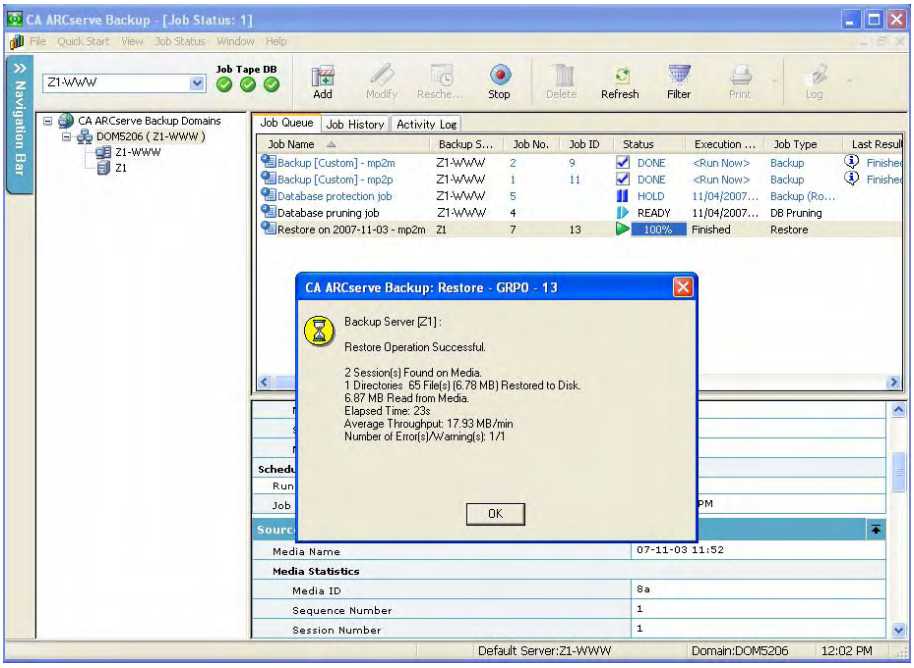
   If the job fails, perform the following troubleshooting tasks:

   - 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.

    The following screen illustrates a successful restore job on a member server:



    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.

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 Choose a Database Application

CA ARCserve Backup lets you use Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition to host the ARCserve database. To choose which application is best for your installation, consider the following general guidelines:

Microsoft SQL Server

- You require a primary server and more than 10 member servers to protect your environment.
- You are upgrading from a previous ARCserve release, and you are currently hosting the ARCserve database instance using Microsoft SQL Server.

Microsoft SQL Server 2005 Express Edition

- You require a single backup server, or a primary server with less than ten member servers to protect your environment.

Note: For more information, see Database Requirements (see page 43).

More information:

Microsoft SQL Server 2005 Express Edition Considerations (see page 44)
Microsoft SQL Server Database Considerations (see page 45)

How to Install and Manage Licenses

The following sections describe how to install and manage CA ARCserve Backup licenses.

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 an ARCserve Primary server and an ARCserve Member server in an ARCserve domain.
- Identify the number of active licenses for each ARCserve component in an ARCserve domain.
- View the names ARCserve Primary and Member servers using active component licenses in an ARCserve domain.
- Release licenses from an ARCserve Primary server or ARCserve Member servers in an ARCserve domain.

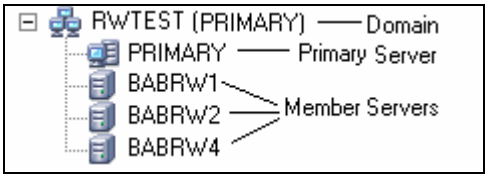
  Note: For information about releasing licenses from servers, see Release Licenses from Servers (see page 332).

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.

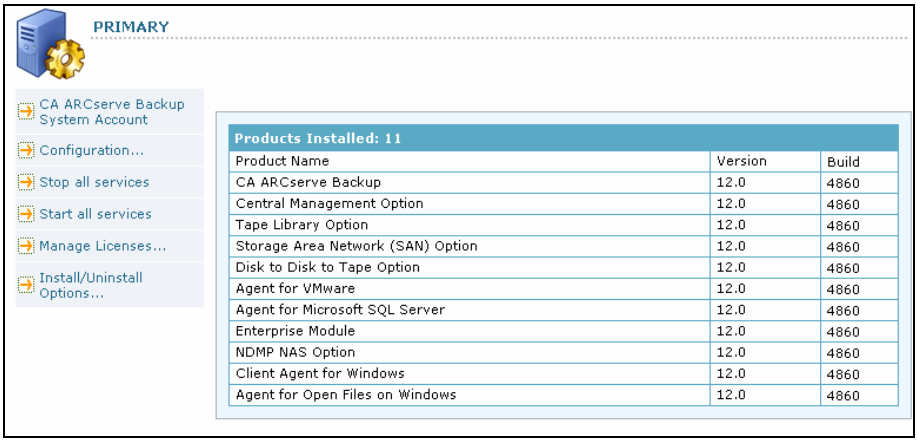
   The Server Admin opens.

