

CA ARCserve® Backup for Windows

Administration Guide

r12.5



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

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

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

Copyright © 2009 CA. All rights reserved.

CA Product References

This document references the following CA documentation sets:

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

- 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 Dynam®/B Backup for z/VM
- CA VM: Tape for z/VM
- CA XOssoft™ Assured Recovery™
- CA XOssoft™
- CA 1® Tape Management
- Common Services™
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM: Operator®

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At <http://ca.com/support>, you can access the following:

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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short [customer survey](#), which is also available on the CA support website, found at <http://ca.com/support>.

Documentation Changes

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

- Added an appendix titled Using Deduplication--Describes how deduplication works, and how to back up data and restore data using deduplication.
- [How Password Management Works](#) (see page 75)--Describes how password management works and how to manage jobs using session and encryption passwords.
- Added the following topics that relate to User Profile Management:
 - [How User Profile Management Works](#) (see page 77)--Describes how user profile management works.
 - [Roles and Permissions](#) (see page 79)--Describes roles and tasks associated with specific types of CA ARCserve Backup user profiles.
 - [Using the Audit Log](#) (see page 96)--Describes the tasks you can perform to audit CA ARCserve Backup user profiles.
- [CA ARCserve Backup Enterprise Module](#) (see page 39)--Updated the description of the CA ARCserve Backup Enterprise Module.
- [Submit a Backup Job](#) (see page 129)--Updated the procedure that describes how to submit a backup job.
- [Backup Manager Backup Media Options](#) (see page 150)--Updated the descriptions of various Backup Media options; either for clarity or updated functionality.
- [Backup Manager Operation Options](#) (see page 155)--Updated the descriptions of various Backup Operation options; either for clarity or updated functionality.
- [Backup Manager Pre/Post Options](#) (see page 160)--Updated the descriptions of various Pre/Post options; either for clarity or updated functionality.
- [Backup Manager Agent Options](#) (see page 162)--Describes options that you can specify to protect virtual machines (VMs) and Microsoft SQL Server databases.
- [Back Up an Entire Node](#) (see page 186)--Updated the procedure that describes how to back up an entire node that contains database files.
- [Configure Device Groups to Use Staging](#) (see page 201)--Updated the description of the Purge to Threshold option.
- [Specify Miscellaneous Options for Disk Staging Backups](#) (see page 208)--Updated the description of various Miscellaneous Staging Backup policies.

- [Back Up Data Using Disk Staging](#) (see page 215)--Updated the procedure that describes how to submit a backup job using the staging option.
- [Back Up Data Using Tape Staging](#) (see page 230)--Updated the procedure that describes how to submit a backup job using tape staging (B2T2T).
- [How to Add, Import, and Export Nodes](#) (see page 315)--Updated the procedure that describes how to simplify the process of setting up a CA ARCserve Backup environment that consists of a large number of nodes and agents.
- [Deduplication Device Management](#) (see page 341)--Describes tasks that you can perform to manage deduplication devices and deduplication device groups.
- [Online and Offline Drives](#) (see page 361)--Describes how to status library drives as offline or online from the Device Manager.
- [Media Assure](#) (see page 394)--Describes the Media Assure option, which helps you ensure that the sessions on the media are restorable. The Media Assure option can be accessed from the Media Assure & Scan utility.
- [How CA ARCserve Backup Records Events in the Windows Event Viewer](#) (see page 467)--Describes the information that CA ARCserve Backup records in Windows Event Viewer.
- [Reconfigure Node Tier Assignments](#) (see page 479)--Describes how to use CA ARCserve Backup to classify nodes based on their level of importance to your environment.
- [Restore the CA ARCserve Backup Job Queue](#) (see page 506)--Describes how to restore the CA ARCserve Backup Job Queue in the event it becomes damaged or is deleted in error.
- [Demote a Primary Server to a Member Server](#) (see page 522)--Updated the procedure that describes how to demote a primary server to a stand-alone server. Database migration scenarios are described in the topic.
- [Install and Uninstall CA ARCserve Backup Server Based Options](#) (see page 527)--Updated the procedure that describes how to install options using the Server Admin. You must now uninstall the Agent for Virtual Machines using Windows Add or Remove Programs.
- [CA ARCserve Backup Agent Deployment](#) (see page 528)--Describes how to deploy agents to multiple remote hosts using a wizard-like application called Agent Deployment.
- [Restore the CA ARCserve Backup Database \(Different Domain\)](#) (see page 587), [Restore the CA ARCserve Backup Database \(Same Domain\)](#) (see page 590), and [Restore the ARCserve Database Using the ca_recoverdb Command](#) (see page 593)--Added information that describes expected results.
- [Configure the Catalog Database](#) (see page 600)--Updated the procedure that describes how to configure the CA ARCserve Backup catalog database.

- [Move the CA ARCserve Backup Catalog Database to a Different Location](#) (see page 602)--Describes when and how to move the CA ARCserve Backup catalog database to a different location in your backup environment.
- [Manage a Different CA ARCserve Backup Server](#) (see page 781)--Describes how to manage multiple CA ARCserve Backup servers via the Microsoft EBS Administration console.

Contents

Chapter 1: Introducing CA ARCserve Backup 23

Introduction	23
CA ARCserve Backup Functionality	23
CA ARCserve Backup Managers, Wizards, and Utilities	25
CA ARCserve Backup Utilities	28
CA ARCserve Backup Command Line Utilities	35
CA ARCserve Backup Security	35
Enterprise Level Password Management Utility	38
How Centralized Cross-platform Management Works	38
CA ARCserve Backup Enterprise Module	39
How to Protect Virtual Machine Environments	40
How Backup and Restore Operations Function on 64-bit Windows Platforms	40

Chapter 2: Protecting Data Using CA ARCserve Backup 43

CA ARCserve Backup Components	44
Open the Manager or Manager Console	44
Central Management	45
Central Job Management	48
Central Job Monitoring	49
Central Database Management	50
Central Logging	50
Central Reporting	51
Central Alert Management	52
Central ARCserve Server Administration	52
Central Device Management	52
Central License Management	54
Central Job History	56
Locate Information Using Quick Search	72
How Password Management Works	75
Change a Session/Encryption Password	76
Enable Password Management	77
How User Profile Management Works	77
Roles and Permissions	79
Windows User Authentication	86
Configure Windows Security Setting Option	87
Log in to CA ARCserve Backup	87
Add a Windows User	89

Add a CA ARCserve Backup User	90
Change Your Password From the Home Page GUI	91
Modify Windows User Properties	92
Modify CA ARCserve Backup User Properties	93
Delete a User	94
Add a User to a Role	95
Remove a User from a Role	96
Using the Audit Log	96
Create an Audit Log Report	100
Data Security	101
Encryption and Decryption	101
Federal Information Processing Standards (FIPS)	102
CA ARCserve Backup and FIPS Compliance	102
CA ARCserve Backup Data Encryption	103
How You Manage Media	108
Configure Devices Using the Device Wizard	108
Configure a Device Group	109
Back Up and Restore Data	111
Backup Requirements Plan	111
Add Computers to the Preferred Shares/Machines Tree	112
Backup Media Rotations and Scheduling Options	112
Rotation Schemes	113
Media Pools	113
Create Media Pools	116
Wizards	116
GFS Rotations	120

Chapter 3: Backing Up Data **125**

How You Can Back Up Data	125
Specify Local Backup Options	126
Submit a Backup Job	129
Backup Manager	130
Specify the Source	131
How CA ARCserve Backup Lets You Browse a Large Number of Items in the Backup Manager	133
Backup Manager Considerations on 64-bit Windows Platforms	135
Options You Can Specify on the Backup Manager Destination Tab	136
Backup Job Schedules and Rotations	137
Local Backup Options for UNIX Agents	139
Global Backup Options	140
Backup Manager Alert Options	141
Backup Manager Media Exporting Options	143

Backup Manager Advanced Options	143
Backup Manager Encryption/Compression Options	146
Backup Manager Volume Shadow Copy Service Options	148
Backup Manager Backup Media Options	150
Backup Manager Verification Options	152
Backup Manager Retry Options	153
Backup Manager Operation Options	155
Backup Manager Pre/Post Options	160
Backup Manager Agent Options	162
Backup Manager Job Log Options	172
Backup Manager Virus Options	172
Files and Objects that CA ARCserve Backup Does Not Back Up	173
Enable CA ARCserve Backup to Manage Open Files on Remote Computers	175
How Multistreaming Processes Backup Data	176
Specify Multistreaming Options	178
How Multiplexing Processes Backup Data	178
Functions Supported by Multiplexing	181
Multiplexing Job Options	182
Preflight Checks for Your Backups	184
Entire Node Backups	185
Back Up an Entire Node	186
Create Repeating Backup Jobs	188
Back Up Remote Servers	189
Backup Staging Methods	190
How to License the Disk to Disk to Tape Option	191
How Backup to Disk to Tape Works	191
How to Manage Backup Data Using Tape Staging	223
Disaster Recovery	236
Back Up BrightStor ARCserve Backup for Laptops & Desktops Data	236
Migrated Files Management	237

Chapter 4: Restoring Data **239**

Restore Manager	239
How to Find Files That You Want to Restore	241
How CA ARCserve Backup Lets You Browse a Large Number of Items in the Restore Manager	244
Restore Manager Considerations on 64-bit Windows Platforms	247
Version History	247
Duplicate Backup Sessions	248
Smart Restore	248
Restore Data by Query on UNIX and Linux Platforms	249
Restore Manager Markers	250

Restore Manager Location Options	252
Restore Job Schedules	252
Specify Run as Administrator on Windows Server 2008 Systems	253
Global Restore Options	254
Restore Manager Backup Media Options	254
Restore Manager Destination Options.....	255
Restore Manager Operation Options	258
Restore Manager Pre/Post Options	260
Restore Manager Job Log Options	261
Restore Manager Virus Options	261
Restore Manager Alert Options	262
System State Restore Options	263
Restoring Data Scenarios.....	264
Restore Data Backed Up Using Staging	264
Restore a Remote Agent on a System without the Disaster Recovery Option	266
Restore CA ARCserve Backup Member Servers without the Using the Disaster Recovery Option	267
Best Practices - How to Recover a Stand-alone Server from a Disaster Using the Disaster Recovery Option	269
Best Practices - How to Recover a CA ARCserve Backup Server from a Disaster Without Using the Disaster Recovery Option	271
Restore BrightStor ARCserve Backup for Laptops & Desktops Data	282
Restore Migrated Files	283

Chapter 5: Customizing Jobs 285

How You Can Customize Jobs	285
Dynamic Job Packaging	286
Explicit Job Packaging	286
Rotation Schemes	287
How You Can Manage GFS Rotation Jobs on File System Devices	288
Media Pool Specification	291
Backup Method Options	291
How Job Filters Work	291
Filter Options	294
Types of Filters	294
Schedule Custom Jobs	296
Custom Schedules	297
Tasks You Can Perform Using the Job Status Manager	298
Modify Pending Data Migration Jobs	299
Update Multiple Jobs	301
How to Manage Jobs Using the Job Queue Tab	302
View Job Details Using the Activity Log	310

Tape Log Tab	314
Job Detail Tab	314
Job Log Tab	314
How Save Node Information Works	315
How to Add, Import, and Export Nodes	315
Add, Import, and Export Nodes Using the User Interface.....	316
Add Multiple Nodes and Agents Using a .csv and .txt File	319
Export Multiple Machines to a Text File	320
Filter Nodes	321
Modify a Node	321
Delete a Node	322
How to Use the Job Scheduler Wizard to Schedule Jobs.....	322
Job Scripts	323
Create a Job Script	323
Execute a Job Using a Script	324
Job Templates	324
Create Custom Job Templates	325
Windows-Powered NAS and Storage Server 2003 Device Configuration	325
Access CA ARCserve Backup Through the Windows-powered NAS Device	326
CA ARCserve Backup and Windows-powered NAS Device Configuration	326

Chapter 6: Managing Devices and Media 329

Device Management Tools	329
Tape Library Configuration.....	329
RAID Device Configuration Option	334
Virtual Library Configuration Option	335
Control Devices Using Removable Storage Management	336
How to Create File System Devices	337
Configure Devices Using Enterprise Module Configuration	339
Deduplication Device Management	341
Device Manager	355
Maintenance Tasks	356
Schedule Device Management Jobs.....	364
Device Management Functions for Libraries	364
Identify a Library as a VTL.....	379
Media Movement	381
Device Group Configuration Using the Device Manager	381
Universal Serial Bus (USB) Storage Devices.....	386
Prerequisites for Backing Up to Removable Drives	387
Filter Libraries	388
Removable Drive Support.....	389
Write Once Read Many (WORM) Support.....	389

Device Group Configuration	391
DLTSage Error Handling	391
How CA ARCserve Backup Cures Tape Drive Errors	392
How to Ensure that CA ARCserve Backup Spans Media in a Single Drive Autoloader	393
Media Assure	394
How Uninterrupted Drive Cleaning Works	395
How to Optimize Tape Usage	396
Media Maximization	396
Consolidation During Migration	397
How Media Pools Work	401
Save Sets and Scratch Sets	403
Serial Numbers	404
GFS Media Pools	405
Media Maximization in GFS Rotation Jobs	407
Media Pool Manager	411
How You Can Create a Rotation	412
Media Management Administrator (MM Admin)	413
Media Management and Tape Service	413
Media Management Administrator Terms	413
MM Admin Interface	414
MM Admin Toolbar	415
MM Admin Window	415
Schedule Object	416
Reports Object	418
Find Media in Vault Object	420
Status Object	420
Reset the Status of Vault Processing	420
How the Media Management Process Works	421
Vault Management	422
Create a Schedule	424
Delete a Tape Volume Movement Schedule	425
How You Can Manage Tape Volumes and VCDs	425
Tape Volume Retention Policies	427
Slot Detail and Status Information	430
Find Specific Media in a Vault	432

Chapter 7: Administering the Backup Server **433**

How CA ARCserve Backup Engines Work	433
How Engine Status Affects CA ARCserve Backup Operations	434
Service State Icons	435
Stopping and Starting CA ARCserve Backup Services	435
CA Antivirus Maintenance	441

Configure CA ARCserve Backup Engines	450
Job Engine Configuration	451
CA ARCserve Backup Services, Components, and Applications that Require the Highest Available Privileges	454
Tape Engine Configuration	462
Database Engine Configuration	472
Alert Configuration	476
Additional Server Admin Functions	478
Change or Modify the CA ARCserve Backup System Account	478
Reconfigure Node Tier Assignments	479
Manage CA ARCserve Backup Component Licenses	481
Release Licenses from Servers	483
Configure Multiple Network Interface Cards	483
Authentication Levels for CA ARCserve Backup Services, Components, and Applications	484
CA ARCserve Backup Services, Components, and Applications that Require Administrative Privileges	485
CA ARCserve Backup Domains	490
Manage Domain Users and Groups Using the ca_auth Command Line Utility	491
Create caroot Equivalence	491
How to Process Computer Name Changes in an ARCserve Domain	494
Re-initialize the CA ARCserve Backup Database	504
Restore the CA ARCserve Backup Job Queue	506
Manage ARCserve Servers Using the Server Configuration Wizard	509
Tasks You Can Perform Using the Server Configuration Wizard	511
Data Migration Limitations in a CA ARCserve Backup Domain	512
Start the Server Configuration Wizard	514
Promote a Member Server to a Primary Server	515
Demote a Primary Server or Stand-alone Server to a Member Server	518
Move a Member Server to a Different CA ARCserve Backup Domain	522
Change the Password for the CA ARCserve Backup Domain Administrator (caroot) Account ...	522
Repair the CA ARCserve Backup Configuration	523
Repair the ARCserve Database Connection on a Primary Server	525
Repair the ARCserve Database Connection on a Member Server	526
Install and Uninstall CA ARCserve Backup Server Based Options	527
CA ARCserve Backup Agent Deployment	528
Deploy Agents to Remote Hosts Using Automatic Upgrade	532
Deploy Agents to Remote Hosts Using Custom Deployment	535
Deploy Agents to VMs Using Virtual Machine Deployment	538
Discovery Configuration	541
How the Discovery Service Detects Other Computers	542
IP Subnets/Windows Domains Discovery	544
Enable Discovery Using TCP/IP Subnet Sweep	545
Discovery Configuration for the SAN Option	548

Discover Client Agent Systems with Non-default IP Addresses	548
Allow CA ARCserve Backup Services and Applications to Communicate Through the Windows Firewall	549
How to Configure Your Firewall to Optimize Communication	549

Chapter 8: Managing the Database and Reporting **551**

How to Manage the Database and Reports	551
Database Manager	552
Database Views	552
Enable Media Pool Maintenance	555
How to Protect the CA ARCserve Backup Database	555
Agent for ARCserve Database	556
How the Database Protection Job Works	560
How to Back Up the CA ARCserve Backup Database	561
Modify, Create, and Submit a Custom Database Protection Job	562
Specify Microsoft SQL Server 2005 Express Backup Options	565
Specify Microsoft SQL Server Backup Options	567
Start the CA ARCserve Backup Database Protection Job	571
Delete the CA ARCserve Backup Database Protection Job	572
Recreate the CA ARCserve Backup Database Protection Job	573
How to Restore the CA ARCserve Backup Database	574
Open the Agent Restore Options Dialog	576
Restore the CA ARCserve Backup Database (Different Domain)	587
Restore the CA ARCserve Backup Database (Same Domain)	590
How to Recover the ARCserve Database When the SQL Server Instance Hosting the ARCserve Database is Not Functional	593
Restore the CA ARCserve Backup Database Using the ca_recoverdb Command	593
How the Catalog Database Works	597
Catalog Browsing	599
Catalog Database Pruning	599
How a Centralized Catalog Database Works	600
Configure the Catalog Database	600
Move the CA ARCserve Backup Catalog Database to a Different Location	602
Using Microsoft SQL Server as the CA ARCserve Backup Database	605
Microsoft SQL Server Database Considerations	605
Remote Database Considerations	607
Specify ODBC Communication for Remote Database Configurations	608
How to Calculate the Number of Required SQL Connections	608
How to Enable TCP/IP Communication on Microsoft SQL Server Databases	609
Database Consistency Checks	609
Specify a CA ARCserve Backup Database Application	609
Configure Microsoft SQL Server as the CA ARCserve Backup Database	610

Move the CA ARCserve Backup Database to a Different System or Instance	613
Configure Microsoft SQL Server 2005 Express as the CA ARCserve Backup Database	616
CA ARCserve Backup Logs and Reports	617
Activity Log Data	617
Tape Log	617
Job Log	618
Report Manager	618
Report Manager Reports	620
Custom Report Job Scheduling	628
Create Custom Reports Using the Report Writer Utility	629
Report Generation for Multiple CA ARCserve Backup Servers	631
Run a Session Details Report for ARCserve Backup for Laptops & Desktops	631
Monitor Activity Using the Unicenter Monitoring Agent	631
CA ARCserve Backup Diagnostic Utility	632
Diagnostic Utility Components	632
Create a Report Using the Express Mode Diagnostic Utility	633
Create a Report Using the Advanced Mode Diagnostic Utility	635
View a Report Using the Diagnostic Report Manager	636

Chapter 9: Using the Alert Manager **639**

How the Alert Manager Works	639
Alert Manager Components	641
Set Up Alerts	641
Alert Manager Configuration	643
Ports Option	643
Broadcast Alerts	644
CA Unicenter TNG	644
Email Notification	646
Windows Event Log Notification	647
Alert Manager Pager Options	648
SMTP Notification	649
SNMP Notification	649
Trouble Tickets	650
Event Priorities	650
Message Testing	650
Alert Activity Details	651

Appendix A: Troubleshooting **653**

Log in Problems	653
Unable to Log In After Changing the caroot Password	653
Makeup Jobs Created When the Media is Full	654

Unable to Log In to CA ARCserve Backup After Changing the Computer Name.....	655
CA ARCserve Backup Cannot Communicate after Changing the IP Address of a CA ARCserve Backup Server	656
Authentication Errors Occur When Stopping and Starting the CAportmapper Service.....	660
Jobs Do Not Start on Schedule.....	661
Hardware Does Not Function as Expected	661
CA ARCserve Backup Does Not Detect a Cleaning Tape	663
CA ARCserve Backup Cannot Detect RSM Controlled Devices on x64 Platforms	664
Authentication Problems.....	664
Authentication Security Settings	664
Restricted Users Cannot Access the Activity Log and the Audit Log	666
Cannot Back Up Open Files	668
Tape Errors Occur When Backing Up or Restoring Data	670
Copy the Data to a New Tape	671
Create a New Backup Tape	671
Discovery Service Does Not Function Properly	671
GUI Freezes in Active Directory Restore Mode	672
Restore Job Fails on Citrix Server	672
Local Restore Data Backed Up with Compression and/or Encryption Failed	673

Appendix B: Using Deduplication **675**

How Data Deduplication Works	676
How to Plan a Deduplication Installation	678
Deduplication Considerations	679
Supported Functions Matrix	680
Licensing Requirements for Deduplication.....	681
How to Configure Your Implementation for Deduplication.....	681
Deduplication Device Group Configuration	683
Device Commands for Data Deduplication Devices	683
Backup Data with Deduplication	683
How Regular Backup Jobs Work with Deduplication	684
How Staging Jobs Work with Deduplication	684
How to Back Up Deduplication Devices	689
Global Deduplication	694
Recover Deduplicated Data	695
Restore Deduplicated Data.....	695
Scan Jobs with Deduplication	698
Merge Jobs with Deduplication	699
GFS Rotation Jobs on Deduplication Devices	699
Deduplication Device Purge	699
Deduplication Reports	700

Appendix C: Using CA ARCserve Backup in a Storage Area Network 701

How to License the Storage Area Network (SAN) Option	701
The SAN Environment	702
How the Option Works	703
Server Management	704
Backup Plans	704
Benefits of Using the Option	705
Terminology	705
Installing the SAN Option	705
Operating System Compatibility	706
Installation Prerequisites	706
SAN Option Installation	707
Using the SAN Option	709
Create Shared Device Groups	709
Data Backup and Restore in a SAN Environment	711
Device Management	712
Media Management	712
Control of Job Runtime	713
Reports and Logs	713
ARCserve Virtual Libraries	714
Troubleshooting SAN Configurations	714
Devices are Not Shared	715
Devices are Not Shared and the Tape Engine is Running	715
Shared Devices Appear as Unavailable or Offline	716
Shared IBM Devices Appear as Unavailable or Offline	717
Backup Jobs Fail	718

Appendix D: Using CA ARCserve Backup in a Cluster-aware Environment 719

Cluster Overview	719
How Failover Works	722
Resource Group	723
Virtual Name and Virtual IP Address	723
Shared Disks	724
Mirrored Disks	725
Quorum Disks	726
Deployment Considerations	726
Protecting Your Cluster with CA ARCserve Backup	727
MSCS Protection	729
NEC CLUSTERPRO/ExpressCluster Protection	731
Deploy CA ARCserve Backup Server on MSCS	733
MSCS Hardware Requirements	733

MSCS Software Requirements	734
Plan Your CA ARCserve Backup HA Deployment	734
MSCS Cluster Resource Preparation	736
Installation of CA ARCserve Backup in Each MSCS Cluster Node	737
CA ARCserve Backup HA Server to Support of Job Failover	737
Stop HA Service Monitoring by MSCS	739
Rebuild Cluster Resources Manually	741
Delete CA ARCserve Backup Cluster Resources	742
Manage CA ARCserve Backup Cluster Servers in a MSCS Cluster	743
Change the CA ARCserve Backup Domain in a MSCS Cluster	744
Uninstall CA ARCserve Backup from an MSCS Cluster	746
Deploy CA ARCserve Backup Server on NEC Cluster	747
NEC CLUSTERPRO/ExpressCluster Hardware Requirements	747
NEC CLUSTERPRO/ExpressCluster Software Requirements	747
Plan Your CA ARCserve Backup HA Deployment	748
NEC CLUSTERPRO/ExpressCluster Resource Preparation	750
Installation of CA ARCserve Backup in Each NEC CLUSTERPRO/ExpressCluster Node	751
CA ARCserve Backup HA Server to Support of Job Failover	756
Stop HA Service Monitoring by NEC CLUSTERPRO/ExpressCluster	757
Change the CA ARCserve Backup Domain in NEC CLUSTERPRO/ExpressCluster	758
Manage CA ARCserve Backup Cluster Servers in NEC CLUSTERPRO/ExpressCluster	760
Stop NEC Cluster Groups	761
Enable CA ARCserve Backup in NEC Cluster Scripts	762
Disable CA ARCserve Backup in NEC Cluster Scripts	765
Uninstall CA ARCserve Backup from a NEC CLUSTERPRO/ExpressCluster	768
Troubleshooting CA ARCserve Backup Cluster Support	769
Prevent Job Failures	769
Back Up MSCS Nodes on Remote Machines	770
Back Up CA ARCserve Backup Database in a Cluster Environment	771
Job Failure: Media Not Mounted	771

Appendix E: Using CA ARCserve Backup for Microsoft Windows Essential Business Server 773

CA ARCserve Backup for Microsoft Windows EBS Overview	773
Microsoft Windows EBS Overview	775
How CA ARCserve Backup Communicates with CA ARCserve Backup for Microsoft Windows EBS ..	777
Install CA ARCserve Backup for Microsoft Windows EBS	777
Uninstall CA ARCserve Backup for Microsoft Windows EBS	778
Microsoft Windows EBS Administration Console	778
Access CA ARCserve Backup for Microsoft Windows EBS	779
How to Execute Tasks Using the Administration Console	779
Troubleshooting	787

Failed to Create Equivalence	788
Equivalence was Not Created	788
Failed to Get the CA ARCserve Backup Job List	788
Failed to Parse the CA ARCserve Backup Job List	789
CA ARCserve Backup was Not Detected	789

Appendix F: Using JIS2004 Unicode Characters with CA ARCserve Backup 791

Introduction to JIS2004 Unicode Characters	791
Configuration Requirements	792
Platforms Supporting JIS2004 Unicode Characters	792
Tasks You Can Perform Using JIS2004 Unicode Characters with CA ARCserve Backup	793
CA ARCserve Backup Applications Supporting JIS2004 Unicode Characters	794
Limitations of Using JIS2004 Unicode Characters with CA ARCserve Backup	795

Index 801

Chapter 1: Introducing CA ARCserve Backup

This section contains the following topics:

[Introduction](#) (see page 23)

[CA ARCserve Backup Functionality](#) (see page 23)

Introduction

CA ARCserve Backup is a comprehensive, distributed storage management solution for distributed and multiplatform environments. The application can back up and restore data from all the machines on your network, (including machines running Windows, UNIX, NetWare, and Linux) using optional client agents. CA ARCserve Backup also provides media and device management utilities.

CA ARCserve Backup offers control from one management console. It can support small-scale and large-scale enterprise environments comprising of one machine or many, across different platforms and organizations.

CA ARCserve Backup Functionality

CA ARCserve Backup provides the components, functions, and utilities required by network managers to obtain and actively manage network backups.

Start the CA ARCserve Backup Manager by selecting the Manager icon from the program group. The My First Backup tutorial opens the first time you start the Manager. Subsequently, the Home Page appears, but you can still access the tutorial from the Help menu. From the Home Page, you can start and access any CA ARCserve Backup function using the following navigational features:

Home Page

Provides news and support that links you to tools you can use to help solve problems with your computer. It also provides links to Quick Start, Configuration, Wizards, and Utilities.

Navigation Bar

Quickly lets you independently access the Managers, Wizards, Utilities, and the most recently used screens. You can easily show or hide the Navigation Bar by selecting Navigation Bar from the View menu on the CA ARCserve Backup Home Page.

Quick Start

Provides quick links to CA ARCserve Backup Manager functions.

Configuration

Provides access to Device Configuration, which lets you quickly configure the backup devices on your server and to SAN configuration.

From the Configuration menu you can also access Device Group Configuration, which lets you configure device groups and staging groups.

Wizards

Simplifies the most common tasks of CA ARCserve Backup. You can access the Backup, Restore, Device, Create Boot Kit, Job Scheduler, and Diagnostic Wizards.

Utilities

Offers several utilities that you can use to manage your database and media. The utilities are Merge, Scan, Compare, Count, Copy, Purge, User Profile, and Report Writer.

CA ARCserve Backup Managers, Wizards, and Utilities

CA ARCserve Backup managers, wizards and utilities provide the front-end interfaces used to perform all functions necessary to protect your data. You can access these components from the Navigation Bar on the Manager Console. The following is a list of the components, the menu from which you can access the component, and the functions they perform:

Quick Start Menu

- **Job Status Manager**--Monitors all pending, completed, and active jobs from the Job Status Manager window. You can schedule pending or completed jobs, submit new jobs, delete jobs, and stop active jobs. Log information is provided for each completed job.
- **Backup Manager**--Backs up data to media. You can schedule and configure backups of your machines and servers. Information about each backup job (such as the path and name of each file, as well as the media used) is logged in the CA ARCserve Backup database. Using the Backup Manager you can:
 - Specify the source (data that you want to back up) and the destination (media) for your backup job.
 - Define your backup job to back up data on computers running other operating systems such as NetWare, UNIX, Linux, and Windows.
 - Use database agents running under Windows 2000, Windows Server 2003, and Windows XP.
- **Restore Manager**--Restores data that has already been backed up by CA ARCserve Backup. Using the Restore Manager you can:
 - Find all the versions of the files that were backed up.
 - Specify the source and destination of the restore job.
 - Define a backup method and specify a backup schedule.
 - Perform a complete or partial restore of you data.
- **Server Admin**--Allows you to modify the CA ARCserve Backup system account and manage the core CA ARCserve Backup services: Job Engine, Tape Engine, and Database Engine. The Configuration icon allows you to configure tasks for these services including generating an alert and defining message logging. The Database Engine tab allows you to configure the database pruning job.
- **Dashboard**--Provides you with a snapshot overview of your backup infrastructure and your storage resource management (SRM) environment. For more information, see the *Dashboard User Guide*.

Monitor & Reports Menu

- **Job Status Manager**--Monitors all pending, completed, and active jobs from the Job Status Manager window. You can schedule pending or completed jobs, submit new jobs, delete jobs, and stop active jobs. Log information is provided for each completed job.
- **Report Manager**--Generates reports from data in the CA ARCserve Backup database. Various reports include information about backup schedules, media errors, backup devices, media pools, and media status and policies.
- **Report Writer**--Creates custom reports or generate predefined reports based on backup activity for a defined period.
- **Dashboard**--Provides you with a snapshot overview of your backup infrastructure and your storage resource management (SRM) environment. For more information, see the *Dashboard User Guide*.

Protection & Recovery Menu

- **Backup Manager**--Backs up data to media. You can schedule and configure backups of your machines and servers. Information about each backup job (such as the path and name of each file, as well as the media used) is logged in the CA ARCserve Backup database.
- **Restore Manager**--Restores data that has already been backed up by CA ARCserve Backup.
- **XOsoft**--CA XOsoft is a data protection solution that uses asynchronous real-time replication to provide disaster recovery capabilities. This link is active when you install CA XOsoft.
- **Backup Wizard**--Using the Backup Wizard you can easily select files that you want to backup, the media to use, and then quickly complete the remaining steps needed to start your backup job.
- **Restore Wizard**--Provides a quick and efficient method for submitting restore jobs. It lets you select one of two restore methods, the files you want to restore, a destination, and restore options.

Administration Menu

- **Server Admin**--Allows you to modify the CA ARCserve Backup system account and manage the core CA ARCserve Backup services: Job Engine, Tape Engine, and Database Engine. The Configuration icon allows you to configure tasks for these services including generating an alert and defining message logging. The Database Engine tab allows you to configure the database pruning job.g)
- **Device Manager**--Displays information about your storage devices and media. It also allows you to change a drive's compression mode, and perform media functions such as compression, formatting, erasing, ejecting, and retensioning. CA ARCserve Backup supports a wide variety of media including 4mm, 8mm, DLT, QIC, Iomega's Zip or Jazz media, PDs, MO, and WORM formats.
- **Device Configuration**--A tool that lets you to easily configure backup devices, such as tape and optical libraries, RAID devices, virtual libraries, File System Devices (FSD), and Deduplication devices (DDD). It also lets you enable or disable devices for Removable Storage Management (RSM).
 - **Maximum number of devices supported:** 255 (includes physical devices, FSDs, and DDDs)
 - **Maximum number of FSDs and DDDs supported:** 255 (only if the number of physical devices configured is 0).
- **Device Wizard**--Displays the devices you have installed on a local or remote system and lets you easily format, erase, compress, and eject your storage media.
- **Device Group Configuration**--A tool that lets you easily configure the device groups in your CA ARCserve Backup environment and select the groups that you will use for the staging of data.
 - **Maximum number of Device Groups supported:** 128
- **Media Pool Manager**--Manages, creates, and maintains logical groupings of media for easy identification of backups, to allow efficient scheduling of the maintenance and recycling of your media. You can design media rotation schemes to suit your particular archive needs.
- **MM Admin**--Provides the tools you need to organize tape movement to off-site storage locations and protect, control, and manage media resources.

Note: To use the MM Admin, you must install the Enterprise Module.
- **Database Manager**--Displays information from the CA ARCserve Backup database, such as the jobs processed by CA ARCserve Backup, the media used by CA ARCserve Backup, and the devices you are using with CA ARCserve Backup.
- **Alert Manager**--Sends messages to people in your organization, using various methods of communication, regarding events that occur during the functioning of CA ARCserve Backup.