   The ARCserve 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 an ARCserve Primary server and an ARCserve 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:



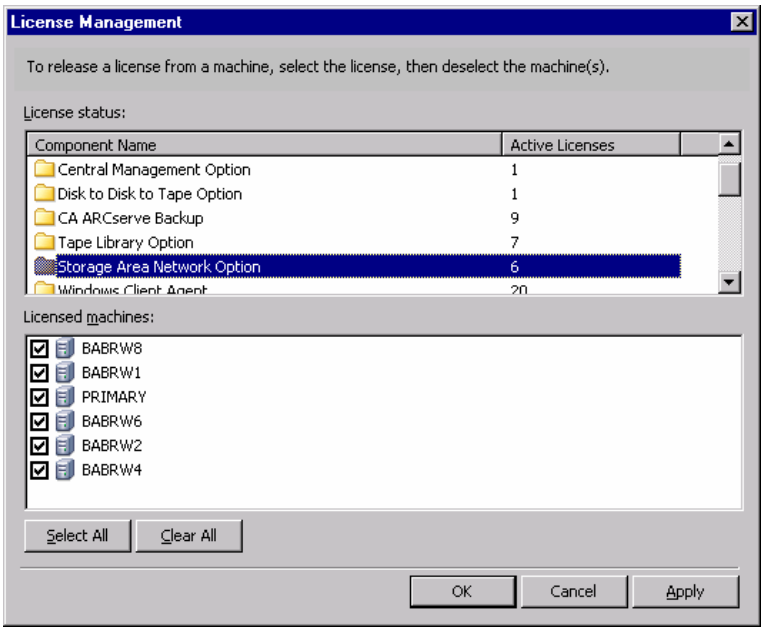
3. To view the component and licensing relationships in an ARCserve domain, right-click the Primary server and select Manage Licenses from the pop-up menu.

   The License Management dialog opens.

   The License Management dialog provides you with the following information:

   - The License status section identifies the number of active licenses for each ARCserve component in an ARCserve domain.
   - The Licensed machines section identifies the names of the servers using an active license for the selected ARCserve component.

   For example, the following diagram illustrates that there are six active licenses for the Storage Area Network Option. The names of the six machines using the Storage Area Network Option licenses display in the Licensed machines field.



More information:

Release Licenses from Servers (see page 332)

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
- Disk to Disk to Tape Option
- Agent for VMware

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*.

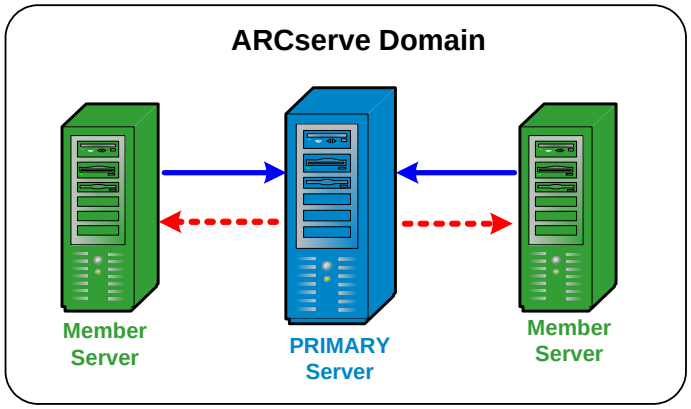
How to Use CA ARCserve Backup to Manage Daily Activities

The upgrade scenarios described in this appendix require you to install CA ARCserve Backup Primary Servers and CA ARCserve Backup Member Servers. When you install the CA ARCserve Backup Primary Server, you must also install the CA ARCserve Backup Central Management Option.

The following sections describe how you can use CA ARCserve Backup, along with the Central Management Option, to manage your daily activities.

Central Management

The Central Management Option allows you to manage one or more ARCserve servers through a single central system. Within an ARCserve domain, this central system is called the primary server and the other (subordinate) servers are called member servers.



Primary Server

A primary server provides you with a single point to manage the primary server and one or multiple member servers in an ARCserve domain. From the primary server you can centrally manage and monitor jobs that run locally on that primary server and jobs that run remotely on one or more of the member servers in the domain. There can be only one primary server within an ARCserve domain.

Note: You can designate any CA ARCserve Backup server as the primary server. However, because the primary server is responsible for managing and initializing the shared member servers, you should use your most reliable server as the primary server.

Member Server

A member server executes jobs that are dispatched from the primary server. Within an ARCserve domain, member servers can only belong to one primary server.

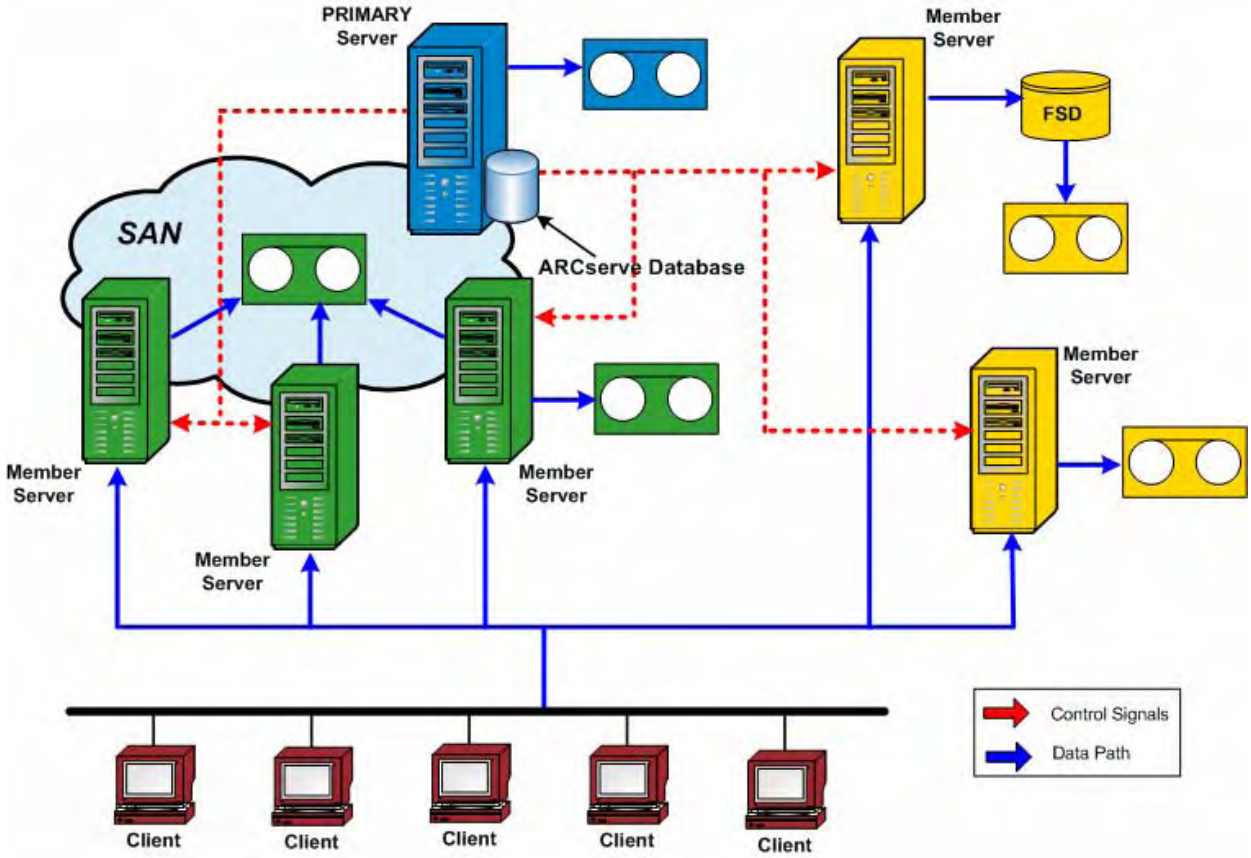
ARCserve Domain

An ARCserve domain is a logical grouping of a primary and one or more member servers that allows easier monitoring and managing of CA ARCserve Backup servers and users. Within an ARCserve domain, there can only be one primary server and there can be multiple member servers that are controlled by the primary server. An ARCserve domain allows you to manage the domain and select any server from within the domain to perform CA ARCserve Backup tasks without being required to log in to each server separately.

The ARCserve database (ASDB) can be installed on a primary server or on any remote system in your environment. Be aware that to install the ASDB on a remote system, you must host the ASDB instance using Microsoft SQL Server.

The primary and member servers may or may not be connected through a Storage Area Network (SAN). If the member servers are located on a SAN, the primary server must also be on the SAN.

Note: A SAN environment within an ARCserve domain is an environment where multiple ARCserve servers can share one or more devices (for example, tape libraries).

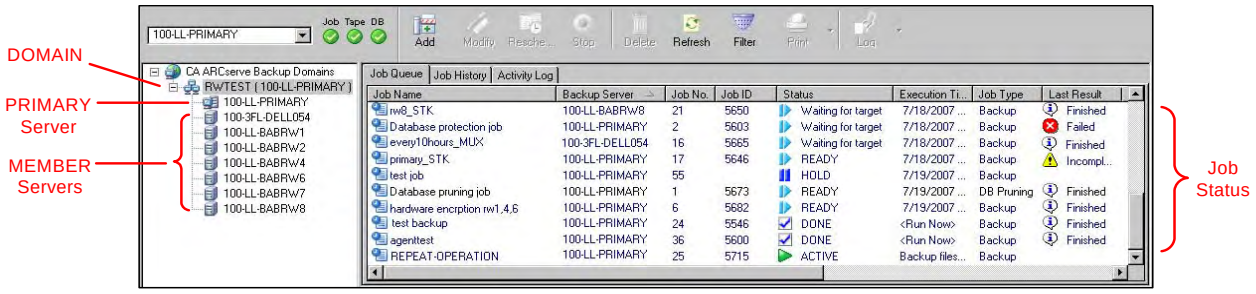


Central Job Management

Central job management allows you to create, manage, and monitor CA ARCserve Backup jobs from one central location. Jobs are always submitted on the primary server and can be run either locally on the primary server itself or remotely on any of the associated member servers. With central job management, you can perform job management operations (for example, backup, restore, merge, scan, data migration, tape copy, compare, copy, count, and so on) on all ARCserve servers from the primary server.