- **User Profile Manager**--Lets you assign roles privileges to CA ARCserve Backup user accounts.

Note: To enable the enhanced User Profile Manager, role management, and Windows account support, you must install and licence the CA ARCserve Backup Enterprise Module on the Primary Server.

- **Agent Deployment**--Lets you install and upgrade a collection of CA ARCserve Backup agents on multiple remote hosts simultaneously.

Utilities Menu

- **Job Scheduler Wizard**--Provides an easy way to quickly package and submit jobs that you would typically submit from the Command Prompt window. In addition to the commands associated with CA ARCserve Backup, you can use this wizard for virtually any executable.

- **Create Boot Kit Wizard**--Creates and updates precautionary and machine-specific boot kits that will allow you to quickly recover your data if a disaster occurs.

Note: The Create Boot Kit wizard is available only if the CA ARCserve Backup Disaster Recovery Option is installed on your system. The CA ARCserve Backup Disaster Recovery Option is licensed separately.

- **Diagnostic Wizard**--Gathers and packages various CA ARCserve Backup system logs, which may be necessary for troubleshooting.

Note: The Diagnostic Wizard appears only if you install the Diagnostic Utility.

- **Merge Utility**--Lets you take media that contains one or more backup sessions and merge the information from the media into your CA ARCserve Backup database.

- **Media Assure & Scan Utility**--Lets you collect information about your media backup sessions and helps you ensure that the sessions on the media are restorable.

- **Compare Utility**--Lets you compare the contents of a media session to files on a machine.

- **Count Utility**--Lets you count the number of files and directories on a machine.

- **Copy Utility**--Lets you copy files from one location to another.

- **Purge Utility**--Lets you to delete files and directories from a machine.

CA ARCserve Backup Utilities

CA ARCserve Backup offers several utilities that you can use to manage files. You can access the Utilities from the Navigation Bar on the Home Page. These utilities are described in the following section. For more information about the options available for each utility, see the online help.

Merge Utility

If you need to restore files to a CA ARCserve Backup server that you did not use to create the backup, or if you removed information from your CA ARCserve Backup database that you now need, you can use the Merge utility.

The Merge utility lets you take media that contains one or more backup sessions and merge the information from the media into your CA ARCserve Backup database. The database information from the media is appended to your existing database files.

Each time you run a backup job, CA ARCserve Backup records information in its databases about the computers, directories, and files that have been backed up, and the media that were used. This allows CA ARCserve Backup to locate files whenever you need to restore them. This database information is backed up whenever you back up your CA ARCserve Backup home directory.

If you have media that has a backup session that is not included in the CA ARCserve Backup database (for example, the backup was created using CA ARCserve Backup on a different backup server), you can use the Merge Media option to get the media's information into the database in the CA ARCserve Backup home directory.

Why would you need to use the Merge utility?

You can use the Merge utility when you need to restore files to a CA ARCserve Backup server that you did not use to create the backup. You can also use the Merge utility if you pruned (deleted) information from your CA ARCserve Backup database that you now need.

Merge Utility Options

The Merge utility allows you to merge information from media into the database.

Using the Merge utility you can merge:

- All sessions
- A single session
- A range of sessions, using one of the following types of ranges:
 - Specific start session to a specific end session.
 - Specific start session to the end of the media.

Merge Options:

If you select to merge all sessions, the tape containing Sequence number 1 must be present for this operation to complete successfully.

If the tape containing Sequence number 1 is not present, you will be prompted that the media could not be found and request that you continue (after inserting the proper tape) or cancel the operation.

If you want to merge a session from a different tape other than the one containing Sequence number 1, you can only do so by not selecting to merge all sessions, and instead specify the session number or range of session numbers to be included.

If you want to merge a session that spans more than one tape, you must also have the tape with Sequence number 1 present because the session header information is located on the first tape.

Global Options for the Merge Utility

CA ARCserve Backup provides several types of global merge options. Use the Merge utility option when you want to restore detailed session information in your CA ARCserve Backup database.

For example, if a backup was created using CA ARCserve Backup on a different server, you can use Merge to get the media information into the database in the CA ARCserve Backup home directory. This will allow you to restore media backed up from another server at the file level. This can be useful if detailed information has been pruned from the database. By default, detailed job information is pruned 30 days after the backup to conserve database space. This can be configured in the Server Admin Manager.

Note: By default, all newly merged session details are preserved for one week (7 days) in the CA ARCserve Backup database, even if the newly merged session details are older than the prune retention time.

The available global merge options are listed below:

- Backup Media-Specify media options for the job such as the media timeout period
- Pre/Post-Run commands or batch files before the job runs and/or after it finishes
- Job Log-Enables you to determine the level of detail you want recorded into the Job Queue Log
- [Database](#) (see page 31)-Specify whether you want to record detailed information about the jobs, or job and session-level details only.
- Alert-Send messages about events in your operation

See Job Options to learn how to apply these options to your job.

Merge Utility - Database Global Options

The Database tab on the Global Options dialog of the Merge Utility lets you specify the level of details you want to merge.

- **Merge Detail Information**--Lets you merge all details, including job and session information.
- **Merge Session Headers Only**--Lets you merge only header information, such as job and session data.

Media Assure & Scan Utility

The Media Assure & Scan Utility lets you collect information about your media backup sessions. Each source that you specify to back up is saved on media as an individual session. Using the Media Assure & Scan Utility you can scan the following types of sessions:

- Single sessions or an entire media.
- A range of sessions, for example:
 - Specific start session to a specific end session.
 - Specific start session to the end of the media.

The results of the Scan job display in the Job Queue. You would need to do this if you are trying to recover a CA ARCserve Backup server and you need to identify the most recent backup of the CA ARCserve Backup database so that you can restore it.

If you would like a Scan job to produce a detailed listing of your media contents, use the Log All activity feature on the scan options tab. You can also use the Media Assure & Scan utility if you want a list of the files that were backed up.

Note: For more information about using the Media Assure & Scan utility, see the online help.

Global Scan Options

CA ARCserve Backup provides several types of advanced scan options:

Backup Media

Specifies media options for the job.

Operation

Specifies general options for the job such as to scan files with CRC verification or to enable database recording.

Pre/Post

Runs commands or batch files before or after the job.

Job Log

Determines the level of detail you want recorded in the Job Queue Log.

Alert

Sends messages about events in your operation.

Compare Utility

Compare the contents of a media session to files on a machine. Results of the Compare job can be seen in the Job Queue. You could use this option after a backup to verify that the backup copied all of the files to media without error.

CA ARCserve Backup provides several types of advanced compare options:

- **Backup Media**--Specify media options for the job.
- **Operation**--Specify whether to enable database recording.
- **Pre/Post**--Run commands or batch files before or after the job.
- **Job Log**--Determine the level of detail you want recorded in the Job Queue Log.
- **Alert**--Send messages about events in your operation.

Count Utility

The Count utility counts the number of files and directories on a machine. Results of the Count job can be seen in the Job Queue. You could use this option after a Copy job to verify that the Copy function copied all of the files from one disk to another without error.

CA ARCserve Backup provides several types of advanced count options:

- **Operation**--Specify whether to enable database recording.
- **Pre/Post**--Run commands or batch files before and after the job.
- **Job Log**--Determine the level of detail you want recorded in the Job Queue Log.
- **Virus**--Scan files for viruses before they are counted.
- **Alert**--Send messages about events in your operation.

Copy Utility

The Copy utility allows you to copy files from one location to another. For example, you can run a copy job on your local machine to store files and directories on another machine that is going to be backed up to media.

Copy options determine related actions that occur during or after the copy operation:

- **Retry**--Specify when to retry open files and file sharing options.
- **Operation**--Specify operation options and whether or not to enable database recording.
- **Destination**--Specify options for the directory structure and file conflict resolutions.
- **Pre/Post**--Run commands or batch files before or after the job.
- **Job Log**--Determine the detail you want recorded in the Job Queue Log.
- **Virus**--Scans files for viruses before they are copied.
- **Alert**--Send messages about events in your operation.

Purge Utility

The Purge utility allows you to delete files and directories from a machine. Results can be seen in the Job Queue.

CA ARCserve Backup provides several types of advanced purge options:

- **Operation**--Specify some general options for the job such as to remove directories or enable database recording.
- **Pre/Post**--Run commands or batch files before or after the job.
- **Job Log**--Determine the level of detail to record in the Job Queue Log.
- **Alert**--Send messages about events in your operation.

Note: For more information about using the Purge utility, see the online help.

Report Writer Utility

Create custom reports or generate predefined reports based on backup activity for a defined period. You can specify a query or filter report data. Generated reports can be previewed on screen, printed, and saved in either .csv or .xml format.

How You Can Manage Jobs Using the cabatch Command

The cabatch Utility is a job management tool that allows you perform the following tasks:

- Submit and delete jobs in local or remote CA ARCserve Backup job queues from the command line.
- Modify the execution times of jobs in the job queues.
- Use job scripts created in the CA ARCserve Backup Manager or in a text file created using the cabatch Job Information Template in the CA ARCserve Backup home directory.

For more information on the cabatch utility, see the *Command Line Reference Guide*.

User Profile Utility

The User Profile Utility lets the administrator manage user profiles and provide access to CA ARCserve Backup.

When you install CA ARCserve Backup, the caroot user profile is set up, by default, with the administrator group assigned to it. The Administrator group provides control over all CA ARCserve Backup functions operating within a given CA ARCserve Backup domain.

Using the User Profile utility CA ARCserve Backup server administrators can:

- Add a user.
- Delete a user.
- Change a user's password.
- Assign a user to a group.

CA ARCserve Backup Command Line Utilities

CA ARCserve Backup offers command line utilities that enable direct control over almost all operations that can be performed by a CA ARCserve Backup server via the DOS prompt. It provides an alternative method of accessing almost all of the operations available from the CA ARCserve Backup Manager.

A full description and use of these command line utilities can be found in the *Command Line Reference Guide*.

CA ARCserve Backup Security

The following sections describe CA ARCserve Backup security functionality.

CA ARCserve Backup Administrator Profile

CA ARCserve Backup is designed with a root-level, super user profile that provides complete control of CA ARCserve Backup. This profile, referred to as "caroot," is set up when you install CA ARCserve Backup for the first time. You can set the password for caroot during installation or later using the ca_auth utility.

Important! You should not leave the password blank for caroot.

The caroot user profile controls access to only the CA ARCserve Backup Manager and backup-related functions, and should not be confused with the security required to log in to your operating system.

Equivalence

CA ARCserve Backup allows you to create equivalence to caroot for any Windows account. A user who has been granted equivalence to caroot can run all of the command line utilities but cannot log in to the CA ARCserve Backup Home Page. Creating equivalence has the following advantages:

- **Ease of command line usage**--You create equivalence for a Windows user, the equivalence performs an implicit login on behalf of the logged-in user whenever a command line function requires authentication. Therefore, the command line utilities can be run without requiring the user to enter a user name and password each time a command is submitted.
- **Access Restriction**--Although a user that is equivalent to caroot can run all of the command line utilities, the user does not have access to the CA ARCserve Backup Manager. Access to the interface is granted only through the caroot account or through a CA ARCserve Backup user account with the proper privileges. You cannot use an account that has only been granted equivalency to login to the interface. To give additional CA ARCserve Backup users access Home Page, use the ca_auth utility.

Note: For more information about the ca_auth utility, see the *Command Line Reference Guide*.

System Account

The CA ARCserve Backup services require a valid Windows system account that has Administrator and Backup Operator privileges on the local machine. The services use this account to access local resources, such as the hard drive and the local network.

You are given the option of entering a Windows system account when you first install CA ARCserve Backup. If you enter a Windows account during installation, CA ARCserve Backup automatically grants this account Administrator and Backup Operator privileges. If you select Skip during installation, you must enter a valid Windows system account using the CA ARCserve Backup Administrator and grant it the required privileges manually.

Note: A user in the Backup Operator Group does not have rights to access the CA ARCserve Backup database. As a result member servers are not visible, to the user, in the Backup Manager.

You can change the system account information at any time using the CA ARCserve Backup Server Admin or the Server Configuration Wizard.

Equivalency and the System Account

Do not confuse the caroot user profile with the CA ARCserve Backup System Account. The caroot user profile is used to control access to the CA ARCserve Backup Manager and its related backup functions; the system account provides the security privileges needed by CA ARCserve Backup services to operate on the local machine.

Although the System Account and the caroot user profile perform different functions, in order for CA ARCserve Backup to run all of its jobs successfully, you must grant the System Account equivalency to caroot. For example, if the System Account is named BackupAdmin, and the local machine name is BAB01, use the following ca_auth command to give the account equivalency to caroot:

```
ca_auth -equiv add BackupAdmin BAB01 caroot caroot caroot_password
```

For more information on security, see Administering the Backup Server," in this guide, the *Command Line Reference Guide*, or the online help.

More information:

[Equivalence](#) (see page 36)

Enterprise Level Password Management Utility

When the user password changes, every job in the job queue must be modified to reflect the change. Using the `ca_jobsecmgr` utility you can make global user password changes for all the jobs in the Job Queue for the local CA ARCserve Backup Server (default).

Syntax

```
ca_jobsecmgr [server arguments] <current security> <new security>
```

Options

For a complete description of the options for this command, the *Command Line Reference Guide*.

How Centralized Cross-platform Management Works

CA ARCserve Backup offers Cross-platform Management, which simplifies administration in cross-platform environments, including CA ARCserve Backup for NetWare Version 9.0 and r11.1, and CA ARCserve Backup for Linux Version 9.0, r11, r11.1, and r11.5 backup servers, and remote environments. Its advanced management functionality enables backup administrators to centrally monitor and administer consistent backup policies throughout the environment. From one centralized console you can:

- Back up, copy, and restore any machine in your network
- Group preferred servers
- View job status
- Monitor active jobs
- View Activity Logs
- Administer various CA ARCserve Backup host database systems
- Customize reports

CA ARCserve Backup Enterprise Module

The CA ARCserve Backup Enterprise Module is a separately-installed component that lets you deploy a number of enhanced features, including the following:

- Data encryption performed by, or at, the CA ARCserve Backup server.
- Multistreaming.
- Multiplexing, up to 32 streams.
- Media Management Option.
- Dynamic Device Sharing between the CA ARCserve Backup Storage Area Network (SAN) Option and the CA ARCserve Backup NDMP NAS Option.

Note: For more information, see the *NDMP NAS Option Guide*.

In addition, the CA ARCserve Backup Enterprise Module is a prerequisite component for the following options:

- Enterprise Option for IBM 3494
- Enterprise Option for StorageTek ACSLS
- Image Option
- Media Management Option (MMO)
- Serverless Backup Option
- User Profiles
- Encryption at the server
- Disk to Disk to Tape backups (with greater than two streams)
- Disk to Tape to Tape backups
- CA ARCserve Backup for Windows Enterprise Option for VSS Hardware Snap-Shot (For more information, see the *Microsoft Volume Shadow Copy Service Guide*)

Note: For more information about the above options, see the *Enterprise Module Guide*.

More information:

[Data Encryption at the Agent Server](#) (see page 104)

[How Multistreaming Processes Backup Data](#) (see page 176)

[How Multiplexing Processes Backup Data](#) (see page 178)

[Media Management Administrator \(MM Admin\)](#) (see page 413)

How to Protect Virtual Machine Environments

Use the following methods to protect virtual machine environments using CA ARCserve Backup:

- **CA ARCserve Backup Agent for Virtual Machines**--The Agent for Virtual Machines lets you protect environments that rely on virtual machines (VMs) residing in Windows Server 2008 Hyper-V systems, VMware ESX Server systems, and VMware VirtualCenter Server systems to protect data.

For VMware-based systems, VMware provides a mechanism called VMware Consolidated Backup (VCB) that lets you protect the files and data stored in the VMs and ESX Server systems and VirtualCenter Server systems. To integrate CA ARCserve Backup with VMware VCB and Windows Server 2008 Hyper-V systems, you must install and license the Agent for Virtual Machines.

Note: For information about system requirements and supported platforms, see the readme file. For information about installing and configuring the agent, see the *Agent for Virtual Machines Guide*.

- **Scripted Solution for VMware ESX Server Systems**--The best method of protecting your VMs and ESX Server systems is to install the Agent for Virtual Machines. However, the scripted solution lets you integrate CA ARCserve Backup with VMware ESX Server without installing the Agent for Virtual Machines. The scripted solution helps to ensure that your VMs and ESX Server systems are protected as securely as any other server in your environment.

Note: To use the scripted solution, you must install and license the CA ARCserve Backup Client Agent for Windows.

For information about how to use a scripted solution to protect VMware ESX Server systems, see the *Best Practices Guide for VMware ESX Server Backup* on the Technical Support website at <http://ca.com/support>. The best practices guide describes common methods that you can use for data backups on VMs, and any considerations relating to the different methods.

- **Install CA ARCserve Backup Agents on the VM**--To back up and restore data that resides in your VMs, you can install the CA ARCserve Backup agents that correspond with the guest operating systems and the applications that are running in your VMs.

How Backup and Restore Operations Function on 64-bit Windows Platforms

Due to architectural differences between 64-bit and 32-bit Windows platforms, various elements of 64-bit operating systems cannot be accessed by 32-bit applications. These elements include areas of the Windows System Registry, system settings files included in a System State backup, and Volume Shadow Copy Service writers.

To overcome these limitations, and to successfully perform backup and restore operations when the CA ARCserve Backup server is running a 64-bit version of Windows, you must install the 64-bit version of the CA ARCserve Backup Client Agent on the CA ARCserve Backup server.

This configuration lets the 64-bit Client Agent run as a native process on the local CA ARCserve Backup server, which manifests the capability to perform browse, backup and restore operations on the local file system, System State, System Registry, and Volume Shadow Copy Service writers in the same manner as remote browse, backup, and restore operations using the 32-bit Client Agent for Windows.

For more information about CA ARCserve Backup Agents and Options supported by 64-bit Windows platforms, see the readme file.

Chapter 2: Protecting Data Using CA ARCserve Backup

This section contains the following topics:

[CA ARCserve Backup Components](#) (see page 44)

[Central Management](#) (see page 45)

[How Password Management Works](#) (see page 75)

[How User Profile Management Works](#) (see page 77)

[Data Security](#) (see page 101)

[How You Manage Media](#) (see page 108)

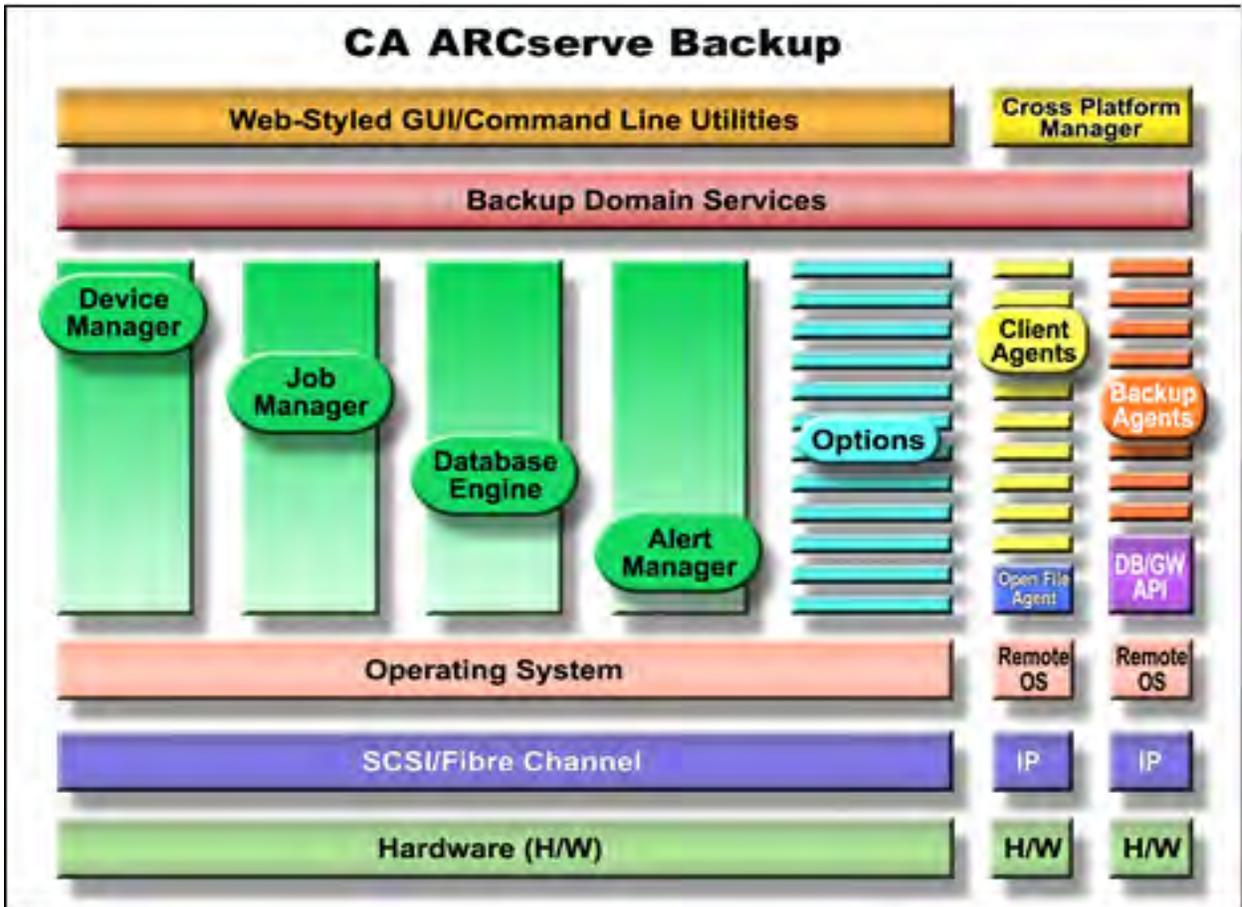
[Back Up and Restore Data](#) (see page 111)

[Backup Media Rotations and Scheduling Options](#) (see page 112)

Note: For information about how to install, upgrade, configure, and set up CA ARCserve Backup preferences, see the *Implementation Guide*.

CA ARCserve Backup Components

CA ARCserve Backup has a flexible design that allows you to manage and protect your environment. It provides powerful components that work together to accomplish critical administrative tasks seamlessly.



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.

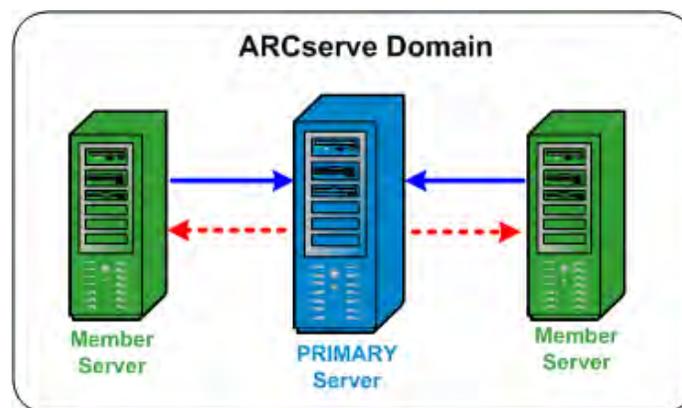
The Manager opens.

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.

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.

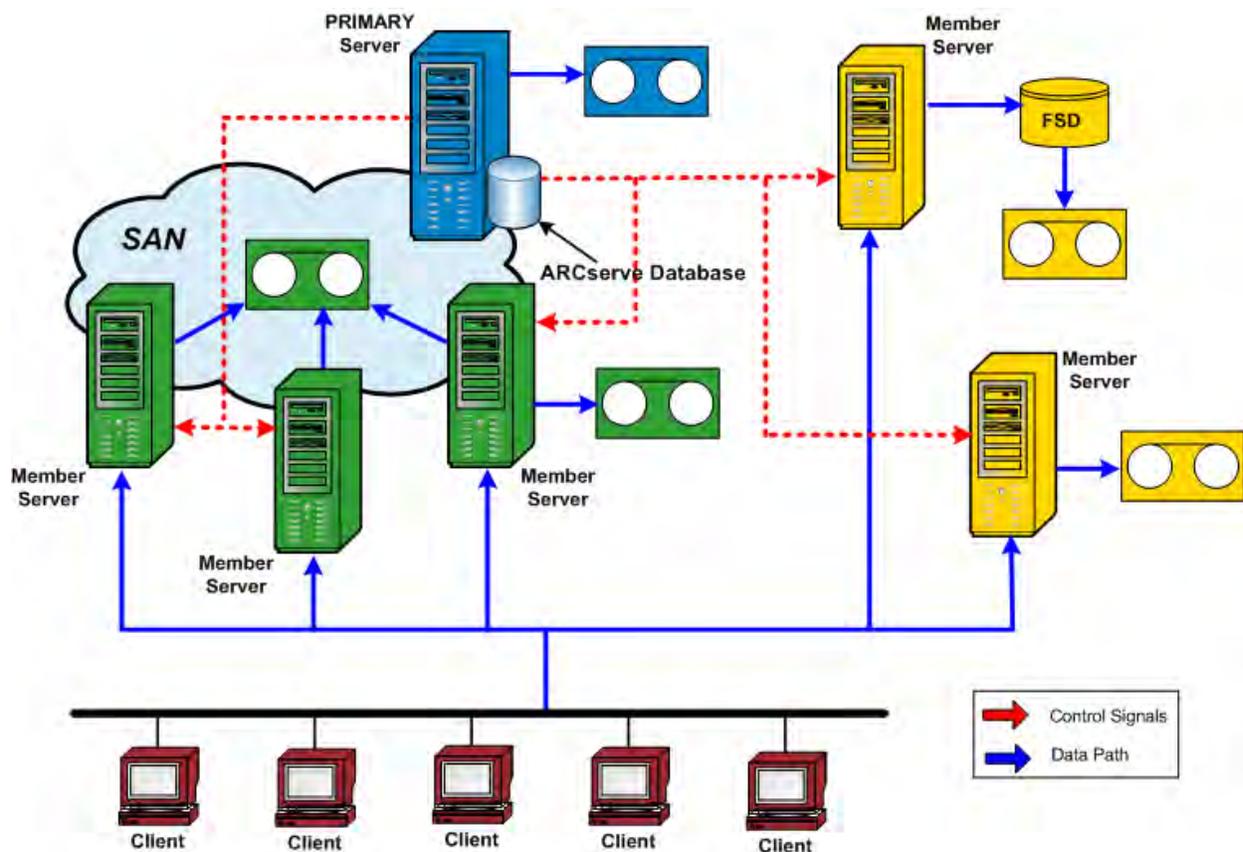
ARCserve Domain

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.

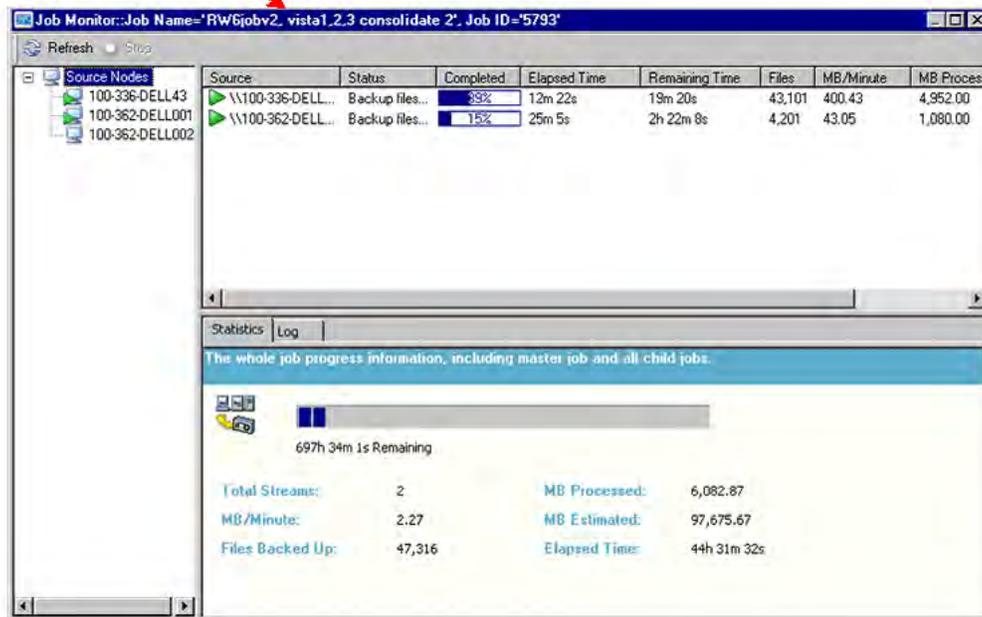
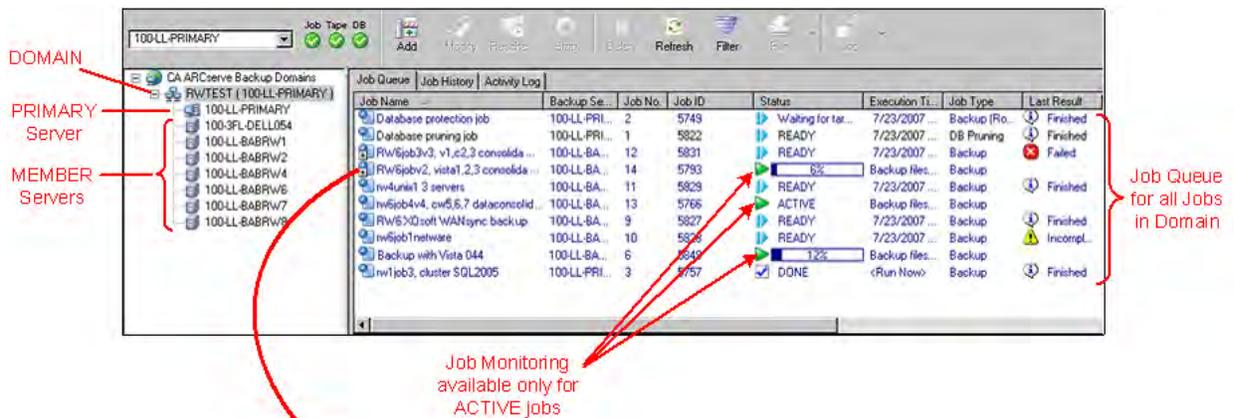
The screenshot displays the CA ARCserve Backup Central Management interface. On the left, a tree view shows the domain structure under '100-LL-PRIMARY'. The main area shows a 'Job Queue' table with columns for Job Name, Last Result, MB, Files, Missed, MB/Min., Time L., Job ID, Job No., and Session No. The table lists various jobs, including hardware scans and system state checks, with their respective results and statistics.

Job Name	Last Result	MB	Files	Missed	MB/Min.	Time L.	Job ID	Job No.	Session No.
100-LL-BABRW2 (5 job execution: 2 finished, 3 incomplete, 0 failed, 0 canceled)									
100-LL-BABRW4 (13 job execution: 8 finished, 1 incomplete, 4 failed, 0 canceled)									
100-LL-BABRW6 (8 job execution: 4 finished, 1 incomplete, 3 failed, 0 canceled)									
2007-07-09 19:00:08 pjob1 hardware e...	Incomplete	24,553.27	85089	2	274.85	01:29:20	5022	7	
2007-07-09 09:10:24 pjob1 hardware e...	Finished	24,636.83	88020	0	544.26	00:45:16	5004	6	
2007-07-08 09:10:24 pjob1 hardware e...	Finished	24,629.21	87962	0	525.64	00:46:46	4914	6	
Event Log Writer pjob1 hardware e...	Finished	27.19	6	0	14.83	00:01:50	4914	6	147
WMI Writer pjob1 hardware e...	Finished	7.14	9	0	4.56	00:01:34	4914	6	150
C pjob1 hardware e...	Finished	2,549.51	14885	0	187.46	00:13:36	4914	6	151
System State pjob1 hardware e...	Finished	829.30	3853	0	171.58	00:04:50	4914	6	155
2007-07-07 09:10:24 pjob1 hardware e...	Failed	18,822.50	68020	0	509.18	00:36:58	4823	6	
2007-07-06 09:10:24 pjob1 hardware e...	Failed	18,863.28	68024	0	436.65	00:43:12	4734	6	
2007-07-05 09:10:30 pjob1 hardware e...	Finished	24,596.96	87732	0	543.38	00:45:16	4641	6	
2007-07-04 09:10:28 pjob1 hardware e...	Finished	24,585.65	87604	0	544.73	00:45:08	4530	6	
100-LL-BABRW7 (40 job execution: 29 finished, 10 incomplete, 1 failed, 0 canceled)									
100-LL-PRIMARY (13 job execution: 10 finished, 3 incomplete, 0 failed, 0 canceled)									

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

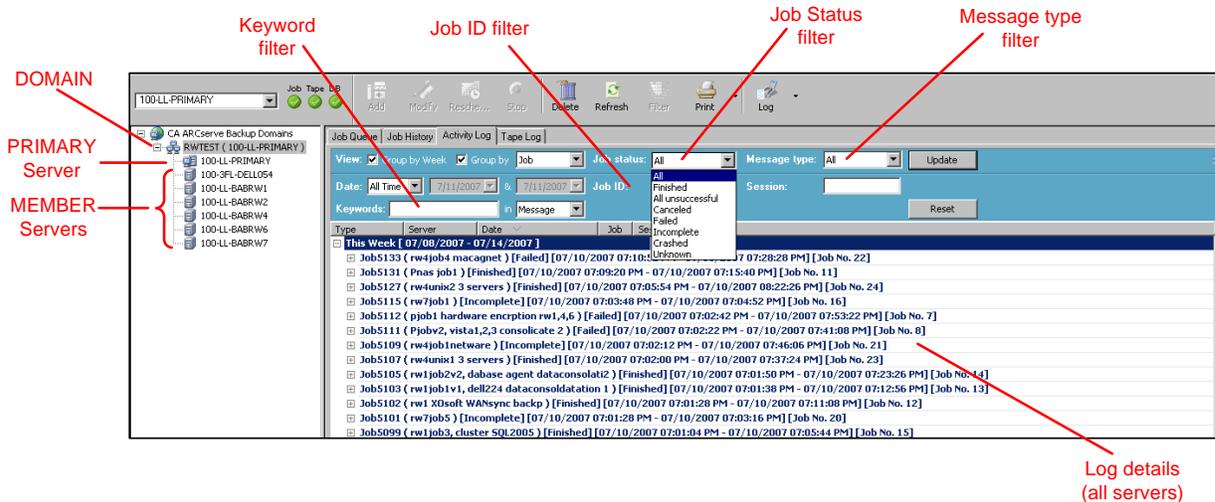
Information from all ARCserve servers within a domain is stored in a single central database that can be managed by the primary server. The central database is configured from the primary server and the associated member servers write relevant information into the central database.

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.

The image consists of two screenshots from the CA ARCserve Backup console, illustrating central server administration.

Top Screenshot: Domain View
 - **DOMAIN:** 100-LL-PRIMARY
 - **Tree View:** RWTEST (100-LL-PRIMARY) containing:
 - 100-LL-PRIMARY (PRIMARY Server)
 - 100-3FL-DELL054
 - 100-LL-BABRW1
 - 100-LL-BABRW2
 - 100-LL-BABRW4
 - 100-LL-BABRW6
 - 100-LL-BABRW7
 - 100-LL-BABRW9 (MEMBER Servers)
 - **Table:** Shows engine status for all servers in the domain. All engines (Job, Tape, DB) are 'Started'.

Name	Job Engine	Tape Engine	DB Engine
100-3FL-DELL054	Started	Started	Started
100-LL-BABRW1	Started	Started	Started
100-LL-BABRW2	Started	Started	Started
100-LL-BABRW4	Started	Started	Started
100-LL-BABRW6	Started	Started	Started
100-LL-BABRW7	Started	Started	Started
100-LL-BABRW8	Started	Started	Started
100-LL-PRIMARY	Started	Started	Started

Bottom Screenshot: Specified Server View
 - **Specified server:** 100-LL-NPRIMARY (100-LL-PRIMARY)
 - **Table:** Shows status of all engines and services on the specified server.

Name	Status	Up Time (days:hours:minutes)	Description
CA ARCserve Communication Foundation	Started	7 : 20 : 19	Provides data used by CA ARCserve Backup Da...
CA ARCserve Database Engine (DEEC)	Started	7 : 20 : 19	Provides database services for ARCserve Backu...
CA ARCserve Discovery Service	Started	7 : 20 : 19	Enables the discovery of all ARCserve Backup pr...
CA ARCserve Domain Server	Started	7 : 20 : 18	Provides the management of domains and authen...
CA ARCserve Job Engine	Started	7 : 20 : 18	Maintains and executes jobs from the ARCserve...
CA ARCserve Management Service	Started	7 : 20 : 18	Provides remote services for command line utiliti...
CA ARCserve Message Engine	Started	7 : 20 : 18	Allows remote management of other ARCserve ...
CA ARCserve Service Controller	Started	7 : 20 : 18	Enables remote start/stop of ARCserve Backup ...
CA ARCserve Tape Engine	Started	7 : 20 : 18	Manages the configuration and operation of bac...

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

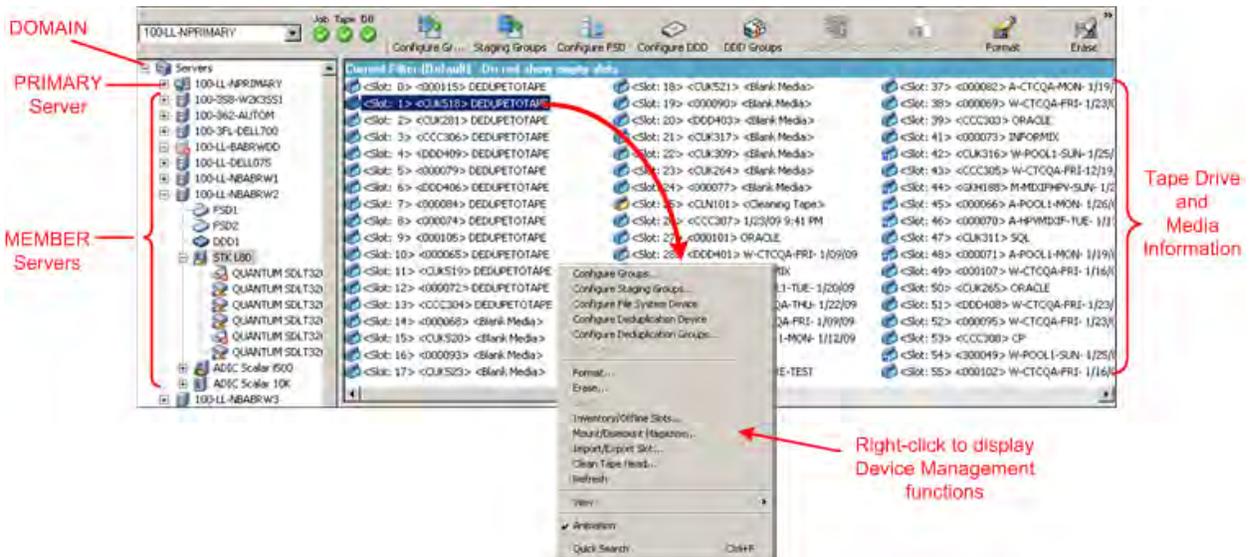
CA ARCserve Backup will now automatically detect the existence of a tape library and configure it. Therefore you no longer need to run the separate Tape Library Option Setup utility and no longer need to reconfigure a library after replacing bad drives or adding new drives. In addition, library settings 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.



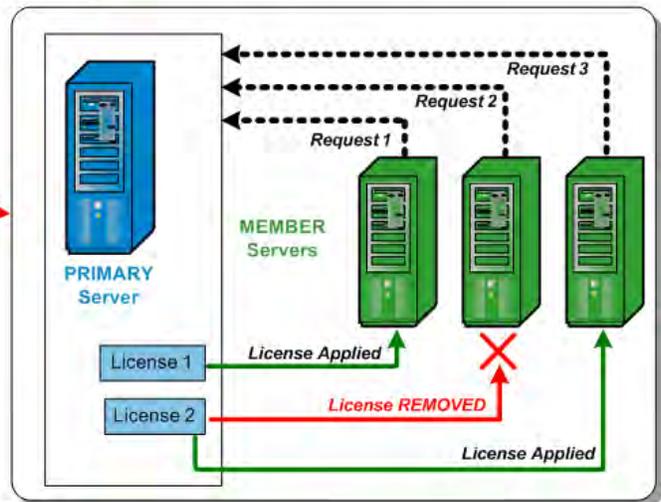
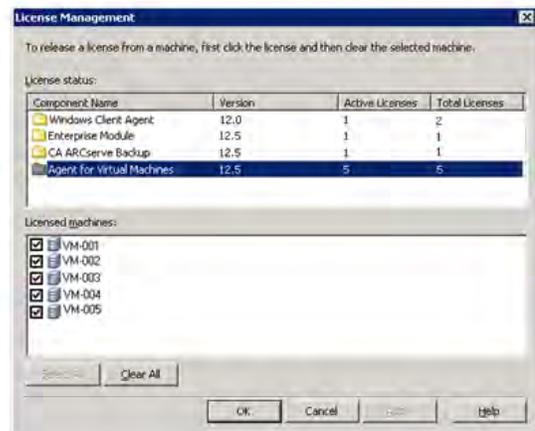
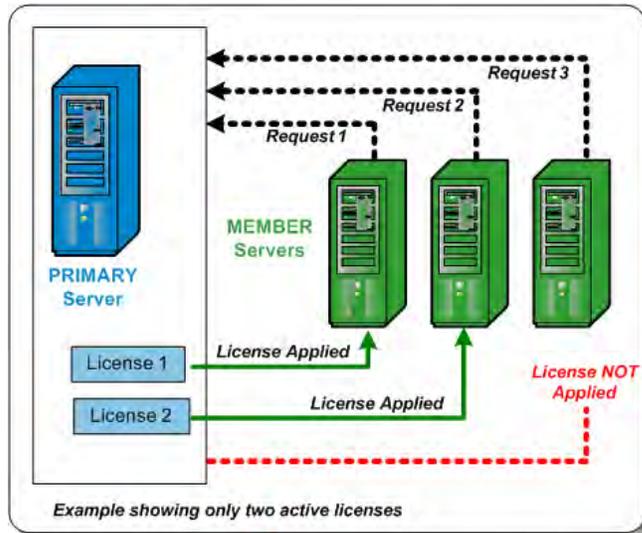
Central License Management

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 481)

[Release Licenses from Servers](#) (see page 483)

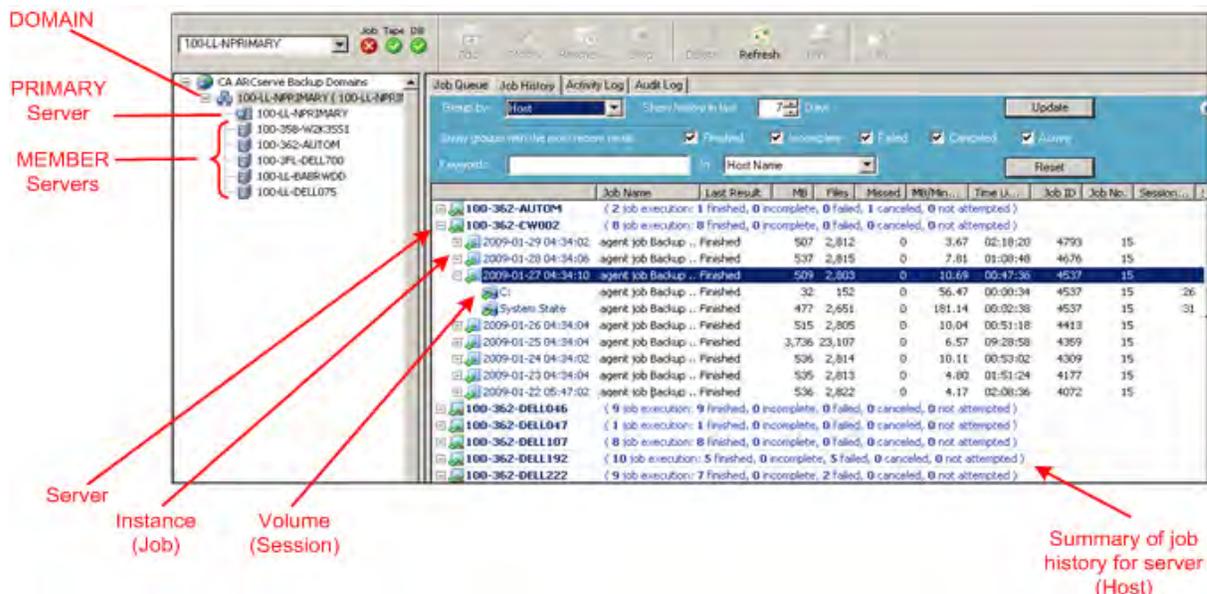
Central Job History

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.



Job View

The Job view displays all executions of a job. Each execution shows all of the hosts that were backed up. You can also drill down on a host and see the sessions that were backed up.

For each job entry, you also see the following summary information:

	Last Result	MB	Files	Missed	MB/Min...	Time Used	Job ID	Job No.	Session...	Subsession No.	Compression R...
This job was submitt... (1 job execution: 1 finished, 0 incomplete, 0 failed, 0 canceled)											
This job was submitt... (1 job execution: 1 finished, 0 incomplete, 0 failed, 0 canceled)											
Job 001 VM1-Backup-17880687 (3 job execution: 3 finished, 0 incomplete, 0 failed, 0 canceled)											
2009-01-29 04:36:22	Finished	17,187	18,895	0	608.75	00:28:14	4794	468			3.64 (72.55%)
100-LL-RWVM1	Finished	17,187	18,895	0	680.22	00:25:16	4794	468			3.64 (72.55%)
RAW	Finished	12,716	18	0	503.27	00:25:16	4794	468	2545		51.58 (98.06%)
E:	Finished	N/A	N/A	N/A	N/A	00:00:00	4794	468	2545	2	1.00 (0.00%)
F:	Finished	N/A	N/A	N/A	N/A	00:00:00	4794	468	2545	3	1.00 (0.00%)
H:	Finished	0	5	0	N/A	00:00:00	4794	468	2545	5	1.00 (0.00%)
I:	Finished	0	2,171	0	N/A	00:00:00	4794	468	2545	6	1.00 (0.00%)
G:	Finished	70	318	0	N/A	00:00:00	4794	468	2545	4	1.00 (0.00%)
C:	Finished	4,401	16,383	0	N/A	00:00:00	4794	468	2545	1	1.00 (0.00%)
2009-01-29 03:52:26	Finished	17,184	18,664	0	754.79	00:22:46	4782	468			3.73 (73.19%)
100-LL-RWVM1	Finished	17,184	18,664	0	839.61	00:20:28	4782	468			3.73 (73.19%)
2009-01-29 01:44:48	Finished	17,184	18,649	0	748.21	00:22:58	4769	468			3.15 (68.23%)
Job 002 CP mixed ... (8 job execution: 8 finished, 0 incomplete, 0 failed, 0 canceled)											
Job 003 Dedupe --... (13 job execution: 0 finished, 4 incomplete, 7 failed, 1 canceled, 1 active)											

- **Number of job execution**--Indicates the number of times the host was supposed to be backed up or backed up by a job.
- **Number of jobs finished**--Number of times the host was backed up successfully.
- **Number of jobs incomplete**--Number of times the host was not completely backed up.
- **Number of jobs failed**--Number of times the backup of the host failed.
- **Number of jobs canceled**--Number of times the backup of the host was canceled.

Backup Execution Details for a Selected Job

When you select a specific job execution the following information is displayed:

Job Queue Job History Activity Log Audit Log												
Group by		Job		Show history in last		7 Days		Update				
		Last Result	MB	Files	Missed	MB/Min...	Time Used	Job ID	Job No.	Session...	Subsession...	Compressi...
		2009-01-30 03:46:04	Finished	7,936	70,964	0	134.89	00:58:50	4925	592		
		2009-01-29 03:45:48	Finished	7,880	70,964	0	146.11	00:53:56	4779	592		
		2009-01-28 03:45:56	Finished	7,826	70,964	0	139.92	00:55:56	4658	592		
		2009-01-27 03:45:52	Finished	7,804	70,964	0	135.56	00:57:34	4526	592		
		2009-01-26 03:45:50	Finished	7,804	70,964	0	156.60	00:49:50	4405	592		
		2009-01-25 03:45:48	Finished	7,789	70,964	0	143.80	00:54:10	4355	592		
		2009-01-24 03:45:52	Finished	7,785	70,964	0	146.24	00:53:14	4301	592		

Detail Job Log									
Summary									
Execution Time	2009-01-27 03:45:52---2009-01-27 04:43:26								
Total Source Host	3(3 Finished,0 Failed,0 Cancel,0 Incomplete,0 Not Attempted,0 Other)								
Total Sessions	17(17 Finished,0 Failed,0 Cancel,0 Incomplete,0 Other)								
Total Migrations	0(0 Finished,0 Failed,0 Incomplete,0 Pending)								
Device and Media									
Device	QUANTUM(Board:3,Bus:0,SCSIID:1,LUN:2)								
Media Used:1	<table border="1"> <thead> <tr> <th>Media Name</th> <th>Barcode</th> <th>SequenceNO</th> <th>RandomID</th> </tr> </thead> <tbody> <tr> <td>CP</td> <td>CCC308</td> <td>1</td> <td>F224</td> </tr> </tbody> </table>	Media Name	Barcode	SequenceNO	RandomID	CP	CCC308	1	F224
Media Name	Barcode	SequenceNO	RandomID						
CP	CCC308	1	F224						
Error and Warning									
No item to display!									

In the top pane, the following information is displayed:

Job Execution Time

The time the job started.

Job Name

The name of the job.

Note: This release of CA ARCserve Backup does not display blank job names in the Job Status Manager. If you upgraded from a previous ARCserve release, migrated the job history data, and the jobs contained blank job names, the names of the jobs display in the Job Name field in the Job Status Manager in the following format:

[<<machine name>>] <<job no>>

Last Result

The last result is determined from the following criteria:

- The status is marked as failed if any of the sessions in the job fail.
- The status is marked as incomplete in any of the sessions are incomplete even if some are successful.
- The status is marked as successful only if all sessions are successful.

MB

The amount of data backed up for the job.

Files

The number of files backed up for the job.

Missed

The number of files missed during the backup.

Note: Use CA ARCserve Backup Agent for Open Files to backup open files to avoid missed files during a backup.

MB/Minute

- At the Job level, MB/Minute indicates the ratio of megabytes and the elapsed time for the entire job, including pre and post scripts, if any, media management activities, and so on. For average master job throughput, refer to the Activity Log.
- At the Host level, MB/Minute indicates the ratio of megabytes and the elapsed time for the entire job, including pre and post scripts, if any, media management activities, and so on for a single host.
- At the Session level, MB/Minute indicates the ratio of megabytes and the elapsed time for a specific volume and its folders, which comprise a single session.

Note: If little or no data is backed up by the backup job, a value of N/A appears in the MB/Minute field.

Time Used

- At the Job level, Time Used indicates the elapsed time for the entire job including pre and post scripts, if any, media management activities, and so on.
- At the Host level, Time Used indicates the elapsed time for the entire job including pre and post scripts, if any, media management activities, and so on for a single host.
- At the Session level, Time Used indicates the elapsed time for the backup of a specific volume and its folders, which comprise a single session.

Job ID

Identifies the specific execution of the job.

Job No.

Identifies the job.

Compression Ratio

The amount of actual data to be stored divided by the amount of data stored after deduplication expressed as a ratio or percentage.

In the bottom pane, the following information is displayed:

Summary

Execution Time

The start time and end time of the selected job.

Total Source Host

The total number of hosts the job attempted to backup.

Total Sessions

The number of sessions that were backed up by the selected job execution.

Total Migrations

The number of sessions migrated in a disk or tape staging job.

Device and Media

Device

The tape drive or file system device used during the backup. Multiple tape drives can also be used for the same host in a single job execution if the job is a multi streaming job.

Media Used

The media that was used during the backup of the host. Multiple media can also be used for the same host in a single job execution if the job is a multi streaming job.

Error and Warning

Displays the errors and warnings that are generated during the back up of a host.

Node Level Details for a Selected Job

When you select the node of an executed job, the following information is displayed:

	Last Result	MB	Files	Missed	MB/Min...	Time Used	Job ID	Job No.	Session...	Subsession No.	Compressid
Job 001 hardware ...	(9 job execution: 2 finished, 0 incomplete, 7 failed, 0 canceled)										
Job 002 mixif all ser...	(8 job execution: 0 finished, 0 incomplete, 8 failed, 0 canceled)										
Job 003 CP mixed ...	(8 job execution: 8 finished, 0 incomplete, 0 failed, 0 canceled)										
Job 004 agent job B...	(8 job execution: 0 finished, 0 incomplete, 8 failed, 0 canceled)										
Job 005 Backup [Cu...	(8 job execution: 8 finished, 0 incomplete, 0 failed, 0 canceled)										
2009-01-30 04:46:40	Finished	0	6	0	.00	00:00:54	4961	139			
2009-01-29 04:46:46	Finished	0	6	0	.00	00:01:28	4804	139			
2009-01-28 04:47:12	Finished	0	6	0	.00	00:01:26	4686	139			
2009-01-27 07:39:14	Finished	0	6	0	.00	00:00:54	4549	139			
2009-01-26 12:01:14	Finished	0	6	0	.00	00:01:02	4424	139			
2009-01-25 04:46:38	Finished	0	6	0	.00	00:01:00	4368	139			
2009-01-24 04:46:38	Finished	0	6	0	.00	00:00:50	4319	139			
2009-01-23 04:46:44	Finished	0	6	0	.00	00:00:38	4188	139			
100-3FL-DELL700	Finished	0	6	0	N/A	00:00:00	4188	139			
E:\hotfix_11_11	Finished	0	6	0	N/A	00:00:00	4188	139	12		

Detail									
Summary									
Execution Time	2009-01-23 04:46:30----2009-01-23 04:46:30								
Total Sessions	1(1 Finished,0 Failed,0 Cancel,0 Incomplete,0 Other)								
Total Migrations	0(0 Finished,0 Failed,0 Incomplete,0 Pending)								
Device and Media									
Device	HP(Board:4,Bus:0,SCSIID:5,LUN:0)								
Media Used:1	<table border="1"> <thead> <tr> <th>Media Name</th> <th>Barcode</th> <th>SequenceNO</th> <th>RandomID</th> </tr> </thead> <tbody> <tr> <td>DELL700</td> <td></td> <td>1</td> <td>4756</td> </tr> </tbody> </table>	Media Name	Barcode	SequenceNO	RandomID	DELL700		1	4756
Media Name	Barcode	SequenceNO	RandomID						
DELL700		1	4756						
Error and Warning									
No item to display!									

Summary

Execution Time

The start time and end time of the selected node.

Total Sessions

The number of sessions that were backed up for the host.

Total Migrations

The number of sessions migrated in a disk or tape staging job.

Device and Media

Device

The tape drive or file system device used during the backup job. Multiple tape drives can also be used for the same host in a single job execution if the job is a multi streaming job.

Media Used

The media that was used during the backup of the host. Multiple media can also be used for the same host in a single job execution if the job is a multi streaming job.

Error and Warning

Displays the errors and warnings that are generated during the backup of a host.

Session Level Details of a Selected Node

Drilling down even more, when you highlight a session, the following details of the session are displayed:

	Last Result	MB	Files	Missed	MB/Min...	Time Used	Job ID	Job No.	Session...	Subsession No.	Compressid
2009-01-30 04:46:40	Finished	0	6	0	.00	00:00:54	4961	139			
2009-01-29 04:46:46	Finished	0	6	0	.00	00:01:28	4804	139			
2009-01-28 04:47:12	Finished	0	6	0	.00	00:01:26	4686	139			
2009-01-27 07:39:14	Finished	0	6	0	.00	00:00:54	4549	139			
2009-01-26 12:01:14	Finished	0	6	0	.00	00:01:02	4424	139			
2009-01-25 04:46:38	Finished	0	6	0	.00	00:01:00	4368	139			
2009-01-24 04:46:38	Finished	0	6	0	.00	00:00:50	4319	139			
2009-01-23 04:46:44	Finished	0	6	0	.00	00:00:38	4188	139			
100-3FL-DELL700	Finished	0	6	0	N/A	00:00:00	4188	139			
E:\hotfix_11_11	Finished	0	6	0	N/A	00:00:00	4188	139	12		

Detail	
Session Detail	
Execution Time	2009-01-23 04:46:30----2009-01-23 04:46:30
Number	12
Type	NTFS
Path	\\100-3FL-DELL700\E:\hotfix_11_11
Status	Finished
Start time	2009-01-23 04:46:30
End time	2009-01-23 04:46:30
Method	Full
Flags	Catalog
MB	0
Files	6
Missed	0
Device and Media	
Device	HP(Board:4,Bus:0,SCSIID:5,LUN:0)

Session Detail

Execution Time

The start time and end time of the selected session.

Number

Indicates the session number.

Type

Identifies the type of session backed up.

Path

The root path of the session.

Status

Indicates the result of the backup session.

Start time

The start time of the session.

End time

The end time of the session.

Method

The type of backup method used for the session.

Flags

The method used to backup the session.

MB

The amount of data backed up for the session.

Files

The number of files backed up for the session.

Missed

The number of files not backed up during the session.

Device and Media

Device

The tape drive or file system device used during the backup of the session.

Media Used

The media that was used during the backup of the session.

Error and Warning

Displays the errors and warnings that are generated during the back up of a session.

Host View

The Host view displays all of the hosts that were backed up and their status each time a job has backed it up. You can also drill down on a host and see the sessions that were backed up. For each host entry, you also see the following summary information:

Number of job execution

Indicates the number of times the host was attempted to be backed up or backed up by a job.

Number of jobs finished

Number of times the host was backed up successfully.

Number of jobs incomplete

Number of times the host was not completely backed up.

Note: To avoid incomplete backups use CA ARCserve Backup Agent for Open Files to back up open files.

Number of jobs failed

Number of times the backup of the host failed.

Number of jobs canceled

Number of times the backup of the host was canceled.

Backup Execution Details of a Selected Host

When you select a specific job execution the following information is displayed:

Job Queue Job History Activity Log Audit Log										
Group by		Host		Show history in last		7 Days		Update		
		Last Result	MB	Files	Missed	MB/Min...	Time Used	Job ID	Job No.	Session...
		2009-01-22 16:16:18	Finished	10	15	0	5.88	00:01:42	4165	241
		2009-01-21 16:16:22	Finished	N/A	N/A	N/A	N/A	00:01:02	4003	241
		2009-01-20 16:16:18	Finished	N/A	N/A	N/A	N/A	00:01:10	3828	241
		2009-01-19 16:16:16	Finished	N/A	N/A	N/A	N/A	00:01:02	3675	241
		2009-01-18 16:16:20	Finished	N/A	N/A	N/A	N/A	00:01:02	3501	241
		2009-01-17 16:16:20	Finished	N/A	N/A	N/A	N/A	00:01:00	3482	241

Detail		Job Log	
Summary			
Execution Time	2009-01-19 16:16:16----2009-01-19 16:17:18		
Total Source Host	2(2 Finished,0 Failed,0 Cancel,0 Incomplete,0 Not Attempted,0 Other)		
Total Sessions	0(0 Finished,0 Failed,0 Cancel,0 Incomplete,0 Other)		
Total Migrations	0(0 Finished,0 Failed,0 Incomplete,0 Pending)		
Device and Media			
No item to display!			
Error and Warning			
Retrieving log from DB...			

In the top pane, the following information is displayed:

Job Execution Time

The time the job started.

Job Name

The name of the job that backed up the host.

Note: This release of CA ARCserve Backup does not display blank job names in the Job Status Manager. If you upgraded from a previous ARCserve release, migrated the job history data, and the jobs contained blank job names, the names of the jobs display in the Job Name field in the Job Status Manager in the following format:

[<<machine name>>] <<job no>>

Last Result

The last result is determined from the following criteria:

- The status is marked as failed if any of the sessions in the host fail.
- The status is marked as incomplete in any of the sessions are incomplete even if some are successful.
- The status is marked as successful only if all sessions are successful.

MB

The amount of data backed up for the host.

Files

The number of files backed up for the host.

Missed

The number of files missed during the backup job.

Note: Use CA ARCserve Backup Agent for Open Files to avoid missed files during a backup job.

MB/Minute

- At the Job level, MB/Minute indicates the ratio of megabytes and the elapsed time for the entire job, including pre and post scripts, if any, media management activities, and so on. For average master job throughput, refer to the Activity Log.
- At the Session level, MB/Minute indicates the ratio of megabytes and the elapsed time for a specific volume and its folders, which comprise a single session.

Time Used

- At the Job level, Time Used indicates the elapsed time for the entire job including pre and post scripts, if any, media management activities, and so on.
- At the Session level, Time Used indicates the elapsed time for the backup of a specific volume and its folders, which comprise a single session.

Job ID

Identifies the specific execution of the job.

Job No.

Identifies the job.

Compression Ratio

The amount of actual data to be stored divided by the amount of data stored after deduplication expressed as a ratio or percentage.

In the bottom pane, the following information is displayed:

Summary

Total Sessions

The number of sessions that were backed up for the host.

Total Migrations

The number of sessions migrated in a disk or tape staging job.

Device and Media

Device

The tape drive or file system device used during the backup job. Multiple tape drives can also be used for the same host in a single job execution if the job is a multi streaming job.

Media Used

The media that was used during the backup of the host. Multiple media can also be used for the same host in a single job execution if the job is a multi streaming job.

Error and Warning

Displays the errors and warnings that are generated during the backup of a host.

Session Level Details of a Selected Host

Drilling down even more, when you highlight a session, the following details of the session are displayed:

Job 001 [1 job execution: 1 finished, 0 incomplete, 0 failed, 0 canceled]									
2009-01-21 00:48:50	Finished	24	18	0	30.00	00:00:48	3861	269	
100-362-DELL192	Finished	24	18	0	102.86	00:00:14	3861	269	
sqlldr@NEW	Finished	6	4	0	90.00	00:00:04	3861	269	1
dbasql@NEW...	Finished	4	2	0	120.00	00:00:02	3861	269	2
dbasql@NEW...	Finished	2	2	0	N/A	00:00:00	3861	269	3

Session Detail				
Execution Time	2009-01-21 00:48:34---2009-01-21 00:48:38			
Number	1			
Type	SQL Server Disaster Recovery Elements			
Path	\\100-362-DELL192\sqlldr@NEW			
Status	Finished			
Start time	2009-01-21 00:48:34			
End time	2009-01-21 00:48:38			
Method	Clone-Snap			
Flags	Agent, Catalog			
MB	6			
Files	4			
Missed	0			

Device and Media				
Device	FSD3(Board:2,Bus:0,SCSIID:2,LUN:0)			
Media Used:1	Media Name	Barcode	SequenceNO	RandomID
	1/20/09 8:50 PM		1	8C4B

Error and Warning
 W3558 2009-01-20 20:50:33 Global Agent Options for Microsoft SQL Server are not applied by agents whose version is below r12.5. (Node=100-362-DELL192, Agent Version=r12.0)

Session Detail

Execution Time

The start time and end time of the selected session.

Number

Indicates the session number.

Type

Identifies the type of session backed up.

Path

The root path of the session.

Status

Indicates the result of the backup session.

Start time

The start time of the session.

End time

The end time of the session.

Method

The type of backup method used for the session.

Flags

The method used to backup the session.

MB

The amount of data backed up for the session.

Files

The number of files backed up for the session.

Missed

The number of files not backed up during the session.

Device and Media

Device

The tape drive or file system device used during the backup of the session.

Media Used

The media that was used during the backup of the session.

Error and Warning

Displays the errors and warnings that are generated during the back up of a session.

Filter the Job Queue

Filter options let you refine how you search the Job Queue.

To filter the Job Queue

1. Open the Job Status Manager.

Select the Job Queue tab.

Expand the header bar by clicking .

Choose from the following filter options:

- **Show jobs with the status**--Lets you filter jobs based on the job status.
 - **Show done jobs with the results**--Lets you filter done jobs based on the jobs status
 - **Keywords**--Lets you filter jobs that contain a particular keyword.
 - **In**--Used in conjunction with Keywords, lets you specify whether the keyword is contained within the Backup Server Name or the Job Name.
 - **Show jobs owned by other users**--Lets you view all jobs or only the jobs that you own.
 - **Show jobs by selected types**--Lets you view jobs based on the type of job. For example, a backup job, a restore job, a migration job, and so on. To specify the types of jobs that you want to view, click Select Types.
2. Click Update.
The filter options are applied.

Filter Job History

Filter options let you refine your job history search.

To filter job history

1. Open the Job Status Manager.

Select the Job History tab.

Expand the header bar by clicking .

Choose from the following filter options:

- **Group by**--Specify the type of group to sort by. The options are by job or by host.
- **Show history in last xx days**--Specify the number of days of job history you need. The range is from 1 to 100 days.
- **Show groups with the most recent result**--Specify what type of result history you want to view. You can specify one, all or any combination of options. The options include: active, finished, incomplete, failed and canceled.

Note: The header bar will turn yellow if there is a change made to the type of result history you want to view indicating that the advanced filter was used.

- **Keywords**--Specify keywords to be used in the sorting of the job history by Job Name or Host Name.

Note: The header bar will turn yellow if a keyword is specified indicating that the advanced filter was used.

- **In**--Specify a Job Name or Host Name. The keywords will be used to identify jobs in the chosen category.

2. Click Update.

The filter options are applied.

View Job History

Use the Job History dialog to identify patterns or areas of repeated errors.

To view a job history

1. Open the Job Status Manager.
2. Select the Job History tab.
3. In the Group By drop-down list, select Host or Job. Depending upon your selection, the job history appears in either Host View or Job View.
4. Click Update.

The Properties panel displays the job history.

Locate Information Using Quick Search

Locating information manually on the user interface can be time-consuming and tedious, especially when there are many jobs, nodes, tapes, etc. in the system. The Quick Search feature allows you to quickly and easily find the information you need on the user interface. You can use Quick Search to find an item on any tree or list in the ARCserve Manager. For example, you can use Quick Search to locate the following type of information:

- Jobs or logs in the Activity Log
- Jobs in Job History
- Nodes when using Restore by Tree
- Tapes or sessions when using Restore by Session
- Media pools from the Media Pool Manager

Important! Quick Search will only search items displayed on the user interface. It will not search for particular data stored on a tape.