All jobs that are scheduled to run on any ARCserve server in the domain will be submitted to the central job queue. This allows you to monitor the job status of all jobs in the domain from the primary server.

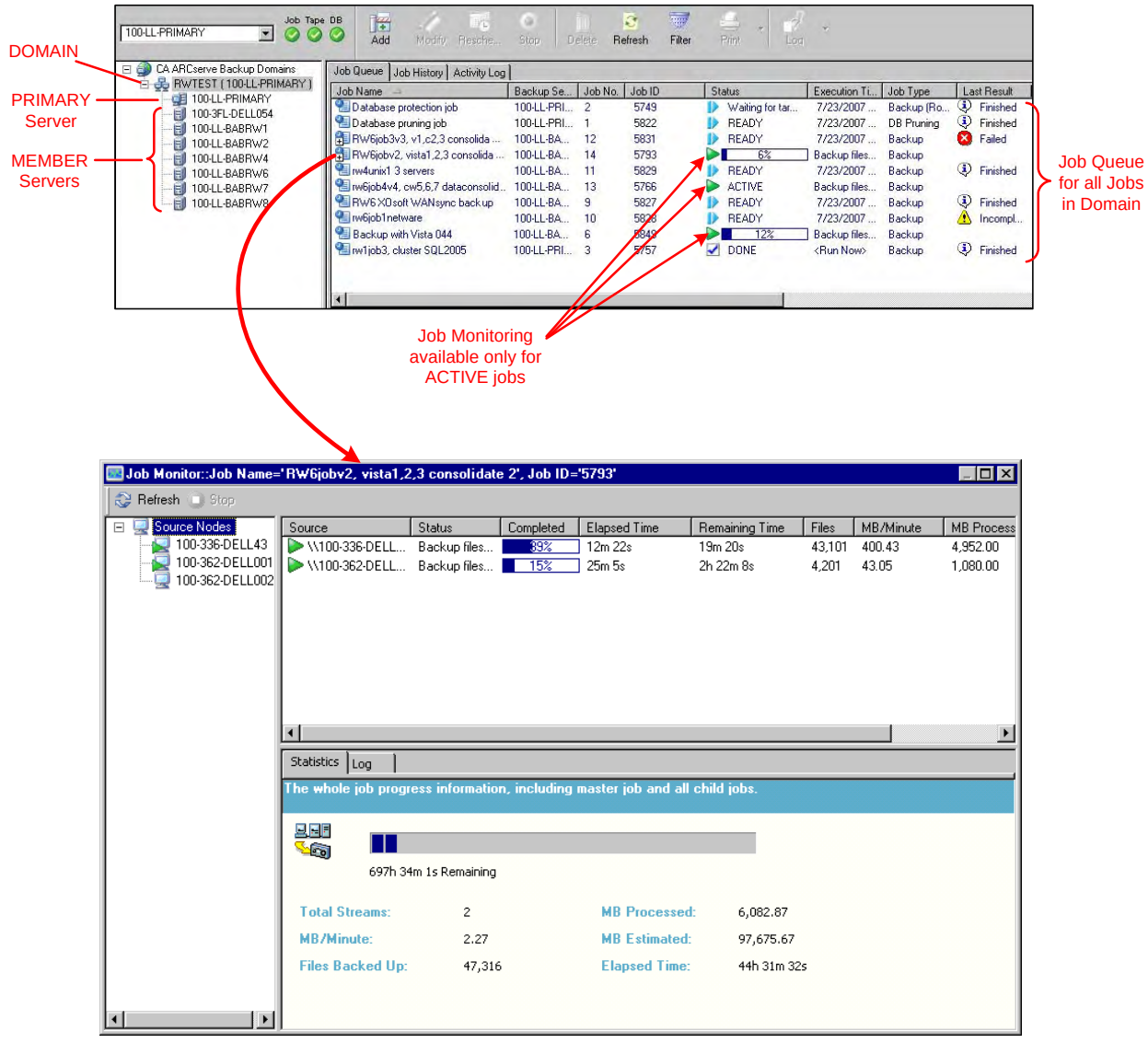
To view jobs running from the Primary Server, select the Primary Server. To view jobs running from a Member Server, select the Member Server.



Central Job Monitoring

Central job monitoring allows you to monitor the progress of all jobs running on any ARCserve server in a domain from the primary server. From the primary server job queue, you can view the real-time status of active jobs within the domain.

Note: Job monitoring is only available for active (running) jobs within the domain. When the job completes, the final status of any job that ran in the domain is displayed in the Job Status Manager.



Central Database Management

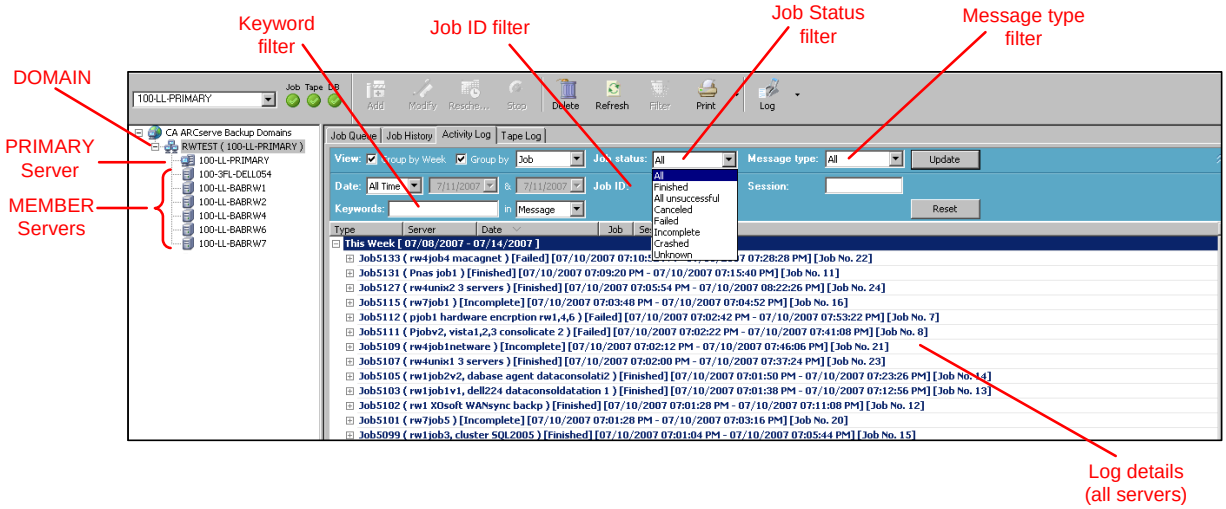
Information from all ARCserve servers within a domain is stored in a single central database that can be managed by the primary server. The central database is configured from the primary server and the associated member servers write relevant information into the central database.

Whenever CA ARCserve Backup performs a backup, all the job, session, and media information from the ARCserve servers is stored in the centralized database. In addition to the database, a central catalog file is also created that contains descriptive information about each session and allows you to select the specific files and directories to be restored without having to query the database itself. The catalog files have been restructured so that they no longer need to be merged into the database to be efficiently searched. When data needs to be restored, CA ARCserve Backup can quickly browse the content of each session in the catalog file from a single central location to locate the information.

Central Logging

With central logging, Activity Logs and Job Logs for all ARCserve servers in a domain (primary and members) are stored in a central database, allowing you to view the logs from one central location.

Central logging also helps you to perform troubleshooting. You can use the various filters (such as Keywords, Job ID, Job status, Message type, and so on) to isolate the log information to display everything that happened for a specific condition. For example, you can specify to only display the logs for failed jobs, or only display logs that contain a certain keyword in a message or job name, or only display logs for certain job names. Central logging allows you to perform these functions for all ARCserve servers within a domain from one central location.



Central Reporting

With central reporting, you can launch and create scheduled reports for all ARCserve servers in a domain from the primary server. Different reports are generated based on the backup activity stored in the CA ARCserve Backup database. Central reporting provides the capability to preview a report, print a report, send email, and schedule when to generate a report for all domain servers from the primary server.

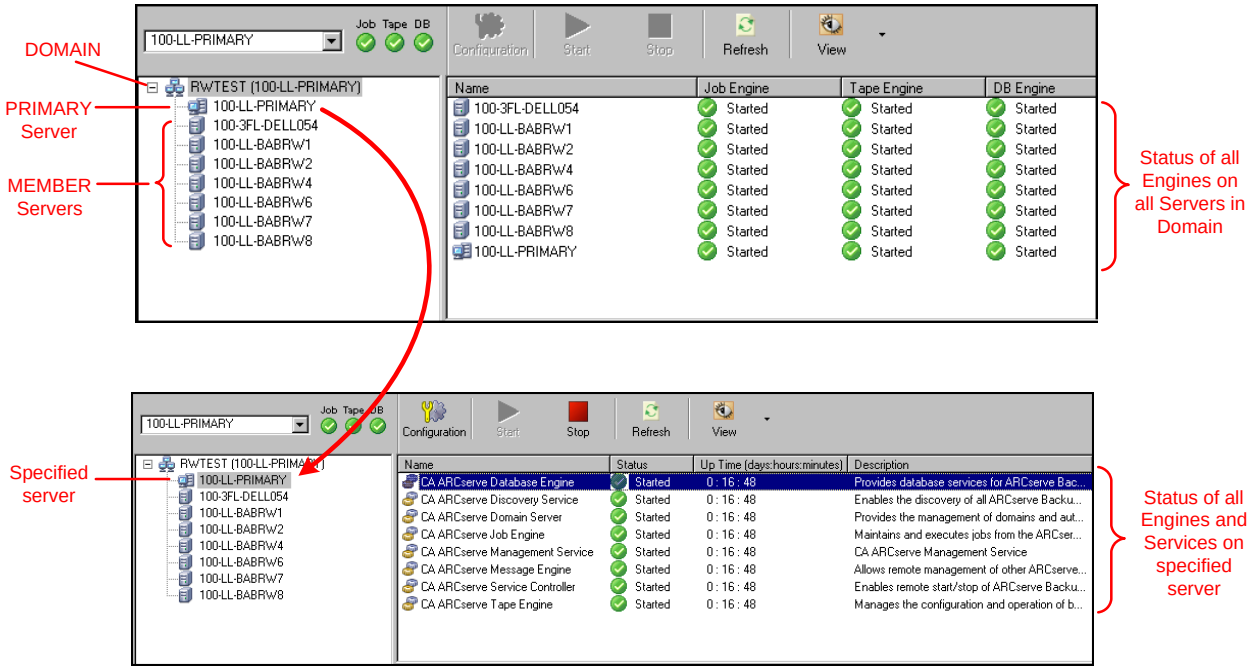
For example, from the primary server you can create a report that identifies the agents that failed the most consecutive times, or the agents with the most failed backup attempts, or the agents with the most partial backups. You can find the percentage of successful, incomplete, or failed backup attempts. You can also find the number of errors and warnings generated for the backup job for each agent which helps in determining the agents with most number of errors.