Note: To enhance Quick Search performance, you can filter the Activity Log to reduce the number of items displayed and queried prior to using Quick Search. For more information about filtering the Activity Log, see [Set Activity Log Queries](#) (see page 312).

To locate information using the Quick Search feature

1. Press CTRL+F to open the Quick Search dialog from any tree or list view on the CA ARCserve Backup user interface.

For a list of where and how you can access the Quick Search feature using **Ctrl+F** from the user interface and a sample of the kind of items that can be searched, see [Quick Search Accessibility](#) (see page 74).

Note: You can also launch Quick Search from the context menu of a tree or list view when you right-click and select Quick Search.

2. Type a keyword to search on or select one from the drop-down list.

If you type a keyword to search on, the search supports the hint during typing feature where the hint is provided from the keyword history. For example, if you type "job" and the keywords "Job 1943" and "Job 2048" have been entered previously, then both "Job 1943" and "Job 2048" will be listed under the text box where you are typing.

Note: The search does not support wildcard characters.

If you click the drop-down arrow, the keyword history displays. By default, the maximum number of keywords remembered is fifty, but this limit can be set in the local registry.

3. (Optional) Click the plus sign icon to expand the Search options field and choose the options that apply.

Match case

Search using case-sensitive capitalization.

Match whole word

Search using whole word matches and not part of a word.

4. Press Enter or click the Search button.

The Search result list displays, showing all the matched items, the number of items found, and the total number of items searched.

Important! The Quick Search feature will only find items that are at the expanded level. Items under a collapsed node will not be found. Therefore, as long as the item is visible on the user interface or can be seen by scrolling, the Quick Search is able to find it.

Note: The search function will work in the background, so you can continue working during long searches without closing the dialog. To stop the search at any time, click the Search button.

5. (Optional) Select or double-click an item from the list of search results.

The search stops if it is still active and the item is selected on the tree or list in the background of the user interface.

6. (Optional) Double-click another item from the results.

The Quick Search dialog remains open.

Note: If the preferred items are not found, you can adjust the keyword and perform another search.

7. To close the Quick Search dialog, press ESC or click the X button to close.

Quick Search Accessibility

The following indicates where and how you can access the Quick Search feature using **Ctrl+F** from the user interface and a sample of the kind of items that can be searched:

Manager	Location	Tree/List View	Searchable Items
Job Status	ARCserve Domain Tree	Tree	Domain, Server
	Job Queue Tab	List	Job
	Job History Tab	List	Job, Host, Job Execution, Session
	Activity Log Tab	List	Job, Log, Message Number, Message
Backup Manager	Source Tab	Tree	Machine, Folder
		List	Machine, Folder, File
	Staging Tab	Tree	Server, Group
		List	Server, Group, Media
	Destination Tab	Tree	Server, Group
		List	Server, Group, Media
Restore Manager (By Tree, By Session, By Image, By Backup Media)	Source Tab	Tree	Machine, Session, Folder, Group
		List	Machine, Session, Folder, Group, File, Media
	Destination Tab	Tree	Machine, Folder
		List	Machine, Folder
Device Manager		Tree	Server, Device
		List	Server, Device, Media
Media Pool Manager		Tree	Media Pool
		List	Media Pool, Media
Database Manager		Tree/List	Job, Media, Session, Folder, File, Device
Merge, Media Assure & Scan, Compare, Copy, Count, Purge		Tree/List	Same as Backup and Restore Manager

How Password Management Works

Password Management provides the option to encrypt session passwords during backup and eliminates the need to repeatedly provide passwords. This feature lets you store session passwords in the CA ARCserve Backup database. During a backup job submission, the passwords are stored in encrypted form and will be automatically used during restore. Along with the session password, information about when to change your password is also stored. If you forget to change your session password, you will receive a reminder through the Activity Log.

Also, part of the enhancement is the ability to restore encrypted tapes on-site without requiring the encryption password. This feature allows other operators to perform different tasks without having to enter the password.

Note: If you run a restore, merge, or compare job for sessions created using an older version of CA ARCserve Backup, encrypted a tape in a different CA ARCserve Backup domain, or if Password Management was not enabled during a backup job, you need to provide the session/encryption password manually.

As a backup session is submitted, the session encryption password is saved to the CA ARCserve Backup database in encrypted format using a random key and the Globally Unique Identifier (GUID) is saved as a binary value. During a restore session, the encrypted password is extracted from the CA ARCserve Backup database and decrypted. To extract the encrypted password, the session GUID must be known. Depending on how the data was encrypted, either Server Side Encryption or Agent Side Encryption, there are two ways to identify the session GUID.

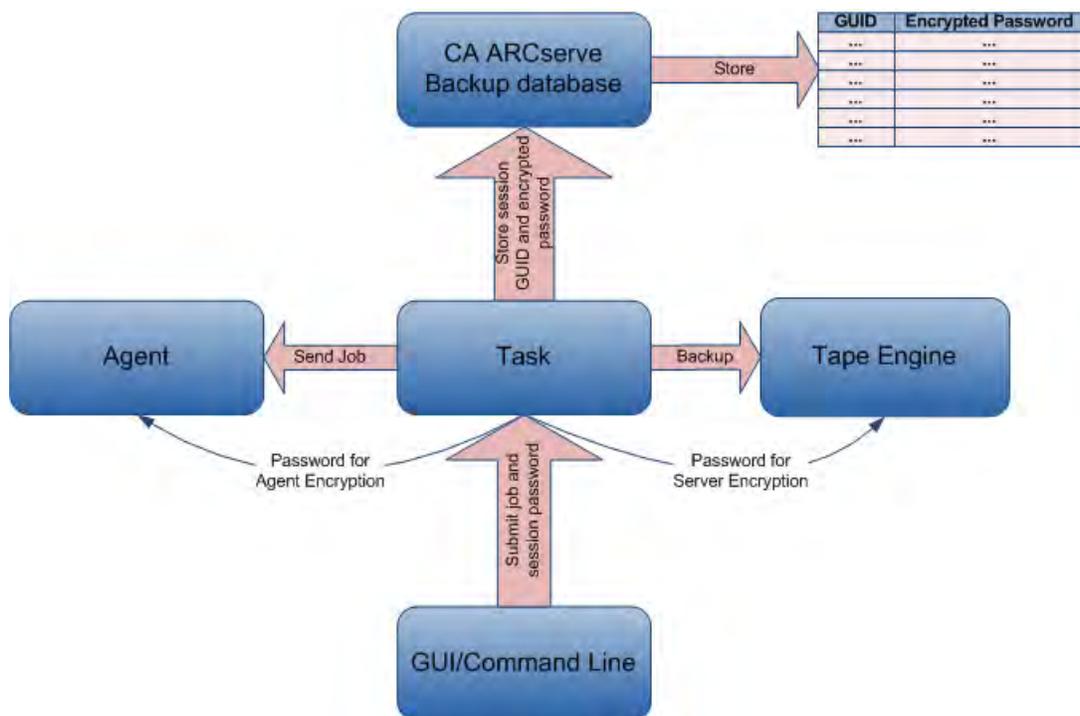
Note: To enable Password Management you must install and licence the CA ARCserve Backup Enterprise Module on the server where the job is to be executed. The password is saved to the CA ARCserve Backup database only when the CA ARCserve Backup Enterprise Module is installed and licensed.

For Server Side Encryption

The restore session reads the Dummy Session Header from the Tape Engine and if server side encryption was used, the session GUID will be extracted from the CA ARCserve Backup database.

For Agent Side Encryption

The restore session reads the Session Header from the Tape Engine and extracts the GUID from the CA ARCserve Backup database.



Change a Session/Encryption Password

An Activity Log warning message is generated seven days in advance of a job session password expiration.

Note: This procedure allows you to change only a Global Option password.

To change a session/encryption password

- 1. From the Job Status Manager, select the Job Queue tab.
- 2. Select a job and right-click.

3. From the right-click menu, select **Modify Encryption Password**.
The Encryption dialog opens.
4. Enter a session/encryption password.
5. Select the option **Save Current Session/Encryption Password into Database**.
6. (Optional) Enter the number of days that must elapse before you need to change the password.

Enable Password Management

When submitting a backup job, you have the option to set a session encryption password.

To enable password management

1. From the Backup Manager, select the Options button on the toolbar.
The Global Options dialog opens.
2. On the Encryption tab, enter a session encryption password.
3. Select the option **Save Current Session Encryption Password into Database**.
4. (Optional) Enter the number of days that must elapse before you need to change the password.
5. Select the Start button on the toolbar to submit the backup job and save the session encryption password to the CA ARCserve Backup database.

How User Profile Management Works

User Profile Management allows you to have different users access CA ARCserve Backup with different privileges. Using the User Profile Manager, you can assign individual users different roles with specific permissions. For example, you can have three users: one having an administrator role, one having a backup operator role, and one having a restore operator role. The ability to assign permissions based on role decreases the chances of an unauthorized user accessing the CA ARCserve Backup domain.

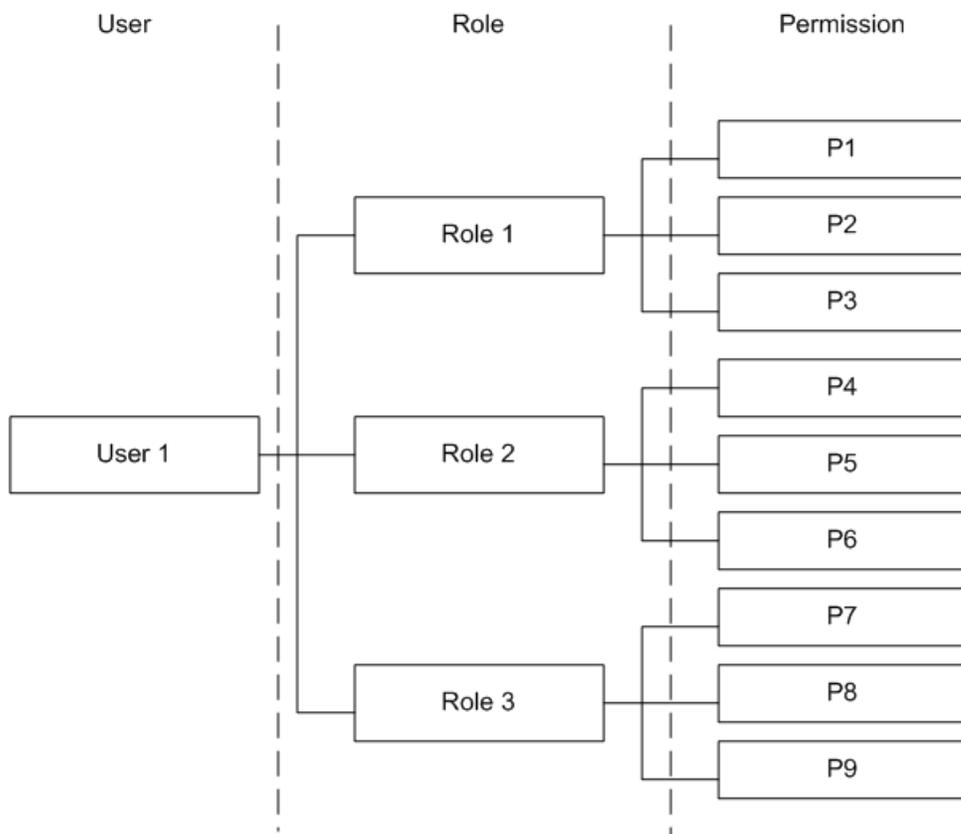
When you install CA ARCserve Backup, the caroot user profile is set up, with the Administrator group assigned to it by default. The Administrator group provides control over all CA ARCserve Backup functions operating within a given CA ARCserve Backup domain.

Note: To enable the enhanced User Profile Manager, role management, and Windows account support you must install and licence the CA ARCserve Backup Enterprise Module on the Primary Server. It is not necessary to install the CA ARCserve Backup Enterprise Module on Member Servers. If the licence expires on the Primary Server you will not be able to access the enhanced User Profile Manager.

Using the User Profile Manager, CA ARCserve Backup supports the following management functions for users and roles:

- Add a user.
- Delete a user.
- Change a user's password.
- Assign a user to a role.
- Delete a user from a role.
- Assign a role to a user.
- Delete a role from a user.

You can assign a user multiple roles, providing the user with a variety of permissions. The following diagram illustrates a user with multiple roles:



Roles and Permissions

You can assign a user multiple roles and each role consists of specific permission set. All users must have at least one role assigned to them. Some of the roles have very restricted permissions. For example, the Report Operator can only view and create reports, while the CA ARCserve Backup Administrator can perform all operations.

Note: Only the Administrator role can add or delete users.

Permission	Role						
	Admin	Backup	Restore	Device	Monitor	Report	Tape
Submit Jobs	X	X	X				
Tape and Device	X	X	X	X	X		X

Permission	Role						
	Admin	Backup	Restore	Device	Monitor	Report	Tape
Job	X	X	X	X	X		X
Log	X	X	X	X	X		X
Reports	X	X				X	X
Service	X	X	X	X	X		X
Media Pools	X	X	X	X	X		
Database	X	X	X				
Dashboard	X				X	X	
MMO	X	X					
Other	X	X	X	X	X	X	X

Submit Job Options Permission Details

The following table outlines the Submit Job Options permission details and identifies corresponding roles:

Submit Job Options	Role		
	Admin	Backup	Restore
Backup	X	X	
Restore	X		X
Compare	X	X	X
Scan	X	X	X
Merge	X	X	X
Generic*	X		
Count	X		
Purge	X		
Copy	X		

* **Note:** This is a job created using the Job Scheduler Wizard.

Tape and Device Operations Permission Details

The following table outlines the Tape and Device Operations permission details and identifies corresponding roles:

Tape and Device Operations	Role					
	Admin	Backup	Restore	Device	Monitor	Tape
View	X	X	X	X	X	X
Format/Erase	X	X		X		
Config FSD	X	X		X		
Config Groups	X	X		X		
Config Staging Groups	X	X		X		
Config DDD	X	X		X		
DDD Groups	X	X		X		
Retention	X			X		X
Compression	X			X		X
Eject	X			X		X
Rebuild	X			X		X
Mount	X			X		X
Import/Export	X			X		X
Clean	X			X		X
Rescan	X			X		X
View Properties	X			X		X
Set Auto Clean	X			X		X

Job Operations Permission Details

The following table outlines the Job Operation permission details and identifies corresponding roles:

Note: The Backup Operator and the Restore Operator can only modify, reschedule, run, stop or delete jobs that they submit. If the Ownership Checking Exemption Privilege permission is checked the Backup Operator and the Restore Operator can operate jobs submitted by any operator.

Job Operations	Role					
	Admin	Backup	Restore	Device	Monitor	Tape
View all Status	X	X	X	X	X	X
Add	X	X	X			
Modify	X	X	X			
Reschedule	X	X	X			
Run/Stop	X	X	X			
Delete	X	X	X			
Modify Username	X	X	X			
Run PFC	X	X				
View current job status	X	X	X			
Modify password	X	X				

Log Operations Permission Details

The following table outlines the Log Operations permission details and identifies corresponding roles:

Tape and Device Operations	Role					
	Admin	Backup	Restore	Device	Monitor	Tape
View Job History	X	X	X	X	X	X
View Activity Log	X	X	X	X	X	X
Delete Activity Log	X					
View Tape Log	X	X	X	X	X	X
Delete Tape Log	X					

	Role					
Tape and Device Operations	Admin	Backup	Restore	Device	Monitor	Tape
View Audit Log	X	X	X	X	X	X
Delete Audit Log	X					

Report Operations Permission Details

The following table outlines the Role Operations permission details and identifies corresponding roles:

	Role			
Report Operations	Admin	Backup	Report	Tape
View/Create	X	X	X	X
Design	X	X	X	X

Service Operations Permission Detail

The following table outlines the Service Operations permission details and identifies corresponding roles:

	Role					
Service Operations	Admin	Backup	Restore	Device	Monitor	Tape
View Service Status	X	X	X	X	X	X
Set Auto Start Engine	X					
Adjust CA ARCserve Backup System Account	X					
Config System engines	X					
Start/Stop all services	X					
Start/Stop specified services	X					
Start/Stop all services in domain	X					
Add/View Licenses	X					
Manage Licenses	X					

	Role						
Service Operations	Admin	Backup	Restore	Device	Monitor	Tape	
View service status	X						
Install/Uninstall options	X						

Media Pool Operations Permission Detail

The following table outlines the Media Pool Operations permission details and identifies corresponding roles:

	Role						
Media Pool Operations	Admin	Backup	Restore	Device	Monitor	Tape	
View Media Pools	X	X	X	X	X	X	X
Create new media pools	X	X					
Delete media pools	X	X					
Move Media between Scratch Set and Save Set	X	X					
Assign Media to Scratch Set and Save Set	X	X					
Remove Media from Scratch Set and Save Set	X	x					

Database Operations Permission Detail

The following table outlines the Database Operations permission details and identifies corresponding roles:

	Role			
Database Operations	Admin	Backup	Restore	Monitor
View media/sessions in database	X	X	X	X
View jobs in database	X	X	X	X

	Role			
Database Operations	Admin	Backup	Restore	Monitor
View devices in database	X	X	X	X
Delete media/sessions in database	X			
Delete jobs in database	X			
Delete devices in database	X			

Submit Job Options Permission Details

The following table outlines the Submit Job Options permission details and identifies corresponding roles:

	Role		
Submit Job Options	Admin	Backup	Restore
Backup	X	X	
Restore	X		X
Compare	X	X	X
Scan	X	X	X
Merge	X	X	X
Generic*	X		
Count	X		
Purge	X		
Copy	X		

* **Note:** This is a job created using the Job Scheduler Wizard.

MMO Operations Permission Detail

The following table outlines the MMO Operations permission details and identifies corresponding roles:

	Role	
MMO Operations	Admin	Backup
All MMO operations	X	X

Other Operations Permission Detail

The following table outlines the Other Operations permission details and identifies corresponding roles:

Other Operations	Role						
	Admin	Backup	Restore	Device	Monitor	Report	Tape
Configure Alert Manager	X	X	X	X	X	X	X
View Alert Manager	X	X	X	X	X	X	X
Use Diagnostic Manager	X	X	X	X	X	X	X

Extended Permissions

The extended permissions include:

Security Administrator

The Security Administrator permission is only selectable if CA ARCserve Backup Administrator role is selected. In order to perform user management task the Security Administrator must be selected.

Ownership Checking Exemption Privilege

The Ownership Checking Exemption Privilege is only selectable if the Backup or Restore Operator role is assigned to a user. If the Ownership Checking Exemption Privilege permission is checked the Backup Operator and the Restore Operator can operate jobs submitted by any operator.

Windows User Authentication

Windows User Authentication simplifies your user management by allowing users to log in to the CA ARCserve Backup domain with their Windows user login account information. Users are able to log in to CA ARCserve Backup after the CA ARCserve Backup administrator has added the user to the CA ARCserve Backup database. Any valid Windows user can be added as a user from the User Profile Manager. Window User Authentication is a two step process. The process is as follows:

- The user must be authenticated in the Windows domain.
- The user must be authenticated in the CA ARCserve Backup database.

Note: To make sure a Windows user with a blank password will not fail to log on to CA ARCserve Backup, you must configure a [Windows Security Setting Option](#) (see page 87).

Configure Windows Security Setting Option

To make sure a Windows user with a blank password will not fail to log on to CA ARCserve Backup, you must configure a Windows Security Setting Option.

To configure windows security setting option

1. From the Start menu select Control Panel.
The Control Panel opens.
2. Select Administrative Tools.
The Administrative Tools dialog opens.
3. Select Local Security Policy.
The Local Security Policy dialog opens.
4. Double-click **Accounts: Limit local account use of blank passwords to console logon only**.
5. Select Disable and click OK.
The Windows Security Setting Option is configured to accept blank passwords.

Log in to CA ARCserve Backup

When you open the CA ARCserve Backup Manager Console, you must log in to CA ARCserve Backup. The first time you log in to CA ARCserve Backup, you can log in as caroot, which has administrator privileges, and provide the appropriate password in the password field. Optionally, you can log in to CA ARCserve Backup using the Windows account that was provided when you installed CA ARCserve Backup, or with any Windows administrative account associated with the computer that you are logging in to.

After you log in, you can change the password for the caroot user and add new users. You can also add new users using the command line utility, `ca_auth.exe`. For information about `ca_auth.exe`, see the *Command Line Reference Guide*.

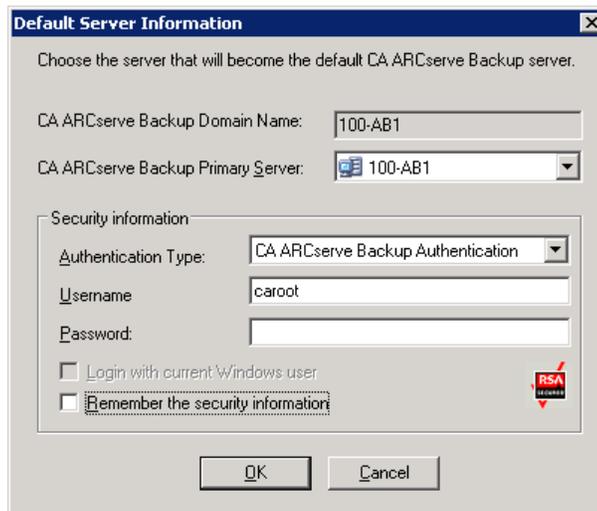
To log in to CA ARCserve Backup

1. Open the CA ARCserve Backup Manager Console.

To open the Manager Console, click Start on the toolbar, select Programs, CA, ARCserve Backup, and click Manager.

The Default Server Information page appears.

2. To change the default server or specify a different server, select a server from the CA ARCserve Backup Primary Server list. If the target server does not appear in the drop-down list, you can input the host name or IP address of the server in the CA ARCserve Backup Primary Server list.



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

You must license the CA ARCserve Backup Enterprise Module to have the capability to log in using Windows Authentication and other Windows accounts registered to the CA ARCserve Backup server specified in the CA ARCserve Backup Primary Server field.

By default, CA ARCserve Backup does not remember your security information. To save the user name and password information that you entered for this server, you must explicitly select Remember the security information. If you do not save this information, CA ARCserve Backup prompts you to provide CA ARCserve Backup security credentials the first time you open managers, wizards, and so on, and you must provide a CA ARCserve Backup user name and password.

4. Enter caroot in the User Name field, the appropriate password in the Password field, and click OK.

The first time you log in to CA ARCserve Backup, a tutorial, called My First Backup, appears. This tutorial lets you become familiar with the basics of backing up and restoring data in a controlled and directed way. This tutorial appears automatically only the first time you log in. However, you can access My First Backup from the Help menu.

Add a Windows User

Before users can be assigned a role, you must add them to the CA ARCserve Backup database. A Windows user can log in using their standard Windows log in.

To add a Windows user

1. From the CA ARCserve Backup Manager, select Administration, User Profile.

The User Profile manager opens.

2. Click the Add User button on the toolbar.

The Add User Dialog opens.

3. On the General tab, select Windows Authentication and enter the following information:

Username

Enter the new user name in the following format: domain\username. Alternatively, you can click the Search button for a list of available users.

Description

(Optional) In the description box, enter information about the user account.

4. Select the Roles tab, assign a role for the user.

Note: A minimum of one role must be assigned to a user when the user is created.

5. Click OK.

The Windows user is added to the CA ARCserve Backup database.

Notes:

- Any valid Windows user can be added to CA ARCserve Backup from the User Profile Manager.
- Only the CA ARCserve Backup Administrator with a Security Administrator role can add a user.
- Note: To make sure a Windows user with a blank password will not fail to log on to CA ARCserve Backup, you must configure a [Windows Security Setting Option](#) (see page 87).

Add a CA ARCserve Backup User

Before users can be assigned a role, you must add them to the CA ARCserve Backup database.

To add a CA ARCserve Backup user

1. From the CA ARCserve Backup Manager, select Administration, User Profile.

The User Profile manager opens.

2. Click the Add User button on the toolbar.

The Add User Dialog opens.

3. On the General tab, select CA ARCserve Backup Authentication and enter the following information:

Username

Enter the new user name. You cannot use the "\" character.

Password

You must enter and confirm the password.

Description

(Optional) In the description box, enter information about the user account.

4. Select the Roles tab, assign a role for the user.

Note: A minimum of one role must be assigned to a user when the user is created.

5. Click OK.

The Windows user is added to the CA ARCserve Backup database.

Notes:

- Any valid Windows user can be added to CA ARCserve Backup from the User Profile Manager.
- Only the CA ARCserve Backup Administrator with a Security Administrator role can add a user.

Change Your Password From the Home Page GUI

All users can change their password from the CA ARCserve Backup Home Page GUI or from the User Profile Manager.

Important! One limitation that exists if the Enterprise Module license is expired is that users, other than caroot, do not have access to the User Profile Manager and therefore cannot change their password in the User Profile Manager. They must change their password from the CA ARCserve Backup Home Page GUI.

To change your password from the Home Page GUI:

1. Open the CA ARCserve Backup Manager.

The CA ARCserve Backup Home Page GUI opens.

2. From the menu, select File and Change Password.

The Change User Password dialog opens.

3. Enter the password fields provided and click OK.

If the password credentials are met, your password is successfully changed and a message dialog displays.

4. Click OK on the message dialog and restart all CA ARCserve Backup Managers that are connected to the server.

Modify Windows User Properties

When necessary, you can change a user's assigned roles or suspend or activate the user account.

To modify Windows user properties

1. From the CA ARCserve Backup Manager, select Administration, User Profile.

The User Profile manager opens.

2. Click the Properties button on the toolbar.

The User Properties Dialog opens.

3. On the General tab, choose from the following properties:

Description

Add a information in the description field about the user.

Status

Specify if the user account is active or suspended.

4. On the Role tab, add or delete the roles assigned to the user.

Modify CA ARCserve Backup User Properties

When necessary, you can change a user's assigned roles or suspend or activate the user account.

To modify CA ARCserve Backup user properties

1. From the CA ARCserve Backup Manager, select Administration, User Profile.

The User Profile manager opens.

2. Click the Properties button on the toolbar.

The User Properties Dialog opens.

3. On the General tab, choose from the following properties:

Description

Add information in the description field about the user.

Status

Specify if the user account is active or suspended.

Password

Specify a new password.

Confirm Password

Re-enter the new password.

4. On the Role tab, add or delete the roles assigned to the user.

Delete a User

Use the following steps when you want to delete a user from CA ARCserve Backup.

To delete a user

1. From the CA ARCserve Backup Manager, select Administration, User Profile.

The User Profile manager opens.

2. Select the user you want to delete and click the Delete button on the toolbar.

The delete confirmation box appears.

3. Select Yes.

The user is deleted

Notes:

- Only the CA ARCserve Backup Administrator with a Security Administrator role can delete a user.
- The CA ARCserve Backup user caroot cannot be deleted.
- You cannot delete the current user.

Add a User to a Role

You can add users to a particular role.

Note: Before a user can be assigned a role, you must add them to the CA ARCserve Backup domain.

To add a user to a role

1. From the CA ARCserve Backup Manager, select Administration, User Profile.
The User Profile manager opens.
2. From the Security tree, select Roles.
3. Highlight a role and click the Properties button on the toolbar.
The Role Properties dialog opens.
4. Select the Users tab and click Add.
The Select Users dialog opens.
5. Select a user and click OK. Alternately, you can double click a user.
The Role Properties dialog re-opens.
6. Click OK.
The user is added to the role.

Remove a User from a Role

You can remove users from a particular role.

To remove a user from a role

1. From the CA ARCserve Backup Manager, select Administration, User Profile.

The User Profile manager opens.

2. From the Security tree, select Roles.

3. Highlight a role and click the Properties button on the toolbar.

The Role Properties dialog opens.

4. Select the Users tab.

The Select Users dialog opens.

5. Select a user and click and click Remove.

6. Click OK.

The user is deleted from the role.

Notes:

- You cannot remove a user that is assigned only one role.
- The caroot user cannot be removed from the user list.

Using the Audit Log

The Audit Log maintains a log of critical CA ARCserve Backup operations. For example, user login and logout information, adding a job, deleting a job, and so on.

Note: To view the Audit Log you must install and licence the CA ARCserve Backup Enterprise Module. If the licence expires the Audit Log will not be visible in the Job Status Manager

Filter the Audit Log

Use the filter options to refine your Audit Log search.

To filter the Audit Log

1. Open the Job Status Manager.

Select the Audit Log tab.

Expand the header bar by clicking .

Choose from the following filter options:

Event Types

Specify the type of event to sort by. The options are Success audit and Failure audit.

Source Machine

Specify the machine to audit. The default is All.

Event

Specify what event you want to view. You can choose a specific user task or All user tasks.

Note: The header bar will turn yellow if there is a change made to the type of event you want to view, indicating that the advanced filter was used.

User

Specify the user whose audit log you want to view. The default is All.

Note: The header bar will turn yellow if a user is specified, indicating that the advanced filter was used.

Source Process

Specify a specific CA ARCserve Backup process. The default is All.

From

Specify the start day and time of an event. The option include First Event and Events On.

To

Specify the end day and time of an event. The option include First Event and Events On.

2. Click Update.

The filtered results are displayed in the Properties panel.

View the Audit Log

Use the Audit Log to identify patterns or areas of repeated tasks.

To view the audit log

1. Open the Job Status Manager.
2. Select the Audit Log tab.

The Properties panel displays the audit log.

More information:

[Filter the Audit Log](#) (see page 97)

View an Audit Log Record

You can view the details of a specific audit log.

To view an audit log record

1. Open the Job Status Manager.
2. Select the Audit Log tab.
3. Select the audit record you wish to view.
4. Right click and select Properties. Alternately, double click the record.

The Audit Record Properties dialog opens.

5. On the Audit Record Properties dialog the following options are available:

Prev

Navigate to the previous audit record.

Next

Navigate to the next audit record.

Copy

Copy all the audit record properties to the clipboard.

6. Click OK.

The Audit Record Properties dialog closes.

Copy Audit Log Records

You can copy the audit log records in list format to the clipboard.

To copy audit log records

1. Open the Job Status Manager.
2. Select the Audit Log tab.
The Properties panel displays the audit log.
3. Select the audit log records you want to copy.
4. Press Ctrl+C to copy the records to the clipboard.
5. Open a text editing application and past the copied records.

Export Audit Log

You can export all audit records or selected audit records to a text file.

To export an audit log

1. Open the Job Status Manager.
2. Select the Audit Log tab.
The Properties panel displays the audit log.
3. From the Print button on the toolbar select Print to File.
The Save As dialog opens.
4. Enter a file name and click Save.
The Audit Log is saved as a text file.

Print an Audit Log

The Audit log can be printed to a local printer.

To print an audit log

1. Open the Job Status Manager.
2. Select the Audit Log tab.
The Properties panel displays the audit log.
3. From the Print button on the toolbar select Print.
The Print dialog opens.
4. Click OK.
The Audit Log is printed.

Delete Audit Log

To delete the audit log

1. Open the Job Status Manager.
2. Select the Audit Log tab.
The Properties panel displays the audit log.
3. Click the Delete button on the toolbar.
The Delete Audit Log dialog opens.
4. Select delete options.
Choose from the following delete options:

Entire log table

Delete all records in the Audit Log.

Partial

Delete records in a specified time period.

Older than

Enter a specific time based on the following criteria: 1 to 365 days, 1 to 54 weeks, 1 to 12 months, and 1 to 10 years.

5. Click OK.
The Audit Log records are deleted.

Configure System Event Log

You can add the Audit Log information to the system event log.

To configure the system event log

1. From the Sever Admin, select the Configuration button on the toolbar.
The Configuration dialog opens.
2. Select the Log tab.
3. Select the Enable messages logging into Windows Event Log checkbox.
The Audit Log information is included in the Windows Event Log.

More information:

[Event Log Configuration \(Windows Servers\)](#) (see page 467)

Create an Audit Log Report

You can generate an Audit Log report from the Report Manager.

More information:

[Generate Reports Using Report Manager](#) (see page 618)

Data Security

Data security is the process of protecting sensitive information from unauthorized access or use. Data security helps you to ensure privacy and protect personal data. CA ARCserve Backup ensures that all sensitive data that is stored in a computer or on removable media cannot be read or compromised by any individuals without proper authorization. Often these removable media can contain highly sensitive information which could be lost while in transit between company data centers and their off site storage vaulting service facilities. The data on these media needs to remain secure, even when in transit.

Encryption and Decryption

Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. Decryption is the decoding or conversion of encrypted data into plain text and reversing the encryption process.

The CA ARCserve Backup data protection solution uses secure, industry standard encryption algorithms in various components to achieve the maximum security and privacy of customer data. Starting with CA ARCserve Backup r12, the Windows client agents will use a 256-bit AES algorithm provided in the RSA BSAFE cryptographic library for all encryption purposes. Any data collected by earlier versions of CA ARCserve Backup agents will use either a 168-bit 3DES or a proprietary CA encryption algorithm for encryption purposes. In addition, the Windows base product also uses the same 256-bit AES algorithm to store any sensitive information on the CA ARCserve Backup server.

The AES (Advanced Encryption Standard) feature has been developed to replace the DES (Data Encryption Standard) and is designed to be more secure than DES. The AES is a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.

Note: Encryption and compression are not supported on deduplication devices.

Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards (FIPS) are a set of standards that describe document processing, provide standard algorithms for searching, and provide other information processing standards for use within government agencies. The National Institute of Standards and Technology (NIST) issued the 140 Publication Series to coordinate the requirements and standards for cryptographic modules which include both hardware and software components for use by departments and agencies of the United States federal government.

Security Requirements for Cryptographic Module (FIPS 140-2) specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information within computer and telecommunication systems.

CA ARCserve Backup and FIPS Compliance

CA ARCserve Backup uses FIPS-compliant algorithms for backing up and restoring sensitive information such as username and password credentials.

- If you choose to encrypt your data during backup to a disk or tape, the algorithms used to encrypt this data will be FIPS-compliant.
- During backup time, the username and password will be sent to the CA ARCserve Backup server agent (running on the server to be protected). This username and password will be encrypted using FIPS-compliant algorithms and transferred to the agent.
- CA ARCserve Backup also supports tape drives (from external third-party vendors) that provide FIPS-compliant hardware encryption. This is in addition to FIPS-compliant tape or disk encryption provided by the CA ARCserve Backup software.
- CA ARCserve Backup provides additional agents and options that also use FIPS-compliant algorithms to support data encryption. These agents and options include: Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint, and CA XOssoft.

Change the Current Encryption Algorithm

The current encryption algorithm (AES256) used for CA ARCserve Backup can be changed by modifying the CryptoConfig.cfg file. This file includes a list of all supported encryption algorithms for CA ARCserve Backup products installed on your machine. You can change the current encryption algorithm to any of the alternate candidate algorithm values that are listed. This change will affect all the CA ARCserve Backup products (Agents, Base, Options) installed on that machine.

To change the current encryption algorithm

1. Run the cstop.bat script to stop all services before making the change.
ProgramFiles\CA\ARCserve Backup\cstop.bat
2. Change the current encryption algorithm value to one of the candidate values.
ProgramFiles\CA\SharedComponents\ARCserve Backup\CryptoConfig.cfg
3. Run Configencr.exe to transfer the encrypted repositories to use the new encryption algorithm.
ProgramFiles\CA\ARCserve Backup\Configencr.exe
4. Run the cstart.bat script to start all services after making the change.
ProgramFiles\CA\ARCserve Backup\cstart.bat

CA ARCserve Backup Data Encryption

CA ARCserve Backup provides the flexibility to use encryption to protect sensitive data during various stages of the backup process. Generally, during the backup process, the sooner the data encryption occurs, the more secure your information will be. However, speed, performance, and scheduling restrictions are also factors to consider when choosing the best approach to securing your data.

The three different ways to encrypt data in a backup job are:

- Encryption at the agent server (or source) prior to the backup process
- Encryption at the CA ARCserve Backup server during the backup process
- Encryption at the CA ARCserve Backup server during the migration process (for a staging job)

These encryption options are accessible from the Backup Media tab on the Global Options dialog for the Backup Manager. From this dialog you can choose to encrypt the data at the agent, at the backup server (during backup), or at the backup server (during migration).

You can also create a session encryption password that is saved to the CA ARCserve Backup database. This password is used to encrypt session data. For more information about passwords, see the topic [How Password Management Works](#) (see page 75).

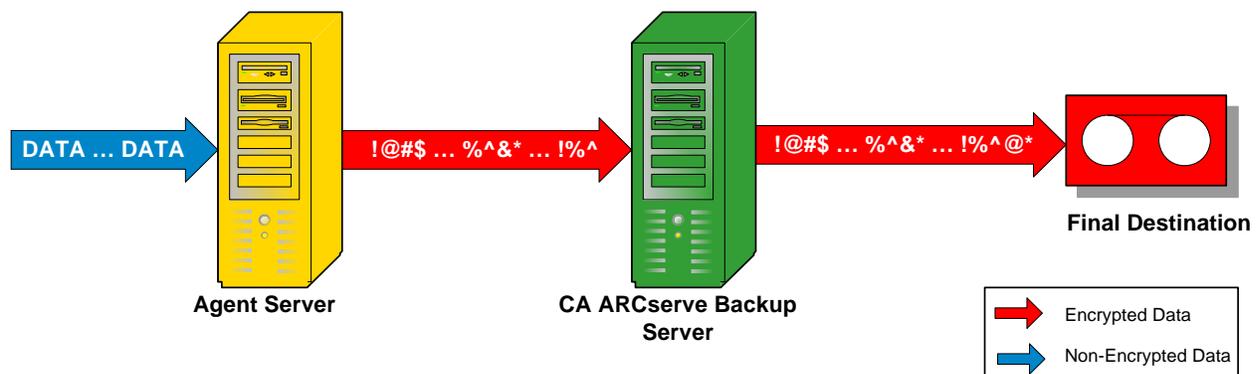
Note: CA ARCserve Backup will only encrypt data that is not already encrypted. If at any stage in the process CA ARCserve Backup detects that the data has already been encrypted, it will not attempt to encrypt it again. Since data deduplication is a form of encryption, you cannot encrypt data saved to a deduplication device.

In addition, there are also two basic methods for encrypting data; hardware encryption and software encryption. The advantages of hardware encryption are speed and improved CPU performance. Encryption using software is slower than encryption using hardware and can result in a larger backup window. By using hardware encryption, you can also avoid unnecessary CPU cycles on either the agent server or the backup server and the drive can compress the data before encrypting.

If you select to have your data encrypted during the backup or migration process, CA ARCserve Backup has the ability to detect if the final destination media (tape) is capable of hardware encryption and by default will automatically choose that hardware method if available.

Data Encryption at the Agent Server

Data can be encrypted at the CA ARCserve Backup agent server (agent server), prior to the actual backup process. The advantage of this method is that it does not transfer un-encrypted data from one location to another at all. However, this method puts added CPU cycles for encrypting the data on the agent server.



Data Encrypted at Agent Server Prior to Backup

Not all CA ARCserve Backup agents have the capability to encrypt data prior to transferring it to the CA ARCserve Backup server.

The following CA ARCserve Backup agents support at the agent server data encryption:

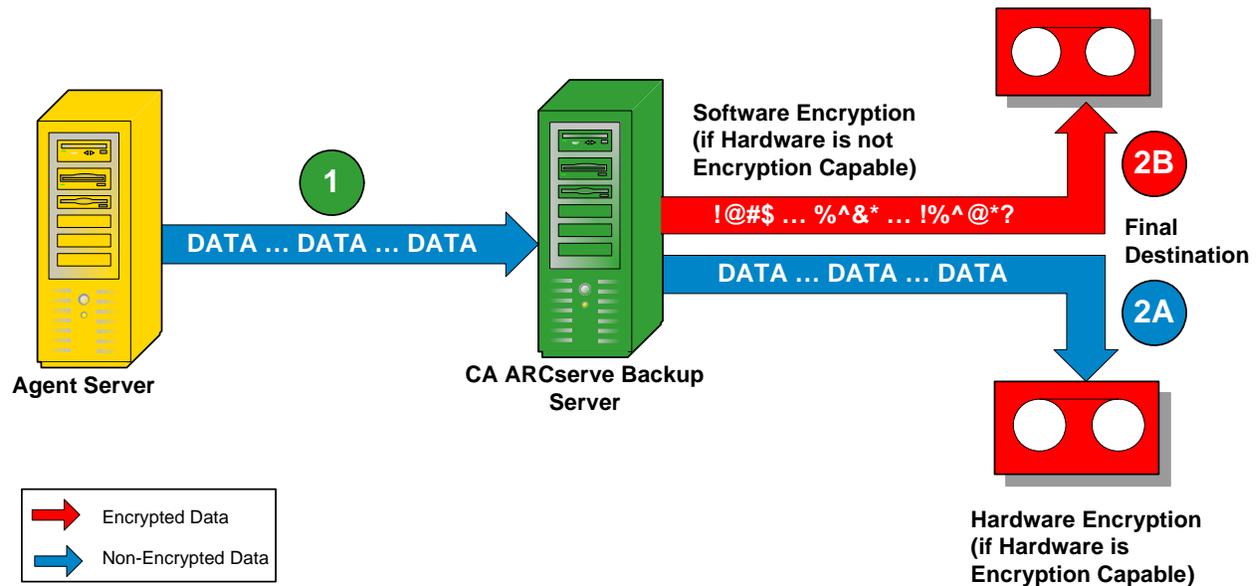
- All CA ARCserve Backup file system agents
- CA ARCserve Backup Agent for Microsoft Exchange
- CA ARCserve Backup Agent for Microsoft SQL Server

The following CA ARCserve Backup agents do not support at the agent server data encryption:

- CA ARCserve Backup Agent for IBM Informix
- CA ARCserve Backup Agent for Lotus Domino
- CA ARCserve Backup Agent for Microsoft SharePoint
- CA ARCserve Backup Agent for Oracle
- CA ARCserve Backup Agent for SAP R3 for Oracle

Data Encryption During Backup

Data can be encrypted at the CA ARCserve Backup server, during the backup process. Using this method, un-encrypted data is transferred from the agent server to the CA ARCserve Backup server. CA ARCserve Backup will then detect if the final destination media is capable of hardware encryption or not. If it is hardware encryption capable, then the un-encrypted data is transferred to the final destination media where it is then encrypted. This is the preferred and default method because it is faster and does not interfere with the backup window. If CA ARCserve Backup detects that the final destination media is not capable of hardware encryption, it will then perform software encryption of the data prior to transfer to the final destination media.

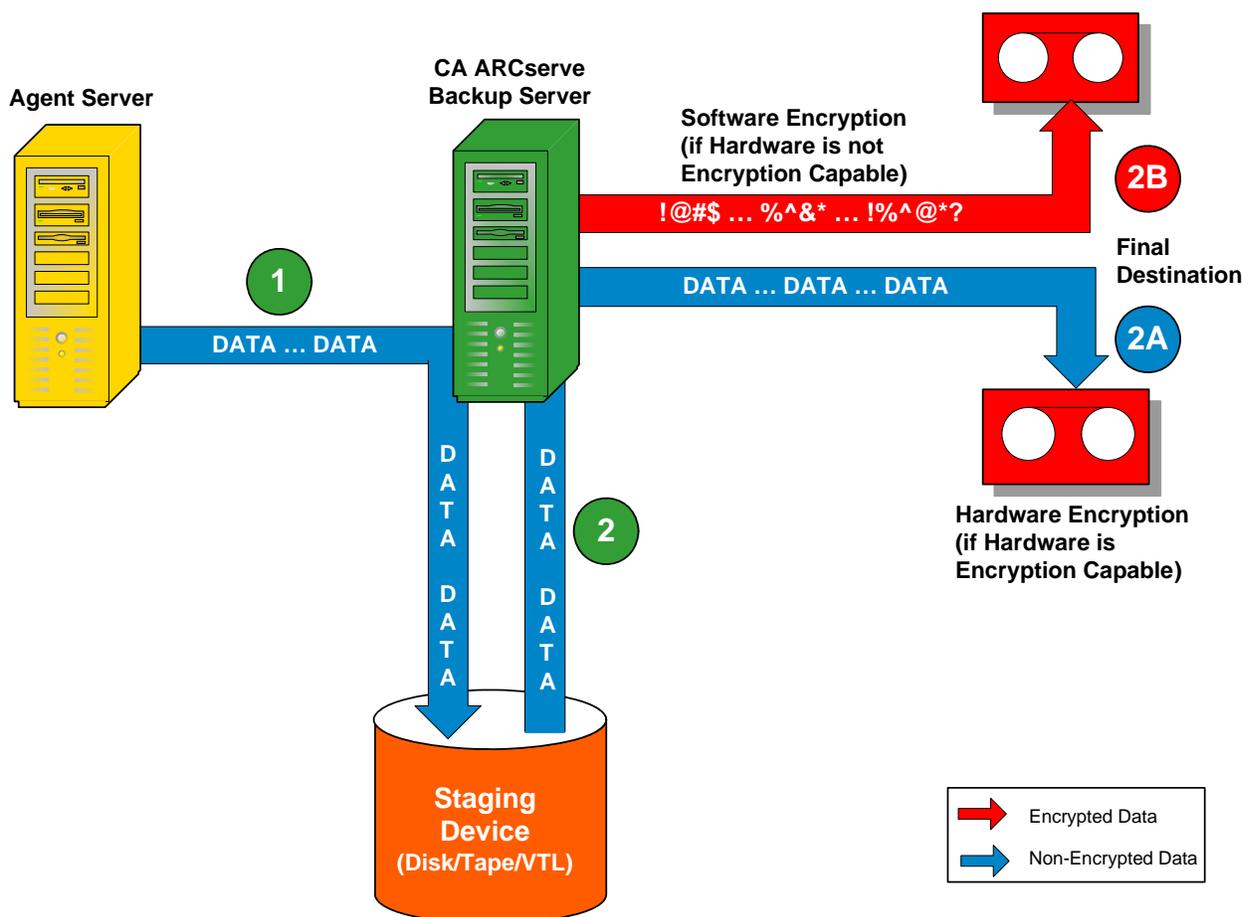


Data in Encrypted at ARCserve Server During Backup

Data Encryption During Migration

Data can be encrypted at the CA ARCserve Backup server, during to the migration process of a staging job.

Using this method, un-encrypted data is transferred during the backup process of a staging job from the agent server through the CA ARCserve Backup server to the staging device. The staging device can either be a disk, tape, or virtual tape library (VTL). When the data is ready for the migration process, CA ARCserve Backup will then detect if the final destination media is capable of hardware encryption or not. If it is hardware encryption capable, then the un-encrypted data is transferred from the staging device to the final destination media where it is then encrypted. This is the preferred and default method because it is faster and does not interfere with the migration window. If CA ARCserve Backup detects that the final destination media is not capable of hardware encryption, it will then perform software encryption of the data prior to migration to the final destination media.



Data in Encrypted at ARCserve Server During Migration

How You Manage Media

Effective media management provides valuable preparation for reliable backup and recovery performance. The type of media can be most types of SCSI or Fibre-attached removable storage.

Because functions such as tracking files to specific storage media are important requirements of your organization's daily production routine, effective media management requires that you know the contents and location of all removable media, such as magnetic tape. CA ARCserve Backup allows you to track your media through the Device Wizard and the Device Manager. Both the Device Manager and the Device Wizard allow you to manage and track your media easily.

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.

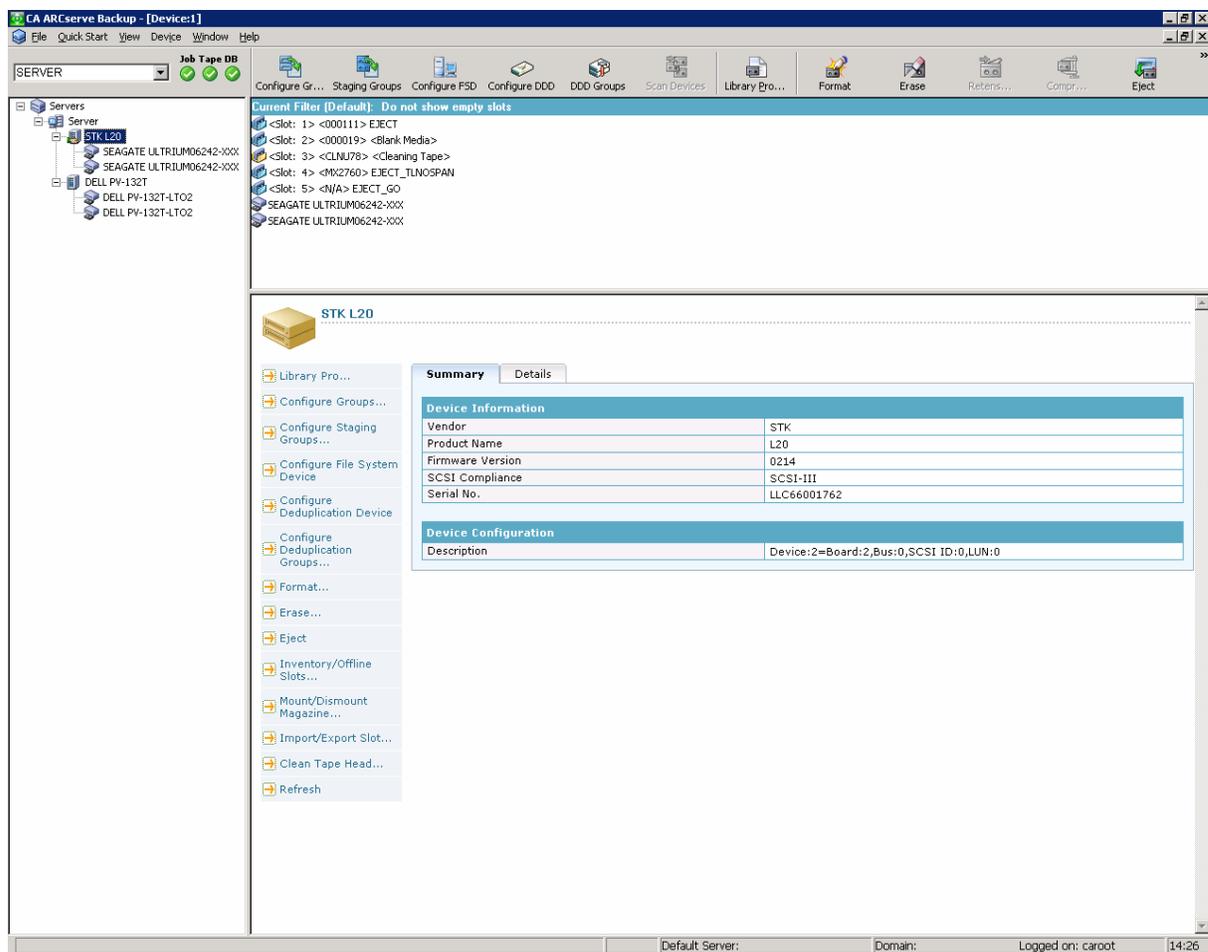
8. The schedule screen that appears lets you choose to run the device command immediately or schedule it for a later date and time. Select Run Now, and click Next to run the job immediately.

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 a Device Group

The Device Manager provides you with information about standalone Tape Drives, on the right side of the Device Manager window.



If you have more than one storage device connected to your network machine, CA ARCserve Backup lets you group the devices. This allows you to have one group perform a backup, while another group performs a restore operation, in a process known as parallel streaming.

If you have several devices in a group, and your job spans more than one media, the Device Manager can automatically span the media for you. You can then submit large backup jobs to CA ARCserve Backup and automatically span multiple media until the jobs are complete.

For example, if you have two media groups, GROUP1 (consisting of one storage device) and GROUP2 (consisting of two storage devices), and you have a large backup job that requires more than one media, you can insert blank (formatted) media into each GROUP2 drive and CA ARCserve Backup automates the media spanning for you. Without media spanning, you must change the media manually.

Note: For deduplication, device groups can contain only one deduplication device.

To configure a device group

1. In the Device Manager, click Configure Groups to open the Device Group Configuration dialog.
2. To assign a device to a new group, highlight it, and click Remove.
3. Click New to create a new group.
4. Enter a name for the new group, and click OK. The new group appears in the Groups field.
5. Highlight both the device and the new group, and click Assign to assign the device to the new group.
6. Click OK.

Important! If you are managing devices that are connected to remote UNIX or Linux servers, the Device Group Configuration dialog opens in read-only mode.

Back Up and Restore Data

Backing up and restoring your data is essential to the success of your organization. By efficiently and dependably protecting and retrieving files, CA ARCserve Backup helps you to ensure that your most valuable asset, your data, is protected.

This section introduces you to the essential CA ARCserve Backup functions of backing up and restoring and describes how to submit jobs using the intuitive Backup and Restore Wizards.

Backup Requirements Plan

Before you use CA ARCserve Backup for the first time, we recommend that you plan your backup requirements. You should consider the following:

- How much data do you need to back up?
 - What is the current disk capacity in your environment?
 - What is the server and data growth you anticipate over the next year?
- How do you want to manage the media you are using for backup?
- How do you plan to store your data? Are you using magnetic tape or does the stability of WORM media better suit your needs?

Add Computers to the Preferred Shares/Machines Tree

The Preferred Shares tree consists of a collection of your favorite backup shares. A share is a shared drive, directory, or entire system. You can manually add individual share points to the Preferred Shares tree; the share point is remembered and displayed regardless of the status of the network connection. This provides a quick access to commonly used shares on your machines. You can also setup preferred machines, which enables you to browse, backup, or restore all of the shared drives on a machine under a single machine.

When you set up a backup job, you must log in to and provide valid credentials on the preferred system to submit the job.

Note: CA ARCserve Backup does not support logging in to systems with passwords that are greater than 23 characters. If the password on the system you are attempting to log in to is greater than 23 characters, you must modify the password on the agent system such that it is 23 characters or less, and then you can log in to the agent system.

To add computers to the Preferred Shares/Machines tree

1. From the Source tab on the Backup Manager window, right-click the Preferred Share/Machines object and select Add Object from the pop-up menu

The Add Preferred Shares dialog opens.

2. Select a Network Provider.

Enter a share name in Uniform Naming Convention (UNC) format.

Example: \\MACHINE\SHARE

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.

Click Add.

The computer is added to the Preferred Shares tree.

3. To add more computers, repeat the previous step.
4. When you are finished adding computers, click Close.

Backup Media Rotations and Scheduling Options

Typically, the most convenient time for you to schedule backup operations is after business hours, when backup processing does not use valuable network bandwidth. CA ARCserve Backup provides you with the tools you need to automate your backup operations.

CA ARCserve Backup allows you to establish a schedule so that your backup automatically repeats at regular intervals, allowing you to regularly and reliably back up your data at any time. The Backup Manager provides you with scheduling options and rotation schemes to help you establish your automatic backup strategy.

Note: If you are using WORM media, you cannot use rotation schemes. By definition, WORM media cannot be overwritten, so you cannot recycle it in a rotation scheme or a media pool.

Rotation Schemes

You can configure backup jobs using custom schedules, using the pre-defined rotation schemes provided by CA ARCserve Backup, or specifying your own rotation parameters. You can select a repeat method and choose from among the following three backup methods in your rotation scheme:

- **Full Backup**--Backs up all of your files. This backup method requires more time to process compared to incremental or differential backups. However, because all of your data is backed up, this strategy requires only the last backup media to restore your data completely.
- **Incremental Backup**--Backs up only those files that have changed since the last full or incremental backup was performed. Since this strategy backs up only new or newly changed files, incremental backups require less time to process. However, this strategy requires the full media set and every incremental set, including the latest set, to fully restore your data after a disaster.
- **Differential Backup**--Backs up only those files that have changed since the last full backup was performed. Since files that were backed up in the last differential job are backed up again, differential backup jobs require more time to process than incremental backup jobs. However, this strategy requires only two sets of media to restore a differential backup, the full media set, and the differential media set.

Note: For any rotation scheme that you use, you should include at least one full backup per week.

Media Pools

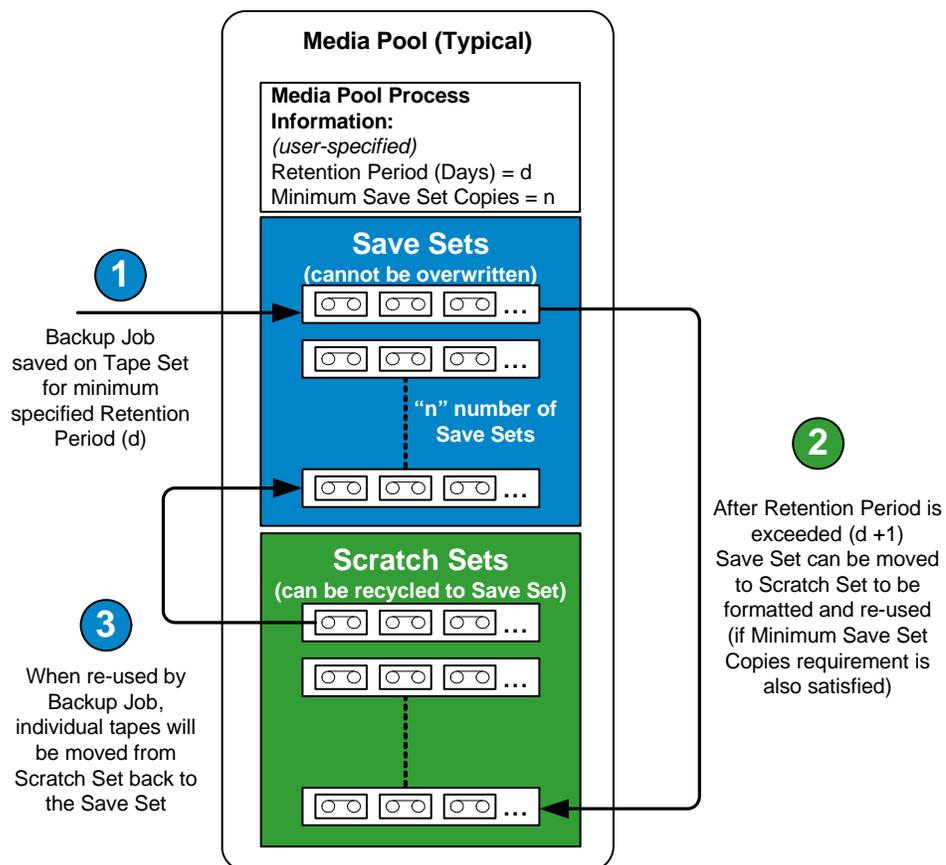
To prevent the accidental overwriting of needed data, CA ARCserve Backup manages media for rotation schemes in media pools. Media pools are logical collections of rewriteable, removable storage media managed as a single unit.

Important! Deduplication devices cannot be assigned to media pools.

A media pool is a collection of backup media (tapes) that is set aside for a specific job and managed as a unit. A media pool is a set of tapes that is logically grouped and used exclusively for a particular recurring backup job. Within CA ARCserve Backup each media pool is automatically divided into a Scratch Set and a Save Set. Any media in a Save Set cannot be overwritten until certain user-specified criteria are met. This prevents the possibility of inadvertently overwriting a tape before adequate backups are preserved. After the user-specified criteria is met, the Save Set becomes a Scratch Set and is recycled to be used again (overwritten).

Once the media has passed certain specified criteria, such as a minimum number of media in the Save Set and a minimum retention period, the media is moved to the Scratch Set. The retention period is the number of days media is kept in the Save Set of a media pool. When these criteria are met, the media is moved from the Save Set to the Scratch Set and is made available for use.

The Media Pool Manager lets you create and maintain the CA ARCserve Backup media pools. Each media pool is assigned a name, and is organized according to serial numbers. The serial numbers assigned are permanent. If you use a device with a bar code reader, the bar code labels are used as the serial number of the media. Media pools are organized by the range of serial numbers of the media they contain. Media pools apply to every media, regardless of which backup type and method were selected.



Create Media Pools

You can use automatic rotation schemes to control the media you use during backups. However, if you choose not to use the automatic features, the Media Pool Manager is an indispensable tool to efficiently schedule the maintenance and recycling of media. The Media Pool Manager helps you to organize your media into media pools, similar to those used in rotation schemes. Just as in rotation schemes, the media pools you create are collections of rewriteable storage media managed as a single unit.

Note: If you are using WORM media, media pool options are disabled. By definition, WORM media cannot be overwritten, so you cannot recycle it in a rotation scheme or a media pool.

For more information about media pools, see "Managing Devices and Media."

To create media pools

1. From Administration menu in the Navigation Bar on the Home Page, click Media Pool.

The Media Pool Manager opens.

2. From the Media Pool Manager, click New.

The Media Pool Configuration dialog appears.

Note: CA ARCserve Backup detects and assigns media serial numbers when media is formatted and placed in a specific media pool.

3. Enter a name for the media pool in the Pool Name field. Fill in the remaining fields appropriately.
4. Click OK when you are finished.

The new media pool you created appears in the Media Pool Manager. You can now assign media to the Save Sets and Scratch Sets of this media pool.

Wizards

With CA ARCserve Backup, performing backup and restore operations is quick, easy, and foolproof. CA ARCserve Backup wizards guide you smoothly through each step. The following sections provide the basic steps required to back up and restore files from your local machine.

Back Up Data Using the Backup Wizard

The Backup Wizard guides you through the steps required to perform the most basic of the CA ARCserve Backup functions - backing up your files - quickly and simply.

To use the Backup Wizard, you must be logged in to a CA ARCserve Backup primary or stand-alone server and have at least one device identified as a storage location for backup jobs.

Note: When you submit a backup job using the Backup Wizard, the destination device must be connected to a primary server or a stand-alone sever. The Backup Wizard does not support submitting a backup job to a device that is connected to a member server.

1. From the Protection & Recovery menu in the Navigation Bar on the Home page, click Backup Wizard.

The Backup Wizard Welcome screen appears.

2. Click Next.

The Login screen appears.

3. Select the server to which you want to connect, and enter your user name and password. Click Next.

4. Select the files you want to back up. The Browser displays the machine tree from which you can select domains, machines, volumes (drives), shares, directories, and files for backup. To select data to back up, click the green box next to your selection.

Select the CA ARCserve Backup home directory to back up the database automatically.

5. To back up your machine, expand the Windows Systems object, browse to your system, click the green box next your system, and click Next.
6. The Backup Wizard prompts you to choose the backup destination by selecting the media for the backup. Select the appropriate media and click Next.

Note: You can use any type of media or a media pool for your backup job. If you are using WORM media, CA ARCserve Backup appends the backup sessions to the existing data on the media, because you cannot overwrite or erase WORM media.

7. The Backup Options screen allows you to customize your backup job. You can specify a full backup or an incremental backup, and you can back up with verification and compression. Select the appropriate Backup Method, and click Next.
8. Verify that the security information is correct, and click Next.

9. The schedule screen lets you choose to run the backup job immediately or schedule it for a later date and time. To start the job immediately, select Run Now, and click Next.

Note: If you choose to schedule your job, CA ARCserve Backup allows you to establish a schedule so that your backup repeats at regular intervals. To check the status of a scheduled job, you can view the Activity Log to review the details of the backup.

10. The last screen allows you to enter a description for your job and specify whether you want to track your job from the Job Monitor. This option is enabled by default.
11. Click Finish to submit the job.

You have just completed performing a basic backup operation. You can see firsthand how easy it is to use CA ARCserve Backup to accomplish your most important tasks.

Restore Data Using the Restore Wizard

The CA ARCserve Backup Restore Wizard makes the second portion of the data storage process - restoring your files - quick and easy.

Before you restore data, verify the status of your backup job to ensure that it is complete. After you have verified that you have a complete backup, you are ready to restore your data.

To use the Restore Wizard, you must be logged in to a CA ARCserve Backup primary or stand-alone server.

Note: When you submit a restore job using the Restore Wizard, the backup data must be stored on a device that is connected to a primary server or a stand-alone sever. The Restore Wizard does not support submitting a restore job from a device that is connected to a member server.

To restore data using the Restore Wizard

1. From the Recovery & Protection menu in the Navigation Bar on the Home Page, click Restore Wizard.
The Restore Wizard Welcome screen appears.
2. Click Next to continue.
The login dialog appears.
3. In the login dialog, select the server where you want to connect, enter your user name and password, and click Next.

4. The next screen allows you to choose a restore method. You can choose to Restore by Session or Restore by Query. The Restore by Query option is useful if you do not know the exact location of the data you want to restore. Select the appropriate restore method, and click Next.
5. The next screen lets you browse the database to find the backup sessions you want to restore. Identify the media containing your backup, click the green box next to it to select it, and click Next.
6. The destination screen allows you to specify whether you want to restore to the original location or select a new location to which to restore the data.

The Restore to the Following Location option allows you to compare the restored data to the original. This is not a required procedure, but it allows you to verify that CA ARCserve Backup has backed up and restored everything on your computer.

Choose a location option, and click Next.

7. The next screen lets you specify whether to overwrite files that already exist. CA ARCserve Backup provides the following options:
 - **Overwrite All Files**--replaces all existing files with the files you are restoring.
 - **Rename Files from Tape**--retains both copies of the files and renames the restored file.
 - **Skip Existing Files**--does not restore or overwrite existing files.
 - **Overwrite with Newer Files Only**--specifies that existing files are to be overwritten only if the restored file has a newer date.
 - **Confirm Overwrites (for Run Now only)**--prompts you to confirm that you want to restore the source files with the same name on the destination.

Note: On 64-bit operating systems, the user prompt does not display and the option does not restore or overwrite existing files.

Select an overwrite option, and click Next.

8. In the next screen, verify that the security information is correct, and click Next.
9. The schedule screen lets you choose to run the restore job immediately or schedule it for a later date and time. To run your job immediately, select Run Now, and click Next.

The Schedule option allows you to specify a future start date and time for the job and lets you specify whether CA ARCserve Backup should repeat the job.

10. The last screen allows you to enter a description for your job. Verify the information displayed in the Restore Wizard Summary fields, and click Finish to submit your restore job.

GFS Rotations

The Grandfather-Father-Son (GFS) rotation strategy is a method of maintaining backups on a daily, weekly, and monthly basis. GFS backup schemes are based on a seven-day weekly schedule, beginning on any day of your choice. The primary purpose of the GFS scheme is to maintain a minimum standard and consistent interval at which to rotate and retire media. This scheme always uses the oldest media first.

You should perform a full backup at least once a week. On all other days, you can perform full or partial backups or no backup at all. The advantage of setting up a GFS rotation scheme is that once it is configured, you need only make sure the right media is in the drive for each day of the week. From that time on, GFS tells you which media to use and manages the backups for you.