Central Alert Management

With central alerting, alerts are posted from all CA ARCserve Backup servers in a domain to the primary server. Job level alerts are configured on the primary server and applied to all jobs that are executed on the primary server or any of the associated member servers within the domain.

Central ARCserve Server Administration

Server administration tasks for all ARCserve servers in a domain are performed centrally from the primary server. From the primary server, you can monitor the state of the CA ARCserve Backup engines (Job Engine, Tape Engine, and Database Engine) for all ARCserve servers in the domain. In addition, you can select an individual server to monitor and manage the state of the engines and services on that server.



Central Device Management

With central device management, you can manage devices for all ARCserve servers in a domain from the primary server by using the Device Manager. The Device Manager provides information about storage devices that are connected to a server, the media in these devices, and the status of these devices. In addition, the Device Manager also allows you to format, erase, inventory, import, and export media. With central device management, all of these functions can be performed from the primary server for devices connected to the primary server or any of the associated member servers.

Tape Library Auto-Configuration

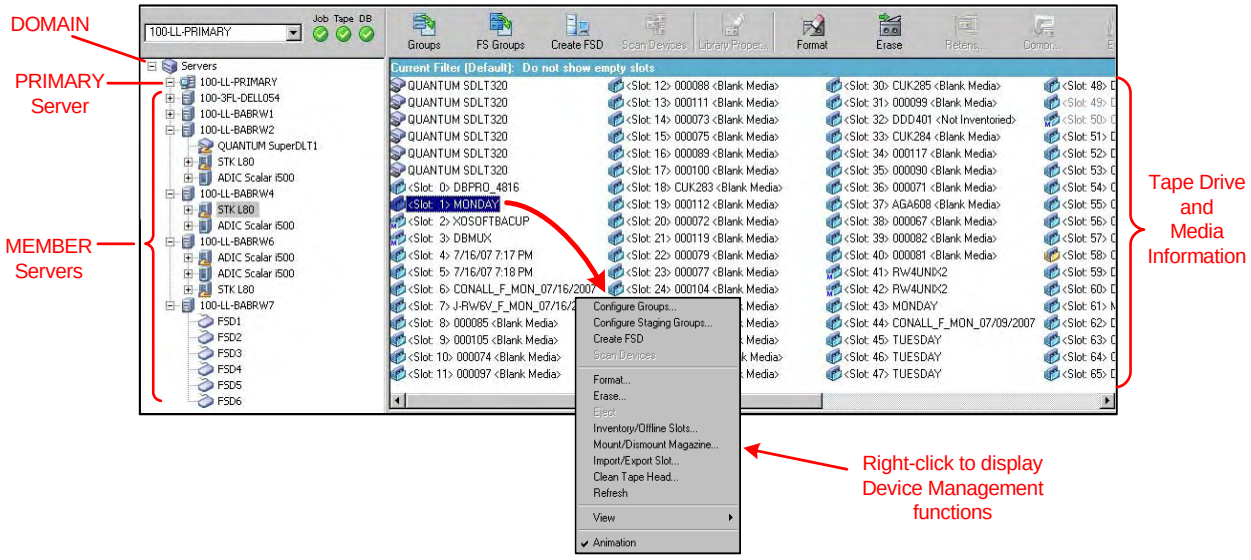
CA ARCserve Backup will now automatically detect the existence of a tape library and configure it. Therefore you no longer need to run the separate Tape Library Option Setup utility and no longer need to reconfigure a library after replacing bad drives or adding new drives. In addition, library settings can be changed on the fly without stopping the Tape Engine for such tasks as cleaning tapes or specifying cleaning settings.

SAN Auto-Configuration

SAN configuration is now tied to CA ARCserve Backup domain configuration, eliminating the need to run SAN configuration. Libraries are automatically detected as “shared” on the fly at the CA ARCserve Backup domain primary server. Domain primary servers can have both SAN and non-SAN domain member servers.

FSD Auto-Configuration

From a central location on the primary server you can create an FSD on any member server without having to stop and start the tape engine.