- Daily backups are the Son media
- A full backup is performed at least once a week. The last full backup of the week is the Father media
- The last full backup of the month (monthly backup) is the Grandfather media

Note: Monthly backups are saved throughout the year and the media on which they are stored should be taken off-site for safekeeping. You can track these media using the Media Management Admin.

Important! GFS rotations create three media pools--daily, weekly, and monthly pools. You cannot entirely customize this rotation and the media used for the rotation scheme must be named automatically. Custom rotation schemes allow you to configure the properties of the scheme, such as the pool or pools involved, the days to back up, and other properties. Deduplication devices are an exception: even though deduplication devices cannot be assigned to media pools, you may still set up GFS rotations. For more information, see [GFS Rotation Jobs on Deduplication Devices](#) (see page 699).

GFS Rotation Scheme Media Example

The following example illustrates how to determine the number of media you need for a GFS rotation scheme:

Your company's business hours are from Monday to Friday. You have specified daily incremental backups from Monday through Thursday, with a full backup on Friday. You have decided to retain monthly full backup data for six months before you recycle your media, and have specified that at least six monthly tapes are to be maintained in the Save Set of your media pool. In addition, you have specified that a minimum of four weekly tapes are to be retained in the Save Set.

Note: For more information about media pools, Save Sets, and Scratch Sets, see "Managing Devices and Media."

In the GFS rotation scheme you have selected, the incremental backups are the Son, the weekly full backups are the Father, and the monthly full backups are the Grandfather.

Your rotation scheme requires four daily incremental backups, requiring one tape for each day. Because the data these tapes contain is maintained on the weekly full backup, these tapes are recycled each week. Therefore, your scheme requires four daily (Son) tapes.

The backup performed each Friday, the weekly full backup, requires one tape for each week of the month. These tapes are retained for one month before they are recycled, and you have specified that a minimum of four tapes are to be maintained in the media pool Save Set. Therefore, you require a minimum of five weekly (Father) tapes.

The last full backup performed each month is the monthly backup. You specified that these tapes are to be retained for six months, and that six tapes are to be maintained in the media pool Save Set. The minimum number of monthly tapes required before the media recycles is six. Therefore, you need seven monthly (Grandfather) tapes.

The total media you need for this rotation scheme is 16.

Set Up GFS Rotation Schemes

This section describes how you can set up a GFS rotation scheme using the Backup Manager. For detailed information about the functions, capabilities, options, and tasks that you can perform using the Backup Manager, see "Backing Up Data."

To set up GFS rotation schemes

1. From the Backup Manager, select a source and destination, and click the Schedule tab.
2. Enable the Use Rotation Scheme option. From the Scheme Name drop-down menu, choose one of the backup schemes.

Note: The Enable GFS option is automatically checked when a GFS scheme is selected.

3. If you want to add the data from one incremental or differential backup session to the same media as the previous backup session, enable the Append Media option.
4. In the Media Pool Name Prefix field, enter the prefix for all of your media names.

CA ARCserve Backup automatically creates and names your backup media using the name you designate.

Note: CA ARCserve Backup prevents you from using the underscore character (_) and the hyphen character (-) when specifying Media Pool names.

5. Specify the Start Date and the Execute Time as required.
6. Click the Start button.

The backup job now runs precisely as you specified, and your media is recycled as you determined.

How GFS Rotations Work

The most commonly used media rotation schedule is the Grandfather-Father-Son (GFS) rotation. This schedule policy uses daily (Son), weekly (Father), and monthly (Grandfather) backup media sets (tapes). GFS rotation schedules allow you to back up your data for an entire year using a minimum of media (tapes). The number of tapes you use for GFS rotations is based on the number of workdays you specify for your backup policy.

The GFS rotation method works as follows:

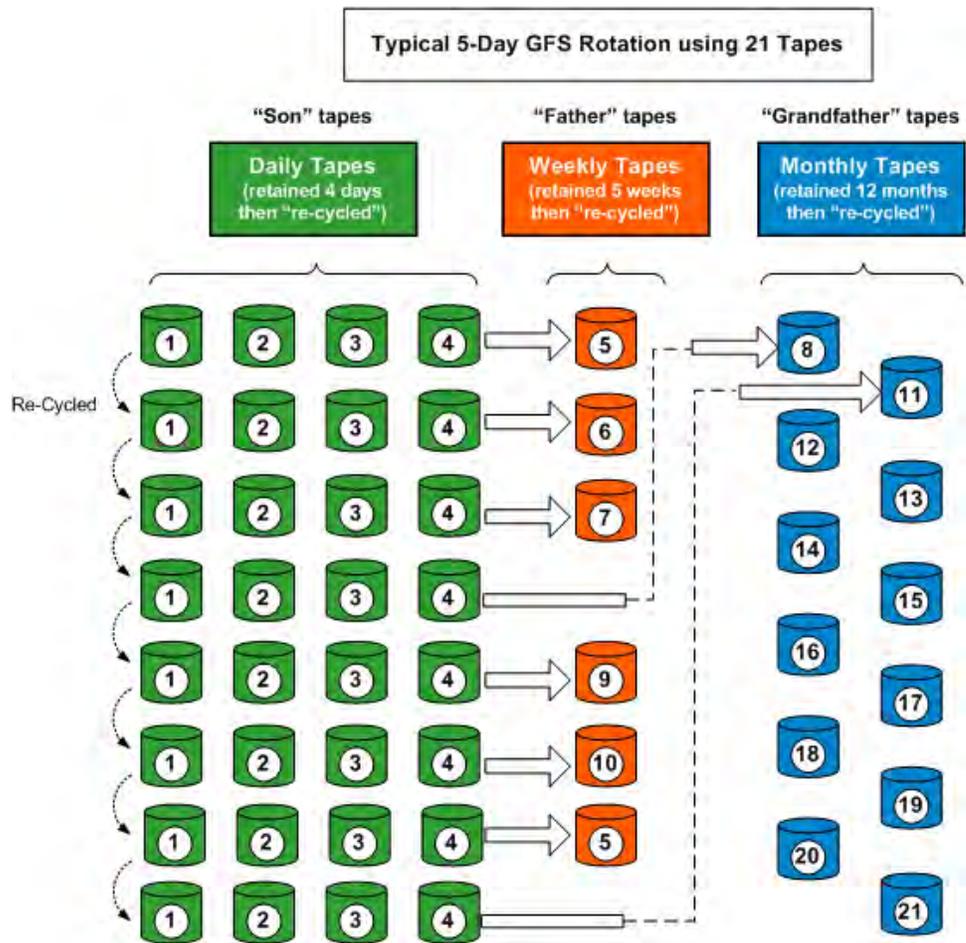
Note: To avoid confusion, it is important to clearly and properly label your tapes.

- You backup your data on a separate tape every working day. You should use a different tape for every daily backup. For example, if your backup cycle is based on a five-day workweek, you will need four "Daily" tapes before you use a weekly tape. (Maybe label the daily tapes Monday, Tuesday, Wednesday, and Thursday or Daily 1 through Daily 4, etc.). You can perform Full, Incremental, or Differential backups for your daily backups. After the fourth day, the first daily tape used is then re-cycled and can be overwritten with the next scheduled daily backup.

Remember, because the daily tapes are used more frequently than the weekly and monthly tapes, you will need to replace them more often.

- On the fifth day, instead of using another daily tape, you will use a "Weekly" tape. You should always perform a Full backup for your weekly backups. You should also use five weekly tapes before you use a monthly tape. (Maybe label the weekly tapes Week 1 through Week 5). After the fifth week, the first weekly tape used is then re-cycled and can be overwritten with the next scheduled weekly backup.
- At the end of the third week, instead of using another weekly tape, you will use a "Monthly" tape. You should also perform a Full backup for your monthly backups. You should have 12 monthly tapes to safely backup a full year of data. (Maybe label the monthly tapes January through December or Month 1 through Month 12, etc.). After twelfth month, the first monthly tape used is then re-cycled and overwritten with the next monthly backup.

The following diagram shows an example of how a typical 5-day GFS rotation policy can be implemented to provide you with a safe and reliable method to perform data backups for an entire year while using a minimum amount of backup media:



Note: A five-day GFS rotation policy would require approximately 21 tapes per year, while a seven-day policy would require approximately 23 tapes per year (adding two additional daily tapes). For both of these schedules, the amount of media needed can vary depending upon your specified retention criteria and the quantity of data that you are backing up. Additionally, the amount of media needed in each schedule can also be affected by the use of multistreaming and if you are appending backup sessions to your media.

Chapter 3: Backing Up Data

This section contains the following topics:

[How You Can Back Up Data](#) (see page 125)

[Submit a Backup Job](#) (see page 129)

[Backup Manager](#) (see page 130)

[Global Backup Options](#) (see page 140)

[Files and Objects that CA ARCserve Backup Does Not Back Up](#) (see page 173)

[Enable CA ARCserve Backup to Manage Open Files on Remote Computers](#) (see page 175)

[How Multistreaming Processes Backup Data](#) (see page 176)

[How Multiplexing Processes Backup Data](#) (see page 178)

[Preflight Checks for Your Backups](#) (see page 184)

[Entire Node Backups](#) (see page 185)

[Create Repeating Backup Jobs](#) (see page 188)

[Back Up Remote Servers](#) (see page 189)

[Backup Staging Methods](#) (see page 190)

[Disaster Recovery](#) (see page 236)

[Back Up BrightStor ARCserve Backup for Laptops & Desktops Data](#) (see page 236)

How You Can Back Up Data

CA ARCserve Backup allows you to back up most machines attached to your Windows network using one of the following sources:

- Administrative shared drives
- User-shared files, directories, and drives

Because CA ARCserve Backup separates and lists Windows machines by the domain or workgroup to which they belong, you can easily back up all the machines belonging to a specific domain or workgroup, by selecting the name of the domain or workgroup.

The optional CA ARCserve Backup Client Agents allow you to communicate with remote workstations in various environments. This provides complete system backups, including system information from non-Windows systems, such as NetWare or UNIX.

Similarly, the optional Backup Agents allow CA ARCserve Backup to back up and restore online databases such as Microsoft Exchange, Lotus Domino, Microsoft SQL Server, Oracle, and IBM Informix.

If you have Unicenter NSM installed, you can use the monitoring agent to monitor CA ARCserve Backup. This agent can be used to start and stop services, monitor the status of the CA ARCserve Backup processes and media, and report on the failure of backup jobs.

More information:

[Monitor Activity Using the Unicenter Monitoring Agent](#) (see page 631)

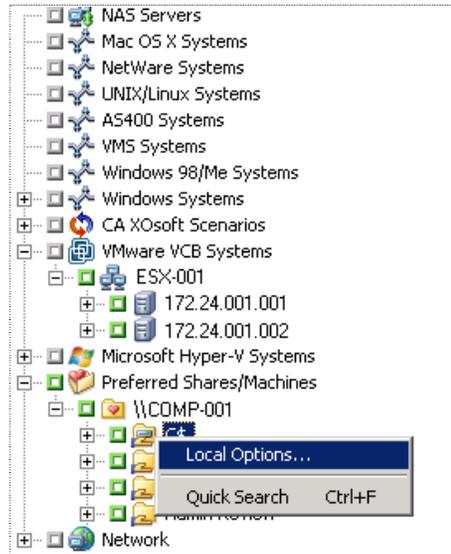
Specify Local Backup Options

CA ARCserve Backup gives you the power and flexibility to customize local options for specific drives that you want to back up.

To specify local backup options

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

Click the green box next to the drive directory, and then right-click the drive and select Local Options.



Important! When setting local options, you must select drives individually as your source even if you want to back up an entire server. You cannot click the green box next to the server name, and then customize local backup options for individual drives.

The Local Options dialog opens.

2. Specify the desired options:

Backup Verification Options

The Backup Verification options enable you to verify that your data was backed up correctly. The following options are available.

- **None**--If you select this, no verification will be performed on the data backed up.
- **Scan Backup Media Contents**--If you select this, CA ARCserve Backup scans the media and check that the header is readable for each file that is backed up.
- **Compare Backup Media to Disk**--Select this if you want CA ARCserve Backup to read blocks from the media and compare, byte for byte, the data on the media against the files.

Session/Encryption Password Option

Use this option to specify a password to protect the data.

- **Session/Encryption Password**--Enter a password for your backup job.

Important! It is important that you remember the Session/Encryption password to restore this session. There is no way to reset this password.

Compression and Encryption Options

Use these options to specify whether files should be compressed or encrypted before they are backed up. These options are not supported on deduplication devices. If you specify a deduplication device group as the backup destination or as the staging destination, compression and encryption are skipped if detected.

- **Compress Files Before Backup Using Software Compression--**Allows you to compress your files before running your backup job. Using this option directs CA ARCserve Backup to compress files before backing them up using a software compression algorithm. Since most tape devices are equipped with a hardware-based compression mechanism, using both software and hardware compression is unnecessary and can lead to a slow backup job and poor compression results. Therefore, you should select this option only if your tape drive is not equipped with a hardware compression mechanism.
- **Encrypt Files Before Backup--**Allows you to encrypt your files before running your backup job.

Important! CA ARCserve Backup performs local compression and encryption at the agent system. When you specify local compression and encryption and ARCserve server-based compression and encryption (global option), CA ARCserve Backup performs the compression and encryption at the agent system.

Note: For more information about specifying ARCserve server-based compression and encryption, see [Backup Manager Backup Media Options](#) (see page 150).

NetWare Volume Options

This option is available for NetWare servers only.

- **Disable Snapshot--**If the CA ARCserve Backup Agent for Open Files is installed on the server and you want to disable open file backup on an NSS volume, select this option.

Note: If you have database agents installed, you can also right-click them to customize local backup agent options. If you do this (similar to setting local options on drives, directories, and files), you must select database agents individually as your source even if you want to back up an entire server (You cannot click the green box next to the server name, and then customize local backup agent options).

3. Click OK.

The local settings are applied to the specified volume.

More information:

[Local Backup Options for UNIX Agents](#) (see page 139)

Submit a Backup Job

This section summarizes how to submit a backup job.

For information about how to use disk staging (D2D2T) and tape staging (D2T2T) to manage your backup operations, see [How Backup to Disk to Tape Works](#) (see page 191).

To submit a backup job

1. From the Backup Manager, select the [Source](#) (see page 131), [Destination](#) (see page 136), and [Schedule](#) (see page 137) tabs to specify the options that you require for the job.

Click the Options toolbar button to specify global options that you require for the job. For more information, see [Global Backup Options](#) (see page 140).

Click the Start toolbar button to submit your job.

The Security and Agent Information dialog opens.

2. On the Security and Agent Information dialog, edit or confirm the security and agent information for your job, and click OK.

Note: If you did not install the CA ARCserve Backup Enterprise Module, click OK on the message that follows to continue:

Enterprise Module is not installed. The session password will not be saved.

3. When the Submit Job dialog opens, select Run Now to run the job immediately, or select Run On and select a date and time when you want the job to run.

Note: For more information about the Run Now option, see Job Queue Tab.

4. Enter a description for your job.
5. If you selected multiple sources to back up and want to set the priority in which the job sessions initiate, click Source Priority. Use the Top, Up, Down, and Bottom buttons to change the order in which the jobs are processed. When you finish setting priorities, click OK.
6. To save the job as a CA ARCserve Backup job script, click the Save Job button.
7. To save the job template, click the Save Template button.

8. To preflight check the job, click the Preflight Check button. If the preflight check failed, click the Cancel button to modify the job settings.

9. On the Submit Job dialog, click OK.

The job is submitted.

Note: For information about how to submit a backup job using the Backup Wizard, see [Back Up Data Using the Backup Wizard](#) (see page 117).

More information:

[How to Manage Jobs Using the Job Queue Tab](#) (see page 302)

Backup Manager

The Backup Manager lets you customize your backup jobs using filters, options, and scheduling. For procedural information on how to submit backup jobs using the Backup Manager, see the online help.

You can use the Backup Manager to:

- Back up to various media or create a customized backup scheme.
- Use filters to selectively exclude or include directories and files from backup jobs.
- Create an automated backup scheme using the Grandfather-Father-Son (GFS) rotation scheme.
- Apply filters to local source objects (such as volumes and nodes) or globally to the entire backup job, or to both at the same time.

CA ARCserve Backup allows you to back up the Windows registry as well as the system state for Windows systems. Each backup job requires a source and a destination (media). The Backup Manager screen provides four tabs to customize your backup job:

- Source
- Staging
- Destination
- Schedule

Specify the Source

The source is the path to the data that you want to back up. You can easily find the files you want to back up by browsing through the Backup Manager directory to select the user-shared drives and directories.

When selecting a source, you can back up an entire server or you can select individual drives, directories, and files to back up. To select an entire server, click the green box next to the server name. When you do this, all of the drives, directories, and files on the server are automatically selected.

To select individual drives, directories, and files to back up, expand a server name and click the green boxes next to each drive, directory, and file.

Custom Local Backup Options

You can right-click individual drives to customize local backup options. If you have database agents installed, you can also right-click them to customize local backup agent options. If you want to customize local backup or local backup agent options, your job must be packaged explicitly, which means you must select drives, directories, files, or database agents individually as your source even if you want to back up an entire server. You cannot click the green box next to the server name, and then customize local backup options for individual drives, directories, files, or database agents. For more information, see [Dynamic Job Packaging](#) (see page 286) and [Explicit Job Packaging](#) (see page 286).

More information:

[Specify Local Backup Options](#) (see page 126)

Manager Markers

Each object displayed in the Backup Manager window has a green or gray box to its left called a marker.

Green marker

Lets you control the extent of the backup for an object directly. Click a marker to exclude an object from a backup or to indicate that you want the backup for the object to be full or partial. As you click the marker, you fill or empty the marker of color, indicating the extent of the backup.

Gray marker

These markers are associated with objects that are not real and that you cannot back up/restore. Typically, these items serve as placeholders under which other objects are grouped and displayed. As you click the green markers under a gray marker item, the fill proportion of the gray marker changes automatically from empty to partial to full depending on the proportion of files you have chosen to backup.

The following table describes the different marker configurations and corresponding backup levels:

Marker	Configuration	Description
	Completely filled center.	Full backup.
	Partially filled center.	Partial backup.
	Empty center.	Do not back up.

Note: Gray marker configurations follow the same pattern as green marker configurations, but reflect the proportion of files under them that are selected for backup.

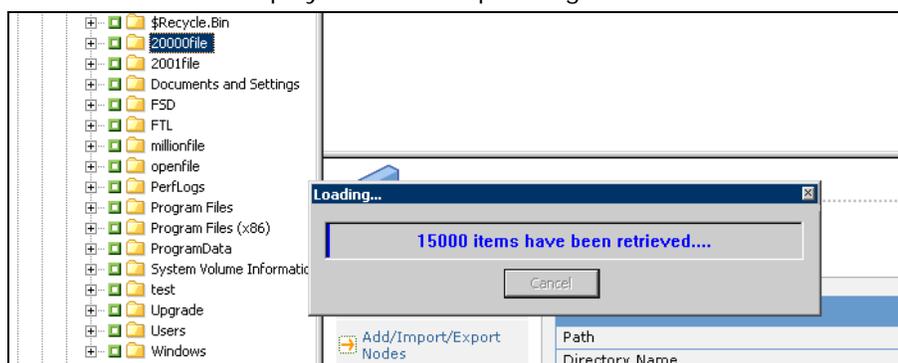
The fill proportion of a marker at a higher level of the directory tree depends on the fill proportions of the markers of the objects at the lower levels.

- If all the markers at the lower levels are completely filled, then the marker at the higher level is also automatically completely filled.
- If the markers at the lower levels are a mix of completely filled and partially filled, then the marker at the higher level is automatically partially filled.
- If you click a marker at a higher level so that it is completely filled, then all the markers at the lower levels are automatically filled completely.

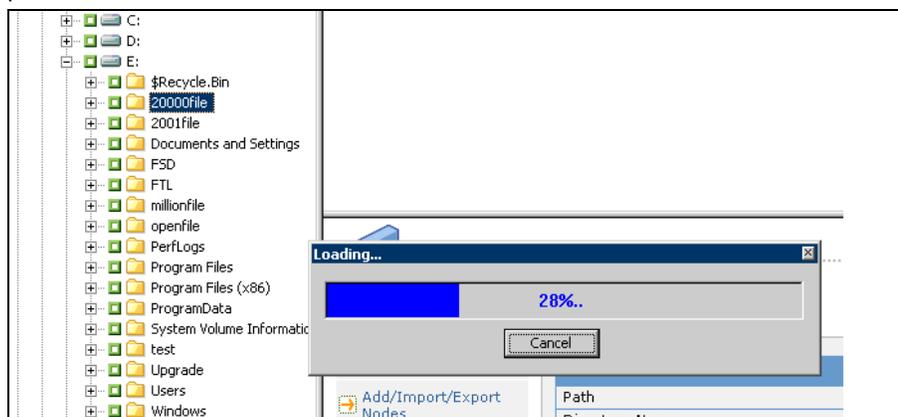
How CA ARCserve Backup Lets You Browse a Large Number of Items in the Backup Manager

CA ARCserve Backup lets you pause the process of loading items in the Backup Manager when you browse a large number of directories, files, and so on. The steps that follow describe how CA ARCserve Backup lets you browse a large number of items in the Backup Manager window.

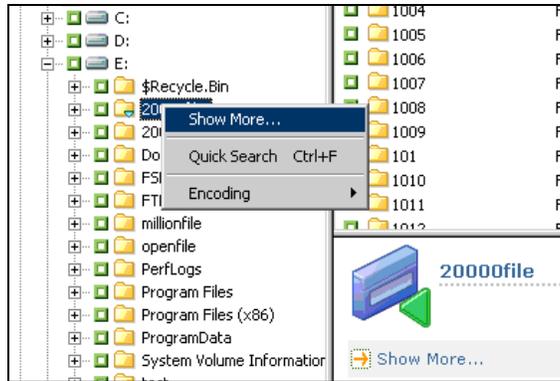
1. When you select a directory in the Backup Manager, Source tree, CA ARCserve Backup displays a Loading dialog to inform you that a large number of items need to be retrieved and loaded into the Backup Manager window. You cannot click Cancel while CA ARCserve Backup is retrieving the list of items to display in the Backup Manager window.



2. After CA ARCserve Backup retrieves the list of items to display in the Backup Manager window, the Loading dialog then displays the percentage of items that are loaded into the Backup Manager. If there are a large number of items to display, you can click Cancel to pause the loading process.



3. After you pause the Loading process, you can continue the Loading process by right-clicking target directory and selecting Show More from the pop-up menu.



4. If you pause the loading process, the icon for the target directory appears as follows:



5. You can pause and continue the loading process as often as necessary. To load more items, right-click the target directory and click Show More from the pop-up menu.

6. When the loading process is complete, the icon for the target directory displays as follows:



Browse a Large Number of Items in the Backup Manager

Use the following procedure when you need to browse a directory that contains a large number of items in the Backup Manager.

To browse a large number of items in the Backup Manager

1. Open the Backup Manager and specify a target directory from the Source tree.

The Loading message box appears, CA ARCserve Backup retrieves a list of items to display in the Backup Manager Window, and then CA ARCserve Backup loads the files into the Backup Manager window.

2. From the Loading message box, click Cancel to stop the loading process.

If CA ARCserve Backup did not load all items, the To show more objects, right-click the target directory and select Show More from the pop-up menu warning message appears.

Note: The message only appears the first time you click Cancel on the Loading message box.

3. From the Source tree, right-click the target directory and click Show More from the pop-up menu.

The Loading message box appears and CA ARCserve Backup continues loading the items.

4. You can pause and continue the loading process as often as necessary until CA ARCserve Backup loads all items in the target directory.

If you pause the loading process, the icon for the target directory displays as follows:



When the loading process is complete, the icon for the target directory displays as follows:



Backup Manager Considerations on 64-bit Windows Platforms

If the CA ARCserve Backup server is running on a 64-bit Windows platform, the following considerations apply:

- Removable drives on the local machine (for example, floppy, flash, CD, and DVD drives) do not appear in the Backup Manager Source directory tree.
- Objects backed up using jobs packaged locally on the 64-bit Windows machine are backed up using the 64-bit Windows Client Agent. The backed up objects can include files, folders, drives, System State files, the Windows Registry, and Volume Shadow Copy Service writer backups.
- Database agent objects backed up using network-based communication (for example, Oracle and Microsoft Exchange) appear in the Backup Manager Source directory tree in the same manner—regardless of whether they were backed up using a 32-bit or 64-bit Windows platform.

Options You Can Specify on the Backup Manager Destination Tab

The destination is the backup media device or disk. You can use the Destination tab in the Backup Manager to browse to and select the groups and device. The Backup Manager Destination tab includes the following backup options:

Multiplexing

The following options regulate how CA ARCserve Backup handles multiplexing.

- **Multiplexing Chunk Size**--Sets the performance of backup operations and memory usage. The chunk size value determines the amount of contiguous data written for one session before data from another session is multiplexed. The higher the value, the faster the restore on some drives, but at the cost of memory size during backup. For most drives, the default value of 1 MB is recommended.
- **Maximum Number of Streams**--Sets the maximum number of streams that can write to a tape at the same time. The default number of streams is 4 and the supported range is between 2 and 32.

Multistreaming

The Multistreaming option lets you split single backup jobs into multiple jobs and use all of the available tape devices in your system to complete the backup. For more information, see [Multistreaming](#) (see page 176).

Group and Media field

Use the Group and Media field to specify the device group that you want to use for the backup job.

- Place an asterisk in the Group or Media field to use the first available drive and media in the group.
- If you want to use any available group, click the Use Any Group option.

Media Pool

Select this option if you want to use a specific media pool for the backup job.

Note: If you select a Media Pool, CA ARCserve Backup automatically checks the other destination and backup options you selected to verify that no restrictions or conflicts occur when you run the job. If CA ARCserve Backup detects a conflict, a warning dialog opens.

Server

This field displays the name of the primary server and member servers in your CA ARCserve Backup domain.

Note: If you did not install the Central Management Option, the name of the current server displays in this field.

Note: To back up to disk using the Disk to Disk to Tape Option, use Device Configuration and Device Group Configuration to configure the staging device. For more information, see [Backup Staging Methods](#) (see page 190).

More information:

[How to Submit a Disk Staging Backup Job](#) (see page 215)

[How Multistreaming Processes Backup Data](#) (see page 176)

How You Can Use Wildcards with Tape Library Groups

The wildcard characters' asterisk and question mark are supported in the Group field. When wildcard characters are used to specify a job's library group destination, the job is sent to a group whose name matches the criteria and has at least one available media, as long as there is at least one available drive associated with the library. A media is available when it is not being used by another job (Note: no special consideration is given to media suitability as determined by the job schema; for example, Media Pool). If more than one job uses wildcards and more than one group matches the selection criteria, all jobs go to the first group with an available media.

Typing a name in the media field forces the job to be directed to a group that matches the criteria and contains the specified media, even if the media is busy. If there is no media with the specified name in any of the matching groups, but there is a blank media in a matching group, it is used and renamed. If there is no blank media, the user is prompted to insert one.

Note: The media field does not support wildcard characters.

When a media pool is specified, a media from that pool is used if there is one available in the first matching group. If there is no such media in the group, but there is a blank media, it is renamed and added to the pool. If there is no blank media the user is prompted to insert one.

Backup Job Schedules and Rotations

You can configure your backup job to use a custom schedule or a rotation scheme by using the CA ARCserve Backup template schemes or by specifying your own rotation parameters. You can also specify a repeat method and the following backup methods for each backup:

- **Full (Keep Archive Bit)**--Performed each time the job is repeated and keeps the archive bit.
- **Full (Clear Archive Bit)**--Performed each time the job is repeated and clears the archive bit.

- **Incremental backup**--Backs up only those files whose archive bits have been set since the last full or incremental backup was performed. After each backup, archive bits are reset so that they are not backed up during the next incremental backup job.
- **Differential backup**--Backs up only those files whose archive bits have been set since the last full backup was performed. Because differential backup jobs do not clear a file's archive bit, the files that were backed up in the last differential job are backed up again. It takes longer to process backup jobs using this method. However, this strategy requires only two sets of media to restore a differential backup; the full media set, and the differential media set. In the case of an incremental backup, you require the full media set and every incremental set until the latest set.

Note: The above-described backup methods do not apply to the Linux Client Agent.

For a description of detailed job scheduling features, see the chapter "Customizing Jobs," or the online help.

Local Backup Options for UNIX Agents

The following are the local options available when backing up a UNIX machine through the UNIX Client Agent.

Additional Options

- **Traverse Symbolic Link File**--CA ARCserve Backup follows symbolic links and backs up the linked files.
- **Traverse NFS--Backs up NFS**--mounted drives.
- **Traverse Across File System**--CA ARCserve Backup automatically includes locally mounted UNIX file systems in the backup.
- **Estimation Off**--Disables the estimation of the number of files and the amount of data to be backed up that takes place at the beginning of the backup job. Selecting this option decreases the time it takes to perform the backup.
- **Preserve File Access Time**--This option directs CA ARCserve Backup to preserve the last access time of files when a backup is performed.

Note: The Access Time of a file is automatically updated by the operating system whenever a file is accessed (read or write). However, after a full backup is performed, the Access Times of all the backed up files are also updated. Therefore, if you want to track whether or not a file has actually been accessed (and not just backed up), you need to preserve the original access time.

- If this option is selected (check in box), CA ARCserve Backup preserves the last file access time of any files that are backed as the original value that was present before the backup was performed (Change Time will be updated). This is the default setting.
- If this option is not selected (no check in box), the last file access time of any files that are backed up is updated to the new value that is present when the backup is completed (Change Time will not be updated).

Note: For Windows based agents, you must apply this option globally. For more information, see Global Backup Options.

Media format to use for backup

- **CA ARCserve Backup format**--This is a CA ARCserve Backup proprietary tape format. This format is designed to overcome the limitations of tar/cpio formats and leverage other features like compression/encryption provided by CA ARCserve Backup. For example, there are certain limitations with tar/cpio while backing up large files and huge data that may span across multiple tapes.

- **Posix tar format**--This is a Standard Posix Tar format. When you select this option, CA ARCserve Backup creates a backup image in Posix Tar format. CA ARCserve Backup or any tar utility can be used to restore data from an image created in this format. Using CA ARCserve Backup format is recommended.

Posix cpio format--This is a Standard Posix CPIO format. When you select this option, CA ARCserve Backup creates a backup image in Posix CPIO format. CA ARCserve Backup or any CPIO utility can be used to restore data from an image created in this format. Using CA ARCserve Backup format is recommended.

More information:

[Global Backup Options](#) (see page 140)

[Specify Local Backup Options](#) (see page 126)

Global Backup Options

This section describes the global backup options you can select when submitting your backup job. For a description of additional backup job options and filtering features, see the chapter "Customizing Jobs."

To access the global options dialog, click the Options toolbar button in the Backup Manager. The available options are as follows:

- [Alert options](#) (see page 141).
- [Media Exporting options](#) (see page 143).
- [Advanced options](#) (see page 143).
- [Encryption and Compression options](#) (see page 146).
- [Volume Shadow Copy Service options](#) (see page 148).
- [Backup Media options](#) (see page 150).
- [Verification options](#) (see page 152).
- [Retry options](#) (see page 153).
- [Operation options](#) (see page 155).
- [Pre/Post options](#) (see page 160).
- [Agent Options](#) (see page 162).
- [Job Log options](#) (see page 172).
- [Virus options](#) (see page 172).

More information:

[Local Backup Options for UNIX Agents](#) (see page 139)

Backup Manager Alert Options

You can use the Alert notification system to send messages about events that appear in the Activity Log during your backup operation. Choose one or more of the following events for which you want to be notified:

- **Job Completed Successfully**--All of the nodes and drives/shares were processed.
- **Job Incomplete**--Some nodes, drives, or shares were missed.
- **Job Canceled by User**--The user canceled the job.
- **Job Failed**--The job was started but could not be completed.
- **Virus Detected**--A virus was detected in one of the files to be backed up. See Virus options (Backup, Copy, Count)
- **Customized Event**--A customized event occurred. To specify this type of event, enter an error, warning, or notification code in the space below the Event drop-box.

Choose one or more of the defined Alert configurations. The <default> configuration means that you will use whatever is configured in Alert Manager. Click Configure to define further configurations. CA ARCserve Backup provides the following defined Alert configurations:

- Broadcast
- Pager

Note: Pager options are not supported on Japanese versions of CA ARCserve Backup.

- SMTP
- SNMP
- Event

- Printer
- E-Mail
- Lotus Notes
- Unicenter TNG

Specify miscellaneous options:

- **Attach Job Log**--Lets you include the job log information in the Alert message. (This option applies for Trouble Tickets and Mail only.)

Note: The list you create using Alert Options is saved with the Job Script and the configuration defined using the Configuration button.

- **Send alert messages only for master jobs**--Lets CA ARCserve Backup send you alerts that reference only the master job number in the Alert message. The alert messages will not reference child and subjob numbers. You can specify this option on all jobs, including multiplexing and multistreaming jobs.

Backup Manager Media Exporting Options

At the end of a backup job, you can move media out of the library or to an off-site location for safe storage. CA ARCserve Backup provides the following media exporting options:

None

No media exporting will take place at the end of a backup job.

Export RAID1 Duplicate Tape After Job

If the job spanned to multiple media, all the duplicate media used in this job is exported.

Note: This option is for RAID 1 support with libraries and mail slots only.

Export All Tapes After Job

CA ARCserve Backup exports all the media for the related backup. If the job spanned to multiple media, all the media used in this job is exported. If there are not enough mail slots to export all the media, the media that could not be exported is moved back to the original home slot. In single mail slot libraries, CA ARCserve Backup retries a few times to check if the mail slot is empty to move the next media to the mail slot. If the operator does not move the media, CA ARCserve Backup writes this information in the activity log.

Note: This option is for RAID 1 support with libraries and mail slots only.

Limitations

Be aware of the following media exporting limitations:

- For staging backup jobs, media exporting options are only effective during the migration phase of the job.
- Media exporting options are functional only for regular and rotation jobs and are supported on media libraries and Tape RAID.
- Media exporting options are not supported when you are performing tape staging (B2T2T) backups and the staging device or the final destination device is a RAID device.
- If the job includes verification, the export is done at the end of the verification.

Backup Manager Advanced Options

The Advanced options determine how CA ARCserve Backup handles the file system extensions during a backup.

Windows System Options

Note: These options are only supported on the Windows 2000, Windows XP, and Windows Server 2003 operating systems.

The Windows system options available are:

- **Traverse Directory Junctions and Volume Mount Points**--Selecting this option causes the backup job to traverse the volume or the directory being specified to and take a backup of it. At the time of restore of this session, you can restore files and directories contained in the referred to volume or directory. When this option is not selected, the backup job does not back up the volume or the directory being referred to by the volume mount point or the directory junction respectively. Therefore, at the time of restore, you cannot restore a file or directory contained in the referred to volume or directory.
- **Backup Mount Points as Part of the volume that they are mounted on**--If you select this, the volumes referred to by the Volume Mount Points will be backed up as part of the same session as the Volume Mount Points. When this option is not selected, the volumes referred to by the Volume Mount Points are backed up as separate sessions

Note: This option is available only when the previous option, Traverse Directory Junctions and Volume Mount Points, is selected.

- **Preserve File Hard Links**--If you enable this, CA ARCserve Backup preserves hard links during a restore.

Disaster Recovery Options

The Disaster Recovery options available are:

- **Generate DR information for partially selected nodes**--Disaster recovery information is normally generated when performing a full machine backup. However, there are special cases where you may need to keep the disaster recovery information updated but cannot perform full machine backups too often (like in a SAN shared disk environment). By enabling this option, you can generate or update a machine's disaster recovery information without having to back up everything on the machine.

- **Include filtered sessions when generating restore session information**--When generating disaster recovery information, the CA ARCserve Backup server keeps track of only the latest non-filtered backup sessions pertaining to the machine. By default, if you back up a machine using filters, the filtered backup sessions will not be used by disaster recovery when recovering the system. By enabling this option, you can alter the default behavior and have disaster recovery use the filtered backup sessions when recovering the system.

Important! Enabling this option is very risky, especially for system volumes. Missing system files may lead to incomplete recovery.

This option is disabled by default. When you enable this option, it works at the job level. If the job contains multiple machine backups, this option will apply to all machines.

Microsoft SQL Server Backup Options

For Microsoft SQL Server, CA ARCserve Backup supports the following global option:

- **Do not apply Scheduled Job Method or Rotation Phase to Microsoft SQL Server databases**--Lets you exclude the backup method specified on the Backup Manager, Schedule tab. With this option specified, CA ARCserve Backup behaves as follows:
 - CA ARCserve Backup ignores the custom schedule, rotation, and GFS rotation method that was specified for the job.
 - CA ARCserve Backup converts the backup method specified on the Schedule tab to Full backup, only if the logic for database level backups and global backup options requires the backup method specified on the Schedule tab.

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

Backup Manager Encryption/Compression Options

CA ARCserve Backup lets you encrypt, compress, or encrypt and compress backup data.

Be aware of the following:

- You must license the CA ARCserve Backup Enterprise Module to encrypt backup data.
- Compression/Encryption are not supported on deduplication device groups. For more information, see [Compression and Encryption with Deduplication](#) (see page 687).
- If you specify encryption and compression options, and the backup destination is a drive that does not support compression, or is a file system device (FSD), CA ARCserve Backup encrypts the backup data and does not compress the backup data.

The following options define how CA ARCserve Backup processes backup data during a backup job and during the migration phase of a staging backup job.

Session/Encryption Password

- **Session/Encryption password**--Specify a Session/Encryption password to restore this data from media.

If you specify a Session Encryption password, you must specify the password to perform the following operations:

- Restore operations where the encryption, compression, or both were processed at the agent or at the backup server.
- Compare operations where the encryption, compression, or both were processed at the agent or at the backup server.
- Merge and Scan operations where the encryption, compression, or both were processed at the backup server. (You do not need to specify the password to perform Merge and Scan operations where the encryption, compression, or both operations were processed at the agent.)

Note: The Session/Encryption password is not required when you Merge or Scan only the session headers.

- **Save Current Session/Encryption Password to the CA ARCserve Backup database**--Use this option to save the password to the CA ARCserve Backup database and enable password management. This option is selected by default. This option is available for both local and global option passwords.

Notes:

- You can only modify the Global Option password from the Session/Encryption password dialog by right clicking on the job in the job queue.
- To use this option, you must license CA ARCserve Backup Enterprise Module.
- **Remind to change password n days after specifying a password**--Specify the number of days a password is valid. Seven days prior to the specified number of days, a message prompting you to change your password will be logged in the Activity Log.

Example:

On Jan. 1 you set n to 30 days. On Jan. 24 the message The backup job password will expire in 7 days, will appear in the in the Activity Log. On Jan. 31 the message The backup job password has been expired. Please change it now appears in the Activity Log.

Compression/Encryption

- **Encryption data**--Use this option to encrypt the backup data. You can specify one of the following options:
 - **At agent**--Select this option to encrypt the backup data prior to the actual backup process. For more information about this option, see [Data Encryption at the Agent Server](#) (see page 104).
 - **At backup server during backup**--Select this option to encrypt the backup data at the backup server during the backup process. For more information, see [Data Encryption During Backup](#) (see page 106).
 - **At backup server during migration**--Select this option to encrypt the backup data during the migration phase of a staging backup job. For more information, see [Data Encryption During Migration](#) (see page 107).

If you encrypt data during the backup phase, CA ARCserve Backup will not encrypt the data again during the migration phase of the staging backup operation.

- **Compress data**--Use this option to compress the backup data. You can specify one of the following options:
 - **At agent**--Select this option to compress the backup data on the system where the agent is installed and running.

Note: CA ARCserve Backup does not support data compression at the agent system when the backup source consists of UNIX, Oracle RMAN data.
 - **At backup server**--Select this option to compress the backup data at the CA ARCserve Backup server during the backup process. This option lets you compress files before backing them up using a software compression algorithm.

Note: With this option specified and the Encrypt data at backup server during backup option or the Encrypt data at backup server during migration option specified, CA ARCserve Backup uses software encryption to compress the data at the backup server before the data is encrypted at the backup server.

Backup Manager Volume Shadow Copy Service Options

You can specify global options for using the Volume Shadow Copy Service (VSS) These options affect all Writers for VSS backups, but they do not apply to transportable VSS backups.

Note: For more information on VSS, see the *Microsoft Volume Shadow Copy Service Guide*.

On the Volume Shadow Copy Service tab, the File System Backup group box lets you specify how you want CA ARCserve Backup to handle open files during file system backups. These options do not affect Writers and Components.

- **Use VSS--**Directs CA ARCserve Backup to use VSS to handle the backup of open files.

If this check box is not selected, VSS support is not used and the CA ARCserve Backup Agent for Open Files (if available) is used to handle open files. If the CA ARCserve Backup Agent for Open Files is not available and Use VSS is not selected, a traditional backup is performed. However, the backup will be incomplete if there are any open files that cannot be backed up.

- **Revert to traditional backup if VSS fails--**Directs CA ARCserve Backup to execute a traditional backup if an attempt to create a VSS backup fails. If the CA ARCserve Backup Agent for Open Files is available, it is used to handle open files if this option is selected and the VSS backup fails.

If this check box is not selected and the VSS backup fails, the backup job fails.

The Writers and Components group box lets you specify how you want CA ARCserve Backup to treat Writers and Components. These global options affect all Writers, except for those with Writer-specific options in place. For more information about setting Writer-specific options, see the *Microsoft Volume Shadow Copy Service Guide*.

- **Files included by a writer will be excluded from file system backups--**Prevents files that belong to a Component from being backed up by a traditional file system backup. This option offers the following advantages:

- Avoids backing up files that have already been backed up by VSS.
- By excluding files from traditional backups, fewer files are processed, and traditional backups take less time to complete.
- Helps achieve successful backups by eliminating certain problems associated with files that must be processed as a group; for example, files associated with a Writer or database application. In a traditional backup, there is no mechanism to ensure that the files are processed together.

- **Files excluded by a writer will be excluded from file system backups--**Prevents files that have been excluded from being backed up by a Component from being backed up by a traditional file system backup.

There may be files associated with an application that should never be backed up (for example, the Windows page file). Each Writer is aware of whether its associated application maintains any such files. Selecting this option allows CA ARCserve Backup to use this information when performing traditional backups.

- **If a component file fails to backup the writer, the backup will terminate**--Cancels the backup of a Writer if the backup of any of the Components fail. The backup of a Component fails if one or more of its files cannot be successfully backed up.

Selecting this option ensures that any backup is consistent and that all of the files associated with a Writer are backed up before the backup is considered successful, regardless of how many Components are associated with the Writer.

Backup Manager Backup Media Options

You can specify the overwrite/append rules for the media used in your backup job while you are configuring the job. This section describes the rules so that you can determine which method is best for your purposes.

CA ARCserve Backup allows up to 20000 sessions on a single tape and up to 101 sequences of a series of spanned tapes. Keep this in mind when planning your backups, because, if your sessions are small, you can reach 20000 sessions very quickly. If you have a large amount of data to back up, you can quickly exceed 101 sequences, depending upon how much data each tape can hold. You can stop appending the data to the tape when the sequence number reaches the maximum limit and start a new tape set by selecting the Overwrite Same Media Name, Blank Media or Overwrite Same Media Name, or Blank Media First, then Any Media option.

For a file system device (FSD), the limitation is 4,294,967,295 sessions on a single FSD.

On FSDs that contain more than 65,535 sessions, jobs may fail when you back up older version of CA ARCserve Backup database and application agents with this release of CA ARCserve Backup server components. Therefore, you must upgrade any older versions of CA ARCserve Backup database and application agents to this release to avoid job failure on devices with a large number of sessions.

First Backup Media

The first backup media is the media you use when the backup job begins. The options for the first media determine the overwrite rules for the first media that is used for the backup job:

Note: If the "Use Rotation Scheme" backup option is selected on the Schedule tab, the Rotation Rules will override these options.

- **Append to Media**--Append job sessions to the selected media.

- **Overwrite Same Media Name, or Blank Media**--Overwrite the media in the drive only if it is the one you specified for the job or if the media is blank. If neither of these conditions are met, CA ARCserve Backup prompts you to supply the specific media name.
- **Overwrite Same Media Name, or Blank Media First, then Any Media**--Overwrite any media found in the drive. If you select this media option, CA ARCserve Backup checks to see if the media in the drive is the one specified for the job. If it isn't, CA ARCserve Backup checks to see if the media is blank. If the media isn't blank either, CA ARCserve Backup reformats whatever media it finds in the device and starts backing up files at the beginning of the media.
- **Timeout for First Media**--Number of minutes CA ARCserve Backup attempts to write to media before canceling job.

Notes:

- The deduplication device does not support **Overwrite Same Media Name**. The backup job will always append to the deduplication device even if **Overwrite Same Media Name, or Blank Media** or **Overwrite Same Media Name, or Blank Media First, then Any Media** is selected.
- If you want to format the deduplication device, format it manually in CA ARCserve Backup Manager.

Additional Backup Media

These options apply to jobs that require more than one media to determine the overwrite rules for the additional media. You need to specify which media CA ARCserve Backup can use when the job spans media.

Note: If the "Use Rotation Scheme" backup option is selected on the Schedule tab, the Rotation Rules will override these options.

- **Overwrite Same Media Name, or Blank Media**--Write to the media in the device only if it has the same media name (but a different media ID) or if it is blank. CA ARCserve Backup remembers the name and ID of the job's first media. When the job requires additional media, CA ARCserve Backup checks if the new media has the same name (but different media ID) or if it is a blank media. As long as the ID is different, CA ARCserve Backup reformats the media, giving it the same name and ID as the first media. The sequence number changes.

Note: To overwrite media based on its name only, select the Distinguish Media by Name Only option.

- **Overwrite Same Media Name, or Blank Media First, then Any Media--**Overwrites any media found in the device (as long as it has a different ID from the first media's ID). If neither of these conditions are met, CA ARCserve Backup reformats whatever media it finds in the drive and starts backing up files at the beginning of the media. All subsequent media are reformatted with the same name and ID as the first media. Only the sequence number changes.

Note: To overwrite media based on its name only, select the Distinguish Media by Name Only option.

- **Timeout for Additional Media--**Number of minutes CA ARCserve Backup attempts to write to media before canceling job.

Distinguish Media by Name Only

CA ARCserve Backup writes to any media that has the name specified in the Media text box on the Destination tab, regardless of the media's ID or sequence number. This option is useful if you are running a repeating Overwrite job with a specific media and you want to ensure that the same media is used for the job each time.

When this option is not enabled, the second time the backup job is run, CA ARCserve Backup might not be able to locate the original tape because some of its identifying features will have changed. When this option is enabled, however, CA ARCserve Backup simply looks for a media that has the name specified in the Media text box and uses it, regardless of the media's other identifying features.

Note: If more than one media in the tape library have the same name, CA ARCserve Backup will use the first media in the device group that matches the specified name. Therefore, we do not recommend that you use this option to perform a one-time overwrite.

Backup Manager Verification Options

CA ARCserve Backup allows you to verify that your data was correctly backed up to media. You can verify data for the entire backup job or for a selected drive in your backup job. The global verification options (applied to the entire job) will be overridden by the options selected for a drive. CA ARCserve Backup provides the following options for verification:

- **None--**The back up will not be verified.

- **Scan Backup Media Contents**--Check the proprietary CA ARCserve Backup data area (the header) of each file on the backup media. If it is readable, CA ARCserve Backup assumes the data is reliable. If it is not readable, the Activity Log is updated with this information. This is the fastest verification method.

If you selected Calculate and Store CRC Value on Backup Media on the Operation tab, CA ARCserve Backup automatically performs CRC verification. This method assigns a value to the data that you copied to media and compares it to the value assigned to the data that you backed up. This enables you to identify the individual data packets that were backed up.

- **Compare Backup Media to Disk**--Data from the backup media is read and compared byte for byte against the source files. This option takes time, but ensures that all data on the backup media are exactly as on the disk. If CA ARCserve Backup finds a mismatch, the errors are recorded in the Activity Log.

Backup Manager Retry Options

When a backup job encounters an open file, CA ARCserve Backup provides you with the following options:

Note: The following retry options are only applicable for local backups on Windows 32-bit operating systems.

- **Open file**--determines how frequently CA ARCserve Backup will attempt to back up or copy open files.
 - **Retry immediately**--Back up or copy the file again, immediately after the first attempt failed. If the file is still unavailable, CA ARCserve Backup writes information to the Activity Log, and the job is labeled "Incomplete."
 - **Retry after job**--Back up or copy the file again after all the other source files have been backed up. If the file is still unavailable, CA ARCserve Backup writes information to the Activity Log, and the job is labeled "Incomplete."

Note: These retry options are applicable for the following backups only:

- Windows 32-bit systems local backups
- Linux/UNIX file system agent backups
- **Maximum retry times**--Number of times you want to try to back up or copy the file.
- **Retry interval**--Period of time you want to wait between attempts.

- **File sharing**--determines how CA ARCserve Backup shares the files with other applications when backing up or copying a file.
 - **Use deny none if deny write fails**--[default] Attempt to place the file in "Deny Write" mode. If this is not possible (because the file is already open), then place the file into "Deny None" mode.
 - **Use lock mode if deny write fails**--Attempt to place the file in "Deny Write" mode. If this is not possible (because the file is already open), then lock the file completely (prohibiting any user from opening or writing to the file). This option ensures the most recent version of the file is backed up or copied.
 - **Deny write**--Prevent another process from writing to the file while CA ARCserve Backup has it open. If another process has the file open before CA ARCserve Backup can open it, CA ARCserve Backup will not back up the file (unless you specified an Open File Retry option).
 - **Deny none**--Allow another process to read or write to the file, regardless of whether CA ARCserve Backup opens it first. This option ensures that your files are up-to-date, although the file that was backed up or copied may not be the most recent version.

Note: If you use applications (such as email) that are in operation 24 hours a day, you may want to choose one of the Deny None methods. As long as no other process is writing to these files during the job, the backup or copy will be consistent. If you want to ensure that only the most current version of every file is backed up or copied, you should select a Deny Write or Lock Mode option.

Backup Manager Operation Options

The operation options for backup determine related actions that occur during or after the backup, and the level of information that is recorded in the database. CA ARCserve Backup provides the following options:

Append Backup of CA ARCserve Backup data at the end of job Options

The following options affect how the level of information that is recorded in the CA ARCserve Backup database for the CA ARCserve Backup underlying database.

- **CA ARCserve Backup database**--This option allows to explicitly select the CA ARCserve Backup database or instance from the Backup Manager, Source directory tree with all backup jobs.
- **Catalog files**--This option allows you to back up the related CA ARCserve Backup database catalog files when the backup job is complete.
- **Job scripts**--This options allows you to back up the related job scripts when the backup job is complete.
- **SQL Server Disaster Recovery Elements for the CA ARCserve Backup Database**--This option ensures that the elements required to recover a SQL Server database from a disaster are backed up after jobs are complete.

Operation Options

The following options affect only backup operations.

- **Disable File Estimate**--By default, file estimation is disabled. To enable file estimation, deselect this option so that before any file is backed up to media, CA ARCserve Backup performs an estimate of how long the job will take.

Notes:

- File estimation is no longer the default value.
- If you are in a Novell server environment and you select Disable File Estimate from the Operations tab of the Global Options dialog, when you look at the View Job Queue/Statistics window from the back-end, there is no status bar at the bottom of the window.
- **Calculate and Store CRC Value on Backup Media**--Calculating and storing the CRC value on the backup media will enable CA ARCserve Backup to perform CRC verification during the backup job. To instruct CA ARCserve Backup to use the CRC value stored on media, see the Backup Options, Verification tab.

- **Delete Source Files After Backup to Media (use with caution)**--This argument deletes the files from the hard disk after the file backup is completed. Select this option if you want to delete source files from the source machine after they have been backed up to media. This option deletes only the files from the specified unprotected folder. It does not delete the empty folder itself.

You can use this option to perform disk grooming. For example, if you set up a backup job with a filter to back up files that haven't been accessed for a certain period of time, you could then include this option to delete those files from the source disk.

Be aware of the considerations that follow:

- On Windows computers, protected system files and files that are excluded from the backup by other filters are not deleted. For a remote backup job or a 64-bit operating system local backup job or a Windows Server 2008 local backup, the Windows Client Agent backs up the files. After the backup, this option deletes only the files from the specified unprotected folder. It does not delete the empty folder itself. Boot files, however, are not protected and can be deleted.
- On NetWare computers, all files that are backed up are deleted, except for those in protected directories, such as SYSTEM, PUBLIC, LOGIN, ETC, MAIL, and the CA ARCserve Backup home directory.
- On Linux/UNIX and Mac computers, all files that are backed up are deleted, except for those in protected directories, such as /bin, /etc, and /lib. To designate additional directories as protected, add them to the groom.cntl file on the client agent machine.

Note: As a best practice, you should specify Verification options when using Delete Source Files After Backup to Media. With verification options, CA ARCserve Backup compares the source files to the backup data to ensure that backup data is identical to the source data. For more information, see [Backup Manager Verification Options](#) (see page 152).

- **Preserve File Access Time (Used for Windows file system only)--**
This option directs CA ARCserve Backup to preserve the last access time of files when a backup is performed.

Note: The Access Time of a file is automatically updated by the operating system whenever a file is accessed (read or write). However, after a full backup is performed, the Access Times of all the backed up files are also updated. Therefore, if you want to track whether or not a file has actually been accessed (and not just backed up), you need to preserve the original access time.

- If this option is not selected (no check in box), the last file access time of any files that are backed up is updated to the new value that is present when the backup is completed. This is the default setting.
- If this option is selected (check in box), CA ARCserve Backup preserves the last file access time of any files that are backed as the original value that was present before the backup was performed.

Note: For UNIX based agents, you must apply this option locally. For more information, see [Local Backup Options for UNIX Agents](#) (see page 139).

- **Reset Archive bit for backup to deduplication device--**Select this option for custom backup jobs in which optimization is enabled to reset the archive bit on all files included in the job after the job completes. Optimization deduplicates only files that have changed since the last backup job, indicated by archive bits with a value of 1. Archive bits must be reset back to 0 so that subsequent backup jobs in which optimization is enabled can deduplicate only changed files. If you do not select this option with optimization-enabled jobs, files that have not changed since the previous backup could be included in subsequent jobs, resulting in significant performance reductions.
- **Back up deduplication device data--**Select this option if you want to forcibly include deduplication device files (index, reference and data files) in the backup job. These files are normally skipped in local backups. If you select this option, you should also enable the Use VSS option and disable the Revert to traditional backup if VSS fails option, both on the Volume Shadow Copy Service tab. If you forget to enable the Use VSS option and disable the Revert to traditional backup if VSS fails option, then the backup job automatically enables this option when the backup job runs.

- **Eject Backup Media upon Completion**--Select one of the following options:

- **Use Default Device Setting**--Select this if you want to use the setting you selected during library configuration.
- **Eject Media**--Select this if you want to eject media from the drive after the job finishes. This helps prevent any other job from overwriting information on this media. If you select this, it overrides the setting you selected during library configuration.
- **Do not Eject Media**--Select this if you do not want to eject media from the drive after the job finishes. If you select this, it overrides the setting you selected during library configuration.

Note: For more information on library configuration, see Tape Cleaning and Changing Configuration Details.

Retry Missed Targets Options

- **Retry Missed Targets**--Reschedule a backup for any workstations, file systems, databases, and so on that failed during the backup job.

You can specify one of the following reschedule options for a backup job:

After Job Finishes

Specifies the number of minutes that you want to elapse after the original job finished to start the makeup job.

Default: 5 minutes

Maximum: 1439 minutes (less than 24*60 minutes)

At

Specifies the time when the makeup is to run.

- **Max Times**--Specifies the maximum number of times to repeat the makeup jobs.

Default: 1 time

Maximum: 12 times

Be aware of the following:

- By default, Retry Missed Targets is enabled, After Job Finishes is selected, and the value of Max Times is 1.
- **File system backups**--If the backup job requiring a makeup job consists of file system backups, and the file system contains directories that reside in different volumes, the makeup job backs up only the failed volumes or directories. The makeup job does not back up the entire file system if it contained successful volume or directory backups.
- **Child jobs**--The child makeup jobs (makeup of makeup jobs) are always scheduled to run at same time as the job completion time. By default the child makeup job is put on hold. For example, if the makeup job that is finished at 10 PM fails, the child makeup job is scheduled to run at 10 PM and is put on hold. If you want to run this job, you must manually set this job to the ready mode.
- **Microsoft SQL Server backups**--If the backup job requiring a makeup job consists of Microsoft SQL Server instance backups, the makeup job backs up only the failed databases. The makeup job does not back up the entire instance if it contained successful database backups.
- **Microsoft Exchange backups**--If the backup job requiring a makeup job consists of Microsoft Exchange Server, database level backups, the makeup job backs up only the failed storage groups. The makeup job does not back up the entire database if it contained successful storage group backups. If the backup job consists of (Microsoft Exchange Server) document level backups, the makeup job backs up only the failed mailbox stores and databases. The makeup job does not back up the all of the items selected if it contained successful mailbox store and database backups.
- **Agent-based backups**--If the backup job requiring a makeup job consists of agent-based backups (for example, Sybase, Informix, Oracle, and so on), the makeup job will attempt to back up all of the source selected (instances, databases, tables, and so on) for the backup. If the makeup job fails after one unsuccessful attempt, CA ARCserve Backup will create another makeup job that consists of all of the source selected for the original job, and submit the makeup job with a status of Hold.

More information:

[Local Backup Options for UNIX Agents](#) (see page 139)

Backup Manager Pre/Post Options

Pre and Post options let you run commands before and after a job is executed.

The list that follows describes commands that you can run using Pre and Post options.

- You can use the Pre option to stop the application that owns the data you are about to back up, and then use the Post option to restart the application after the backup is complete.
- You can use the Pre option to defragment a disk before a backup job starts.
- You can use the Post option to delete files from a disk after that backup is complete.

Be aware of the following behavior when using Pre and Post options:

- CA ARCserve Backup does not support running commands with executables that reside on remote systems.
- Using a Pre option and specifying an exit code prevents the backup operation from starting until after the Pre option process is complete.
- Using a Pre option and specifying an exit code and the Skip Operation option causes CA ARCserve Backup to skip the backup operation and, if specified, prevents the Post option process from starting.
- Post option processes start unless the following conditions are present:
 - An exit code is specified, the Skip Post Application option is specified, and the result exit code is equal to the exit code specified.
 - The result of the backup operation is equal to the value specified for the Do not run Command if option.
- Pre and Post options specified as global options run commands before a job starts or after a job finishes. Pre and Post options specified as node-level (local) options run commands before a node is backed up or after a node is backed up.

For example, a user submits a backup job consisting of nodes A and B. A Pre option is specified as a global option and a Pre option is specified for node B. Immediately before the job runs, the global Pre option executes. While the job is running, the Pre option specified for node B executes before node B is backed up.

Run Command Before Operation Options

Enter the path to and name of the file to be executed on the machine before the job takes off.

- **On Exit Code**--CA ARCserve Backup detects exit codes of other programs. You can specify the following options for a particular exit code:
 - **Run Job Immediately**--The job runs immediately if the selected exit code is returned.
 - **Skip Job**--The job does not run if the appropriate exit code is detected.
 - **Skip Post Application**--Skip any commands specified to run after the job if the appropriate code is detected.
- **Delay in Minutes**--Specify the delay in which CA ARCserve Backup waits before running a job when the appropriate exit code is detected.

Run Command After Operation Options

Enter the path and name of the file to be executed on the machine after the job is completed.

Do Not Run Command If Options

Specify for a command not to run if CA ARCserve Backup detects that a job fails, a job is incomplete, or a job is complete.

Note: This option is not available when you are using CA ARCserve Backup to manage a UNIX or Linux based server.

Run Before/After Command As Options

The User Name and Password corresponds to the system of the host server selected, and is required to check the system privileges on that server.

The user name and password entered into these fields should not be confused with the CA ARCserve Backup User Name and Password.

Example: Submitting a Job Using Pre and Post Commands

A user submits a job that backs up local volume C. The user wants to check and fix errors using `chkdsk.exe` on local volume C before local volume C is backed up. After the job is complete, the user wants to generate an error report using `CAAdvReports.exe`.

Pre Command for the node:

The command that follows checks and fixes errors on local volume C before the backup job starts.

```
chkdsk.exe C: /F", 0n Exit Code = 0, Run operation immediately
```

Post Command for the job:

The command that follows generates an error reports and saves it in a specified location.

```
CAAdvReports.exe -reporttype 5 -maxSize 5 -Server DUVD001 -outfile  
"C:\Program Files (x86)\CA\ARCserve Backup\Reports\Backup Error  
Report_data.xml" -PastDays 1 -AutoName
```

Backup Manager Agent Options

Effective with this release, you may select backup options on a per-database basis or define a set of default options for all databases in a backup job. The Agent then applies the options to each database as appropriate.

Database Level Options -- These options apply to only the selected database and can either extend or override the Global Agent options. Database Level Options are accessed from the Agent Options shortcut menu.

Global Agent Options -- These options let you specify default job options for all selected objects in the SQL Agent type. Global Agent Options are not supported by releases of the Agent prior to r12.5.

Global Agent Options applied at a global level let you specify default job options for all Microsoft SQL Server databases. Options selected for a specific object at the database level can either extend or override the options specified as a global option. As a general rule, options applied at the global level will extend or override options that you specify on the Job Schedule tab.

Note: The agent combines options that you specify at the database level for a specific database with the appropriate global agent options.

You can specify Global Agent Options for the CA ARCserve Backup components that follow:

- [Agent for Microsoft SQL Server](#) (see page 163)--Includes the Agent for CA ARCserve Backup Database, which is supported by CA ARCserve Backup Agent for Microsoft SQL Server, r12.5 and later.
- [Agent for Virtual Machines](#) (see page 170)--Supported by the CA ARCserve Backup Agent for Virtual Machines, r12.5 and later.

Consider the behavior that follows when packaging jobs using the above-described agents:

- Global agent options are not supported by releases of the above-described agents prior to CA ARCserve Backup r12.5, nor are they applied if you use any other agent to back up Microsoft SQL Server databases.
- When you upgrade an older agent to CA ARCserve Backup r12.5, the agent applies both any pre-existing local options and all global options that apply and do not conflict with the database level (local) options.
- For jobs packaged using older agents, local options are carried over as local options.

Agent for Microsoft SQL Server Options

The options described in the sections that follow affect all backups that include Microsoft SQL Server databases and the CA ARCserve Backup database at the job level.

Note: Database level agent options override settings made on the Global Agent Options tab.

Backup Methods

The following backup methods are provided:

Use Global or Rotation Options

Use Global or Rotation Options is the default setting.

CA ARCserve Backup can apply Incremental and Differential global backup methods from the Job Scheduler when backing up Microsoft SQL Server databases. This lets you use rotation schemes to perform differential and Transaction Log backups of Microsoft SQL Server databases, which are dynamically adjusted based on the limitations of each individual database.

In releases of the agent that pre-date CA ARCserve Backup r12, the Global Backup Method or Rotation Scheme from the Job Scheduler override local database options. In this release, the Global Backup Method or Rotation Scheme is applied only if you selected Use Global or Rotation Options in the database level options for the database and in the Global Agent Options for SQL Server.

This option backs up the selected database using the Backup Method from the Job Schedule. The Job Methods are applied using the logic that follows:

- The Full job method will result in a Full backup of the database.
- The Differential job method will result in a Differential backup of the database, unless this database has not yet had a Full backup.
- The Incremental job method will result in a Transaction Log backup With Truncation for databases using the Full and Bulk-Logged Recovery Models, and a Differential backup of databases using the Simple Recovery Model, unless this database has not yet had a Full backup.
- The three main System databases are exempt from the Job Method and from the Backup Method in the Global Agent Options; selecting this option for databases master, model, or msdb will always result in a Full backup.

Full

A Full backup is performed. All files included in the Database Subset selected will be backed up in their entirety.

Differential

Backs up only data that has changed since the last Full backup. For example, if you ran a complete backup of your database on Sunday night, you can run a differential backup on Monday night to back up only the data that changed on Monday.

Note: When selected in the Global Agent Options, this option is ignored by system databases. Databases that have not received a Database Full Backup will revert to a Full Backup.

Transaction Log Only

Backs up only the Transaction log. This option is only available for databases using the Full and Bulk-Logged Recovery Models. For databases using the Simple Recovery Model, CA ARCserve Backup performs a Differential backup when you select Transaction Log Only from the Global Agent Options tab.

Note: When selected in the Global Agents Options, this option is ignored by system databases. Databases that have not received a Database Full Backup will revert to a Full Backup.

The backup method selected on the Global Agent Options tab overrides the selection made in a job's global backup method or rotation phase in the Job Scheduler. If you select the backup method using the Global Agent Options tab, note the following:

- The three system databases (master, model, and msdb) are exempt from the Backup Method in the Global Agent Options tab.
- For databases that have not yet received a Database Full backup, CA ARCserve Backup ignores the backup method set in the Global Agent Options tab and performs a full backup by default.
- For databases using the Simple Recovery Model, CA ARCserve Backup performs a Differential backup when you choose Transaction Log Only on the Global Agent Options tab.

Because any selection other than Use Global or Rotation Method for a database overrides the selection in the Global Agent Options dialog, the Backup Method is not affected by the Override Global Options setting on the database's Agent Options dialog.

Database Subset

Database Subset options let you define the types of database components that you want to back up. You can use this option to choose between the entire database, or a selection of files and FileGroups contained within the database, when the size of the database and performance requirements do not allow you to back up the entire database.

Database Subset options are disabled if the selected Backup Method for a database is Transaction Log Only. Of the following Database Subset options, only the Back up Transaction Log After Database option is available on the Global Agent Options dialog.

Entire Database

Backs up the entire database.

Files and FileGroups

Backs up selected files in a database. Use this option to back up a file or FileGroup when the database size and performance requirements make it impractical to perform a full database backup. This option is only available for databases using the Full and Bulk-Logged Recovery Models.

Note: For Microsoft SQL Server 7.0 databases, CA ARCserve Backup performs a Files and FileGroups Full backup if you set the database subset to Files and FileGroups for the database level and backup method to Differential on the Global Agent Options tab.

Partial Database

Backs up the Primary FileGroup, and any other Read-Write FileGroups. For a Read-Only database, only the Primary FileGroup will be backed up. This option requires SQL Server 2005 or later.