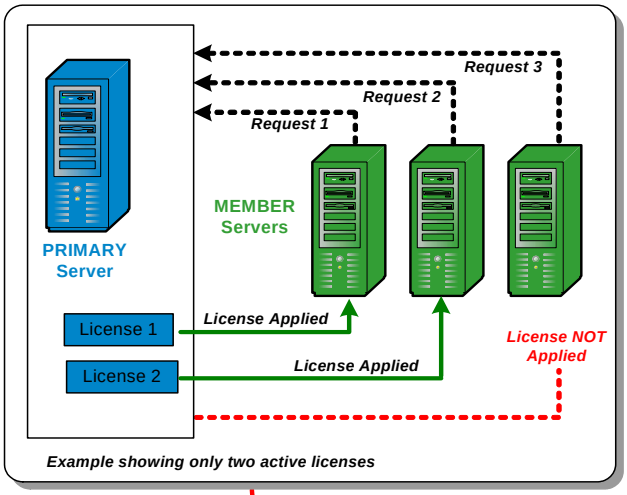
Central License Management

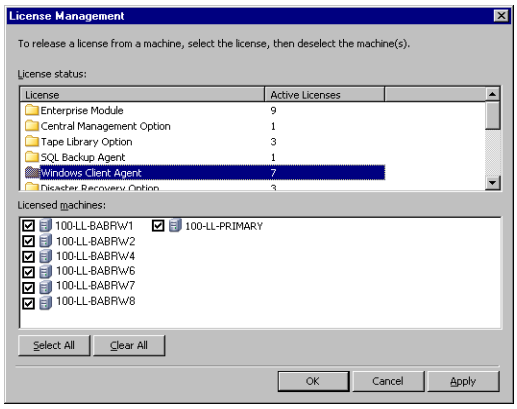
CA ARCserve Backup licensing is count-based with licenses for most ARCserve servers within a domain applied centrally on the primary server. Count-based licensing grants a single overall license to the application with a predetermined number of active license rights included in the overall license pool.

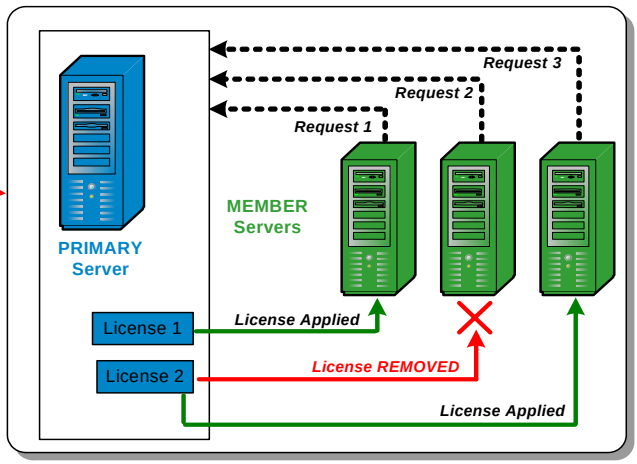
Each new user of the application (member server) is granted an active license from the pool on a first-come, first-served basis until the total number of available licenses has been exhausted. If all the active licenses have already been applied and you need to add a license to a different member server, you would first have to manually remove the license from one of the member servers (to reduce the count) and then have the new member server apply for that license (to take up the count).

With central license management, the license allocation is server based. This means that when a license is allocated to a server, central license management will record this allocation and keep this license exclusively used for that server. Future license requests from the same server will always succeed, and requests from other servers will cause a new license to be allocated to the new server. When all available licenses are allocated, license checking places jobs that are running from an ARCserve Member server into a Hold status, and fails jobs associated with a server that is running an ARCserve agent. For all scenarios, when there are no licenses available, you will get an activity log message warning you that the license is a problem.

Through the use of central licensing, you can easily remove license rights to allow other member servers to gain license privileges. From the Server Admin Manager screen on the primary server, you can access the License Management dialog to view the active license counts for each component and also manage which licenses are applied to which servers.







CA ARCserve Backup licenses are installed on and checked centrally on the CA ARCserve Backup primary server. However, the following agents must be licensed on the servers where you are installing the agents:

- CA ARCserve Backup for Windows Agent for Open Files
- CA ARCserve Backup for Windows Agent for Oracle
- CA ARCserve Backup for Windows Agent for Sybase
- CA ARCserve Backup for Windows Agent for Informix
- CA ARCserve Backup for Windows Agent for Lotus Domino
- CA ARCserve Backup for Windows Enterprise Option for SAP R/3 for Oracle

More information:

Manage CA ARCserve Backup Component Licenses (see page 329)
Release Licenses from Servers (see page 332)

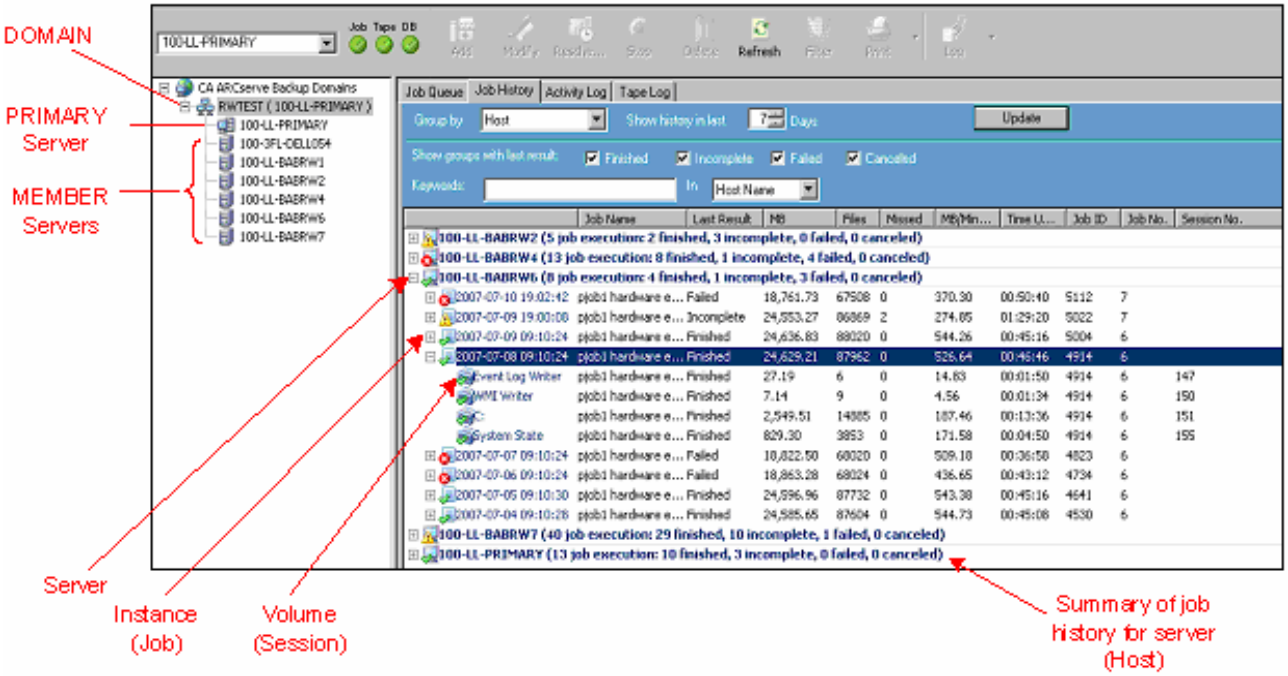
Central Job History

With central job history, you can view the history of backup jobs on all ARCserve servers within a domain from the primary server. You can view the history based upon either the applicable host or the job itself.

Through central job history, you can locate and review the status of the ARCserve servers that were backed up, the instances (or jobs) for each server, and the volumes (or sessions) for each instance.

You can also view information about the device and the media that were used for the backup job. In addition, central job history is helpful in troubleshooting because any errors or warnings that were generated during each job on any server (primary or member) are also displayed from one central location.

Note: On the Job History tab, the MB/Minute field displays the ratio of megabytes per minute for the entire job. In addition to transferring data from the source location to the destination storage area, a job can include media management activities, pre- and post- scripts, and so on. As a result, the value displayed in the MB/Minute field can be different than the actual throughput. To view the actual throughput for the job, click the Activity Log tab, locate the job, expand Logs for the Master Job, and locate the log entry for Average Throughput.



Appendix B: Troubleshooting Your Installation

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

This section contains the following topics:

Unable to Log In to the CA ARCserve Backup Manager Console

Valid on Windows

Symptom:

I installed CA ARCserve Backup, but I cannot log in to the CA ARCserve Backup Manager Console. Am I doing something wrong?

Solution:

The services responsible for authenticating users may not be running. From the Control Panel, go to the Service Panel and see if the CA ARCserve Backup Domain Server, CA ARCserve Backup Service Controller, and CA Remote Procedure Call Server services are running. 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

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 portsconfig.cfg file in the Shared Components\BrightStor directory.

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.

Unable to Determine What Devices Are Supported by CA ARCserve Backup

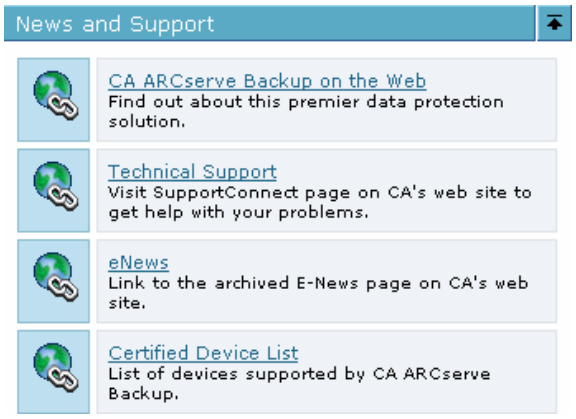
Valid on Windows

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 Certified Device List link under News and Support, as shown in the following illustration:



More information:

CA ARCserve Backup Home Page (see page 141)

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

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm.

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

J

L

M

N

O

P

R

S

T

U