Back up Transaction Log After Database

Backs up the Transaction Log after the database, partial database, or selected set of data files is backed up. This allows you to perform both a Full or Differential backup and a Transaction Log backup in the same job. This option is only available for databases using the Full and Bulk-Logged Recovery Models and is ignored for databases using the Simple Recovery Model if set in the Global Agent Options dialog.

Be aware of the following:

- If you select this option on the Global Agent Options tab and specify Incremental backup method using the Job Scheduler, CA ARCserve Backup performs only one transaction log backup on the database and uses the Transaction Log Truncation Options from the Global Agent Options tab instead of the Incremental backup's default behavior (truncate the transaction log).
- If you select this option using the database level agent options, set the backup method at the database level to Use Global or Rotation, and set the backup method in the Global Agent Options to Transaction Log Only, CA ARCserve Backup performs only one transaction log backup on the database and uses the Transaction Log Truncation Options set from the database level.
- If you select this option in the Global Agent Options dialog and specify Transaction Log Only in Database Level Options, this option and the accompanying global Log Truncation Options setting is ignored for that database.

Log Truncation Options

The Log Truncation Options include the following:

Remove inactive entries from transaction log, after backup

(Truncation) Truncates the Transaction Log files, removing entries included in the backup so that the space in the files can be reused. This is the default option.

Do not remove inactive entries from transaction log, after backup

(No truncation) Retains backed up log entries after backup. These entries will be included in the next Transaction log backup.

Backup only the log tail and leave the database in unrecovered mode

(No recovery) Backs up the log and leaves the database in a restoring state. This option is available for Microsoft SQL Server 2000 or later. Use this option to capture activity since the last backup and take the database offline prior to restoring or repairing it.

The Log Truncation Options are available only when the selected Backup Method is Transaction Log, or when the Backup Transaction Log After Database option is checked.

Important! Do not use the "Backup only the log tail and leave the database in unrecovered mode" log truncation option to back up the ARCserve Database. Performing a backup with this option causes the database to be placed in an offline status, and you can lose the ability to find the backups of the ARCserve Database in order to perform a restore and bring the database online. If you perform a backup of the ARCserve Database using this option, you can use the `ca_recoverdb` command line utility to restore the ARCserve Database and bring it back online.

Log Truncation Options are not affected by the Override Global Options setting on the database level Agent Options dialog. If Transaction Log or Backup Transaction Log After Database is selected for the database, the database Log Truncation Options are used.

Database Consistency Check (DBCC) Options

A database consistency check (DBCC) tests the physical and logical consistency of a database. DBCC provides the following options:

Before Backup

Checks consistency before the backup of the database. (This option is not available for Restores.)

After Backup

Checks consistency after the backup of the database. (This option is not available for Restores.)

Continue with backup, if DBCC fails

Performs a database backup even if a consistency check before backup reports errors. (This option is not available for Restores.)

After restore

Performs DBCC after the restore of the database. (This option is not available for Backups.)

Before restore

Performs DBCC before an Online Torn Page Repair restore of the database. (SQL Server 2005 or later, Enterprise Edition only. This option is not available for Backups.)

Do not check indexes

Checks the database for consistency without checking indexes for user-defined tables.

Note: The system table indexes are checked regardless of whether you select this option.

Check only the physical consistency of the database

Detects torn pages and common hardware failures, but does not check the data against the rules of the database schema. It still checks the integrity of the physical structure of the page and record headers, and the consistency between the page's object ID and index ID. This option is available for Microsoft SQL Server 2000 or later. If this option is selected from the Global Agent Options tab, it is ignored for SQL Server 7.0 databases.

All error messages that are generated during the DBCC are recorded in the Agent for Microsoft SQL Server log file called sqlpagw.log. The log is located in the Backup Agent directory.

Example: How DBCC Options Work

The following example illustrates how DBCC options work in conjunction with Override Global Options on the Agent Backup Options dialog.

- With Override Global Options specified, the DBCC options selected at the database level will be the only DBCC options specified.
- With Override Global Options not specified, all of the DBCC options specified for the database and all of the DBCC options selected in the Global options will be applied together.

On the Global Options dialog, Agent Options tab, the Database Consistency Check options that follow are specified:

- After backup
- Do not check indexes

On the Agent Backup Options dialog, Override Global Options is not selected and the Database Consistency Check options that follow are specified:

- Before backup
- Continue with backup, if DBCC fails

Note: To open the Agent Backup Options dialog, open the Backup Manager, click the Source tab, browse to and expand the CA ARCserve Backup server, right-click the CA ARCserve Backup database, and then select Agent Option from the pop-up menu.

When you submit the backup job, CA ARCserve Backup applies the DBCC options specified in logical order: Perform the DBCC before the backup starts. If the DBCC fails, perform the backup. After the backup is complete, do not check the indexes.

Other Options

Include Checksum Generated by SQL Server

Includes error checking information from Microsoft SQL Server, which can be used to validate the integrity of the backed-up data during restore. This option requires SQL Server 2005 or later and is ignored when set in the Global Agent Options dialog for SQL 7.0 or 2000 databases.

Override Global Options

Causes the Agent to ignore all checkbox-based options from the Global Agent Options tab for only the specified database.

Note: Backup Method and Transaction Log Truncation options are not affected by this option because they can be overridden separately. This option is available only on a per-database basis.

Agent for Virtual Machines Options

The options that follow affect all VM backups in your environment at the job level.

Backup Mode Options

The options that follow determine the backup method used for the backup.

File Mode

Use File Mode when you need to protect individual files and directories. File mode backup lets you perform the tasks that follow:

- Back up files and directories at file level granularity contained in VM.
- Perform full, incremental, and differential backups.
- Restore data at file level granularity.
- Process multiple streams of data simultaneously using the Multistreaming option.
- Filter data using the Filter option.

Note: The elapsed time required to perform a file level backup of a full VM is greater than the elapsed time required to perform a raw (full VM) level backup of the same volume.

Raw Mode

Use Raw mode when you need to protect entire systems for disaster recovery. Raw mode backup lets you perform the tasks that follow:

- Perform full backups of full VM images only.
- Process multiple streams of data simultaneously using the multistreaming option.

Note: Raw mode does not let you restore data at file level granularity or filter raw (full VM) data. Filters applied to raw mode (full VM) backups are ignored at runtime.

Mixed Mode

Mixed mode is the default backup mode. Mixed mode lets you perform the tasks that follow:

- Perform GFS and rotation backup jobs that consist of weekly full backups in full VM (raw) mode and daily incremental and differential backups in file mode in a single backup job.

Note: Rotation and GFS rotation jobs are advantageous in that they contain backup data that provides you with daily protection (file level backups) and disaster recovery protection (raw, full VM backups) in a single backup job.

Allow file level restore

Use Allow file level restore when you need to back up data using Raw Mode efficiency and restore data with File level granularity.

To perform granular file level restores from raw (full VM) backups, you must specify the name of the CA ARCserve Backup server on your VMs. For more information, see Specify the Name of the CA ARCserve Backup Server.

Allow file level restore lets you perform the tasks that follow:

- Restore Raw Mode backups at file level granularity
- Restore Mixed Mode backups at file level granularity
- **Note:** Allow file level restore can be used on all types of backups, including custom backups, rotation backups, and GFS rotations that consist of full, incremental, and differential backups. The full backups are captured in raw (full VM) mode and the incremental and differential backups are captured in file level backup mode. If you do not specify Allow file level restore, CA ARCserve Backup restores only the incremental and differential backups. The full backup, which is captured in Raw mode, is not packaged with the restore.

Incremental / Differential Method for VMware VM Options

Lets you specify the communication method that CA ARCserve Backup will use to transfer incremental and differential backup data on VMware VMs to the backup proxy system.

- **Use VCB--**Lets CA ARCserve Backup use VMware Virtual Consolidated Backup communication to transfer incremental and differential backup data to the backup proxy system. You should specify this option when you want to reduce the load on your network.

Note: Use VCB is the default setting.

- **Use Client Agent--**Lets CA ARCserve Backup use Client Agent for Windows communication to transfer incremental and differential backup data to the backup proxy system. With this option specified, CA ARCserve Backup transfers data via your network.

Backup Manager Job Log Options

The log options determine the level of detail that is included in the log report for the operation. The log options can be set in the following windows: Backup, Restore, Compare, Media Assure & Scan, Copy, Count, and Purge. CA ARCserve Backup provides the following log options:

- **Log All Activity**--Record all of the activity that occurs while the job is running in the Job Log.
- **Log Summary Only**--Record summary information on the job (including source, destination, session number, and totals) and errors.
- **Log Disabled**--Do not record any information about this job in the Job Log.

Backup Manager Virus Options

Since CA Antivirus is bundled with CA ARCserve Backup, you can automatically scan for viruses during the job using the virus scanning options.

Enable Virus Scanning

Select this option to enable virus scanning and the following options:

- **Skip**--Do not back up the infected file.
- **Rename**--If CA Antivirus detects an infected file (for example filename.com), it renames the file and appends 0.AVB to the file name (for example filename.com.0.AVB). If filename.com.0.AVB already exists, eTrust renames the file to filename.com.1.AVB, filename.com.2.AVB, filename.com.3.AVB and so on.
- **Delete**--Delete the infected file.
- **Cure**--Attempts to cure the infected file.
- **Scan Compressed Files**--Check each file in compressed archives individually. Selecting this option might affect the performance of the backup but provides increased virus protection.

Files and Objects that CA ARCserve Backup Does Not Back Up

CA ARCserve Backup does not back up the following files while processing backup jobs:

- DOS system files
- The following Windows files:
 - 386SPART.PAR
 - 386SPART.TMP
 - SPART.PAR
 - WIN386.SWP
- DoubleSpace files (DBLSPACE with any extension)
- DriveSpace files (DRVSPACE with any extension)
- Stacker files (STACVOL.DSK)
- Btrieve delta files
- The following Win32System files:
 - PAGEFILE.SYS
 - NETLOGON.CHG
 - NTUSER.DAT.LOG
 - CPL.CFG
 - EA DATA.SF
- The following CA ARCserve Backup files:
 - RDS.BAK
 - RDS.LOG

- The following registry keys:

\\HKEY_LOCAL_MACHINE\SYSTEM\CLONE

\\HKEY_LOCAL_MACHINE\HARDWARE

\\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup (and all files specified)

The above registry key is controlled by the CA ARCserve Universal Agent. The CA ARCserve Universal Agent service runs under the Local System account. As a result, CA ARCserve Backup will back up the files specified under FilesNotToBackup for the Windows Administrator account. If you do not want to back up the files specified under the Windows Administrator account, you must exclude the files explicitly under the above registry key. Alternately, you can modify the CA ARCserve Universal Agent service to run as the specific Windows Administrator account. To allow the CA ARCserve Universal Agent service to run as the specific Windows Administrator account, do the following:

1. From the Control Panel, choose Administrative Tools and then choose Services.
2. Click the CA ARCserve Universal Agent service from the Services list.
3. Click Action, Stop to stop the service from running.
4. Right-click the service and click Properties.
5. On the Log On tab of the Properties dialog, click This Account and provide the required credentials.
6. Click OK.
7. Restart the CA ARCserve Universal Agent service.

- Registry files with the extensions *.ALT and *.LOG

Note: For a list of exceptions, see the topic Known Issues for the Base Product in the Readme.

- Cluster installation directory files (typically, the WINNT\cluster folder), files with no extensions, and files with the extension *.LOG
- \RECYCLER folder
- \Document and Settings\Administrator\Local Settings\Temp folder
- %systemroot%\Temp (all files and subfolders inside)
- Folders for file system devices.
- If database agents are installed, all files backed up by the agents are skipped.
- Database folders in the CA ARCserve Backup home directory are skipped during regular file backup operations.

Enable CA ARCserve Backup to Manage Open Files on Remote Computers

If the CA ARCserve Backup Agent for Open Files is installed on any of your computers, you can manage the BAOF Engine directly from the Backup Manager.

To enable CA ARCserve Backup to manage open files on remote computers

1. Open the Backup Manager and select the Source tab.
2. From the Source directory tree, select the system that you want to manage remotely.
3. If this server has the BAOF Engine installed, right-click the computer and select the following menu items or simply click these items in the Additional Information pane, on the bottom-right of the screen:
 - **Configure Open File Agent**--This displays the BAOF Configuration screen. From here, you can set various global settings for BAOF on the selected computer.

Note: For more information about the General, File/Group, and Clients options, see the online help or the *Agent for Open Files Guide*.
 - **View Open File Agent Status**--This displays the BAOF Status screen. This shows which files and groups BAOF is currently processing on the selected computer.
 - **View Open File Agent Log File**--This displays the Log File Viewer screen. This shows the log file for the selected computer.
4. Click OK.

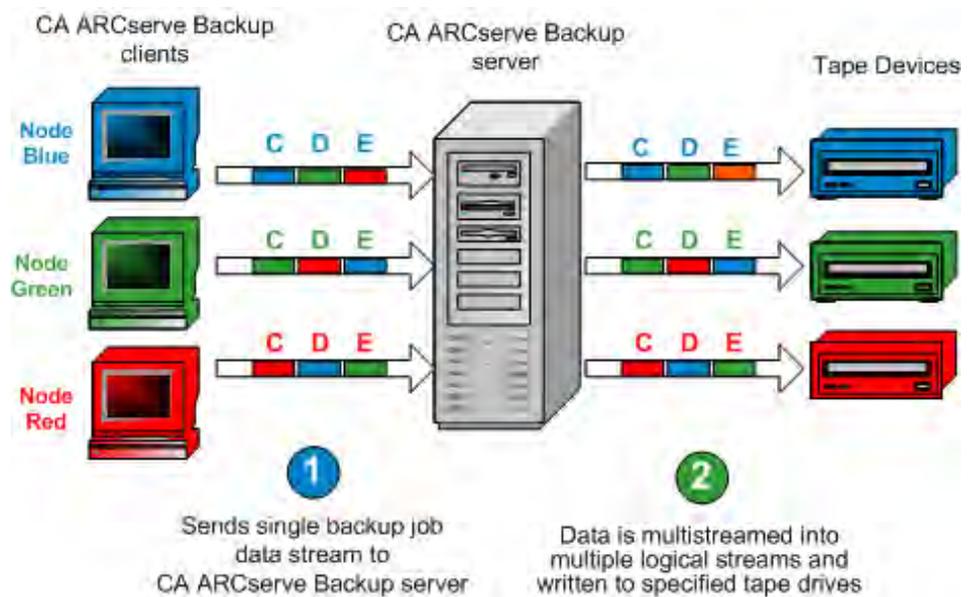
You have successfully applied the open file settings.

How Multistreaming Processes Backup Data

Note: To use multistreaming, you must install and license the CA ARCserve Backup Enterprise Module.

Multistreaming is a process that divides your backup jobs into multiple sub-jobs (streams) that run simultaneously and sends data to the destination media (tape device or file system device). Multistreaming is used to maximize the effective use of the client machines during backup and recovery operations. Multistreaming is useful when performing large backup jobs, since it is more efficient to divide multiple jobs between multiple backup devices.

Multistreaming lets you use all of the available tape devices on the system by splitting your backup jobs into multiple jobs using all available tape devices. As a result, it will increase the overall backup throughput compared with the sequential method.



You can use all of the devices or you can specify a single group of devices. If the CA ARCserve Backup Tape Library Option is installed and the group with the library is selected, multistreaming uses all library devices. If the CA ARCserve Backup Tape Library Option is not installed, you can put devices into separate groups. For a changer, the total number of streams (child jobs) that are created depends on the number of tape devices. For a single tape drive device, the total number of streams depends on the number of device groups.

Multistreaming is performed at the volume level for regular files (two volumes can run simultaneously on two separate devices), and at the database level for local database servers. Multistreaming is performed at the node level for the Preferred Shares folder, remote database servers, and Windows Client Agents.

You can have only as many jobs running simultaneously as the number of devices or groups that are on the system. With multistreaming, one parent job is created that will trigger child jobs for as many volumes as you have. When a job is finished on one device, another job is executed until there are no more jobs to run.

Some characteristics and requirements of multistreaming are as follows:

- Each client machine can have multiple source streams, depending on the number of agents being backed up.
- Each agent can have a separate stream (one stream per agent).
- Multistreaming always requires a media pool selection to prevent the tapes from being overwritten.
- Separate tape devices should be configured in separate groups for regular drives, however for changers, they can be configured to be in the same group..
- Multistreaming works with Rotation and GFS jobs.
- Canceling the parent job cancels all of the child jobs. For Windows, canceling and monitoring is checked between jobs for performance considerations.
- If a job spawns child jobs, the number of child jobs spawned will not exceed the number of streams specified for the job. However, if a job spawns child jobs and you do not specify a number of streams to use, the child jobs will be created and backed up in one continuous stream.
- Pre and post operation and comments is supported at the parent job level. Pre/post operations are not performed for child jobs.
- In the Job Status Manager, each child job has a default job description with this pattern:

```
JOB[ID][Servername](Multistream subjob [SID])[Status][Start time - End time][JOB No.]
```

Note: SID Represents the sub job (child) ID.

- The multistreaming option is ignored if the groups you choose have only one device, or if only one object (volume, database, or remote node) backup is submitted.
- Multistreaming is not supported on optical devices.

Note: You should use the same types of tape devices for multistreaming jobs. In order to achieve the optimum performance with your multistreaming jobs, you should use a high-end server machine with multiple processors and at least 256 MB memory per processor.

Specify Multistreaming Options

To specify multistreaming options

1. Open the Backup Manager window and select the Destination tab.
2. Check the Multistreaming check box.

Specify a **Max (Maximum) Number of Streams** to use. The default number of streams is 4. If you installed the Enterprise Module, the supported range is between 2 and 32.

Note: If a backup job with multistreaming spawns child jobs, the actual number of streams spawned will not exceed the number of streams specified for the job. However, if a job spawns child jobs and you do not specify a number of streams to use, the child jobs will be created and backed up in one continuous stream.

How Multiplexing Processes Backup Data

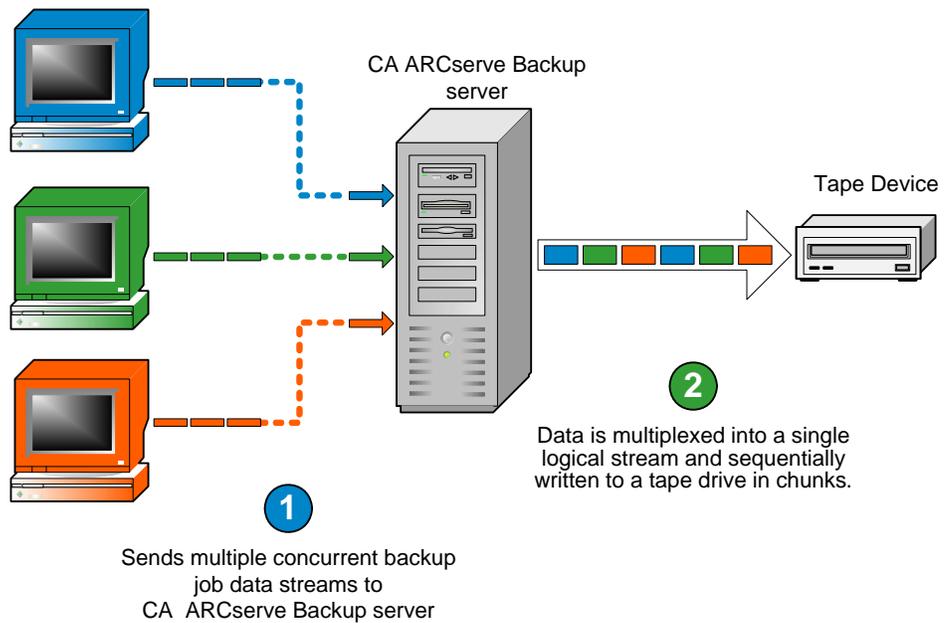
Note: You must install and license the CA ARCserve Backup Enterprise Module to process five or more streams of data simultaneously.

Multiplexing is a process in which data from multiple sources is written to the same media (tapes) simultaneously. Multiplexing is used to maximize the effective use of tape drives and libraries during backup and recovery operations and is useful when the tape drive is much faster than the backup source. Multiplexing keeps the backup hardware running at its maximum capability for the entire length of the backup process. A session included in a multiplexing backup should not be impacted by the speed of other sessions being multiplexed. The only factor that can limit the speed of a backup session is the speed of the hardware device.

The maximum number of jobs that you can multiplex is limited by the amount of available memory. The default number of jobs that you can multiplex is 4, and the minimum number is 2 while the maximum number is 32.

When a job that has multiple sources is submitted with the multiplexing option enabled, it is broken into child jobs with one for each source. These child jobs write data to the same media simultaneously. The number of child jobs spawned will, at most, be equal to the number of streams specified for multiplexing. However, if a job spawns multiple child jobs and the value specified for the Multiplexing Max # of Streams option is zero or one, the child jobs will be created and backed up in one continuous stream (the default Max # Stream is 4).

CA ARCserve Backup clients
(minimum of 2
maximum of 32)



Note: When using multiplexing, you can select the maximum number of streams that can write to a tape at the same time. For more information, see [Specify Multiplexing Options](#) (see page 182).

Multiplexing is useful when your tape drive throughput is faster than the rate at which data can be extracted from the source. Factors that can affect backup throughput are as follows:

- The kind of data being backed up. For example, backing up large number of small files reduces backup throughput because of the larger number of necessary file system operations (file open and close).
- Some databases may be inherently slow in providing data.
- The network throughput of the server being backed up.
- The disk performance on which the data resides.
- The server resources like CPU speed, memory size, page file size, network card, and amount of other activities on the server.
- Network backups that involve hundreds of servers.

When data is backed up over the network from multiple sources, most of the previous factors are involved, which reduces the throughput and increases the amount of time it takes to perform a backup. In addition, if the tape drive is not consistently streamed, the life of the tape drive is reduced drastically because of the "shoe shine" effect: when data is written intermittently, the drive has to stop, and then go back and forth on the media to adjust to the new position from where it has to write again. With multiplexing, data is continuously available and tape drives are constantly streaming. This decreases the amount of time it takes to perform a backup while increasing the life of the hardware.

Multiplexing is performed at the volume level for regular files, two volumes can run simultaneously as two separate child jobs, and at the database level for local database servers. Multiplexing is performed at the node level for the Preferred Shares folder, remote database servers, and Windows Client Agents.

In the Job Status Manager, each child job has a default job description with this pattern:

```
JOB[ID][ServerName](Multiplexing subjob [SID])[Status][Start time - End time][JOB No.]
```

Note: SID Represents the sub job (child) ID.

More information:

[Specify Multiplexing Options](#) (see page 182)

Functions Supported by Multiplexing

The following table includes the functions that are supported and not supported by multiplexing.

Supported	Not Supported
<ul style="list-style-type: none"> ■ Multiple jobs can write to the same tape drive. ■ Single session restore from multiplexing tapes. ■ QFA restore from multiplexing tapes. ■ Merge from multiplexing tapes. ■ Disaster recovery. ■ Session consolidation from a multiplexing tape to a non-multiplexing tape. ■ Scan and compare on multiplexing tapes. 	<ul style="list-style-type: none"> ■ Multiple restores simultaneously from a single multiplexing tape. ■ Multiple session consolidation simultaneously from a single multiplexing tape to multiple non-multiplexing tapes. ■ The Verify after Backup option. ■ Disk staging during multiplexing. ■ Multiplexing jobs cannot be submitted to NAS devices, File System Devices, RAID devices, and WORM media. ■ Multiplexing is not available if you are using the Image Option or the Serverless Backup Option. ■ Multiplexing jobs cannot be submitted to a non-multiplexing media. ■ Multiplexing is not supported on Optical Changers and DVD drives. ■ Multiplexing is not supported for NAS sources. ■ NetWare Directory Services (NDS) for NetWare sessions will be backed up at the end of a multiplexing job.

Multiplexing Job Options

To submit a multiplexing job, you must enable the Multiplexing feature on the Destination tab in the Backup Manager. In addition, you can select any of the following:

- Multiplexing media (multiplexing media appear with a blue circle with an M next to them)
- Blank media
- Media pool

Note: You cannot submit a multiplexing job to a tape library that has WORM media unless you use the Virtual Library option to split the tape library into groups so that one has WORM media and the other does not. If you do this, you can submit a multiplexing job to the group that does not have WORM media. For more information about the Virtual Library option, see Virtual Library Configuration Option.

More information:

[Virtual Library Configuration Option](#) (see page 335)

Specify Multiplexing Options

To specify multiplexing options

1. Open the Backup Manager window and select the Destination tab.
2. Check the Multiplexing check box and complete the following fields:

Chunk Size

Sets the performance of restore operations and memory usage. The chunk size value determines the amount of contiguous data written for one session before data from another session is multiplexed. The higher the value, the faster the restore on some drives, but at the cost of memory size during backup. For most drives, the default value of 1 MB is recommended.

Max (Maximum) Number of Streams

Sets the maximum number of streams that can write to a tape at the same time. The default number of streams is 4 and the supported range is between 1 and 4. If you have the Enterprise Module installed, the supported range is between 1 and 32.

Note: If a backup job with multiplexing spawns child jobs, the actual number of streams spawned will not exceed the number of streams specified for the job. However, if a job spawns multiple child jobs and the value specified for the Multiplexing Max # of Streams option is zero or one, the child jobs will be created and backed up in one continuous stream (the default Max # Stream is four).

How the Job Status Manager Monitors Multiplexing Jobs

After you submit a multiplexing job, you can monitor of the job using the Job Status Manager. In the Job Queue, multiplexing jobs appear in levels so that you can view the status of child jobs related to the parent job.

To view the child jobs, open the Job Status Manager, select the Job Queue tab, and then select and double-click the parent job as illustrated by the following screen:

Job Name	Backup Se...	Job No.	Job ID	Status	Execution T...
[name] - Backup [Custom, MUx] Every 6 h...	100-LL-SE...	11	125	HOLD	3/12/2009 ...
[name] - Backup [Custom, MUx] Every 6 h...	100-LL-SE...	28	125	DONE	3/24/2009 ...

After you double-click the parent job, the child jobs appear in the Job Monitor screen as illustrated by the following screen:

The screenshot shows the Job Monitor window for a specific job. On the left, there is a tree view of source nodes: 100-LL-COMP001 and 100-LL-COMP002 (172.24.36.107). The main pane displays a table of sources with their status, completion percentage, elapsed time, remaining time, and file count.

Source	Status	Completed	Elapsed Time	Remaining Time	File:
\\100-LL-COMP002 (172.24.36.107)\M:	Backup files...	100%	5h 3m 36s	0s	677
\\100-LL-COMP001\H:	Backup files...	100%	4h 26m 15s	0s	50

Below the table, there are tabs for 'Statistics' and 'Log'. The 'Statistics' tab is active, showing a summary of the job progress:

- Total Streams: 2
- MB/Minute: 4,069.31
- Files Processed: 731,708
- MB Processed: 1,247,927.07
- MB Estimated:
- Elapsed Time: 5h 8m 46s

In addition, the status of the parent job is the highest severity status of a child job. For example, if Child 1 is successful, Child 2 is incomplete, and Child 3 has failed, the parent job will denote a FAILED status.

Verify Multiplexing Data Integrity

If you want to verify the integrity of your data after your multiplexing job completes, use the Media Assure & Scan Utility to enable the Scan files global option with CRC verification and perform a scan media job.

For more information about the Media Assure & Scan Utility, see Media Assure & Scan Utility or the online help.

More information:

[Media Assure & Scan Utility](#) (see page 32)

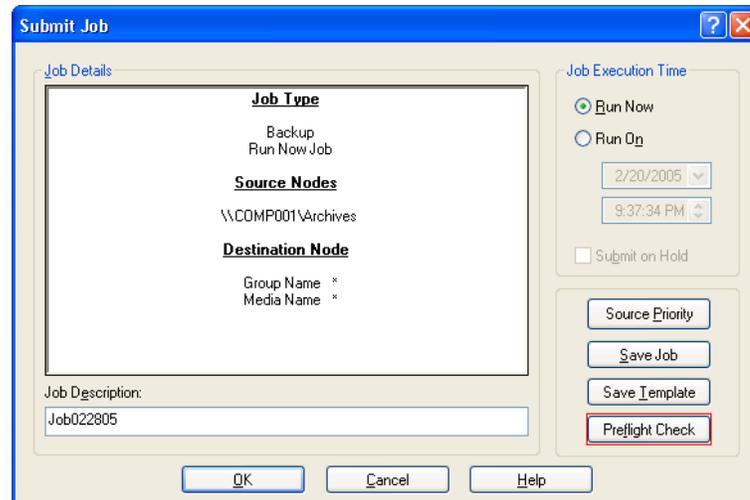
Preflight Checks for Your Backups

The preflight check (PFC) utility enables you to run vital checks on the CA ARCserve Backup server and agents to detect conditions that may cause backup jobs to fail. The checks performed by PFC fall into the following categories:

- **System Checks**--These include checking system requirements for the server, available disk space for the database, and RPC service registration.
- **CA ARCserve Backup Checks**--These include checking the CA ARCserve Backup system account and its privileges, the status of the CA ARCserve Backup engines, SAN server connectivity (if the CA ARCserve Backup SAN Option is installed), and the health of the tape devices attached to the server.
- **Agent Checks**--These include checking the connection and credentials for any client and database agents needed for the job.
- **Media Checks**--These include checking the availability of media in the scratch set (if a media pool is specified for the job), checking the media expiration dates, and checking for source and destination conflicts for File System Devices.

The optimum time to run this command is a couple of hours before your jobs are scheduled to run so that you can have ample time to correct any problems that may appear in the PFC report. For more information on the PFC utility and its associated options, see the *Command Line Reference Guide*.

Before submitting a job, you can run a Preflight Check clicking the Preflight Check button on the Submit Job dialog as shown in the following example:



Example: PFC Utility

You submit a job and run the PFC utility. If the PFC utility detects that a device is not assigned to the device group that you are using for the backup job, the PFC utility reports a failed job. To correct the problem, you must either use a device group with an assigned device or assign a device to the device group that you are using for the job. If you do not take corrective action, the job will eventually fail.

This capability is also supported when you run the PFC command line utility. For more information, see the *Command Line Reference Guide*.

Entire Node Backups

If you want to back up an entire node, CA ARCserve Backup provides the capability to backup all file systems and databases on the specified node. The benefits of backing up an entire node are as follows:

- You can direct CA ARCserve Backup to back up a selected node and all of its contents with a single click in the Backup Manager directory tree. CA ARCserve Backup backs up all file systems, databases, and drives in the directory tree when you specify the node.
- You can create a single backup job for the entire node. Tracking several to many backup jobs on a single node can become a difficult and time consuming maintenance task.

- You can modify the node without having to modify preconfigured backup jobs. For example, if you add a drive to the node, CA ARCserve Backup detects the new drive automatically and backs up the entire node when you run the backup job.

Note: This feature supports Centralized Cross-platform Management.

Back Up an Entire Node

When backing up a node that includes database files, you must provide proper authentication to access all databases when creating the backup job. Proper authentication includes the User Name and Password for the corresponding databases. You do not need to provide this authentication when the backup job runs.

To facilitate database authentication, CA ARCserve Backup presents the Security and Agent Information dialog when you are creating a backup job on an entire node. The Security and Agent Information dialog opens as you click the Submit toolbar button, or if you select Save or Save As from the File menu on the Backup Manager window.

The Security and Agent Information dialog serves two purposes:

- Display a list of all database files on the node.
- Set or change the User Name and Password for the database item selected in the Security and Agent Information dialog.

To back up an entire node (containing database files)

1. Open the Backup Manager and select the Source tab.
2. From the Source directory tree, select the node that you want to back up and click Start on the toolbar to submit the job.

If the node contains database files, the Security and Agent Information dialog opens to display a list of all databases on the node, User Names, and Passwords.

Important! Client Agent Password Security is only supported for the Client Agent for Windows, including the Agent for Open Files and VSS Writers. If Password Security is enabled and any database, application, or messaging agent is installed on the same machine as the Client Agent, whole node backup is not supported. System Security is the default setting. If you have enabled Password Security on the primary or stand-alone server, the automatically-generated Database Protection Job will fail for the job queue and the Catalog Database. You must not enable Password Security in the Agent Configuration on any machine running a database, application, or messaging Agent before submitting the job.

3. Optionally, to set or change a User Name or Password, click the Security button.

Enter the appropriate User Name and Password and click OK.

In the Security dialog, you must specify User Name and Password with backup rights on that machine. For example, Administrator or root.

Note: CA ARCserve Backup does not support logging in to systems with passwords that are greater than 23 characters. If the password on the system you are attempting to log in to is greater than 23 characters, you must modify the password on the agent system such that it is 23 characters or less, and then you can log in to the agent system.

4. Click OK.
The Submit dialog opens.
5. Complete the fields are required for the job and click OK.
The backup job for the entire node is submitted.

More information:

[Submit a Backup Job](#) (see page 129)

Create Repeating Backup Jobs

Repeating backup jobs let you automate the process of protecting systems in your environment. CA ARCserve Backup lets you create repeating back up jobs using CA ARCserve Backup rotation schemes or create custom rotation schemes.

You can perform full, incremental, differential, and Grandfather-Father-Son (GFS) backups.

To create repeating backup jobs

1. Open the Backup Manager window by clicking Backup in the Quick Start menu.
The Backup Manager window opens.
2. Click the Source tab.
3. On the Source tab, browse to and select the files you want to back up.
4. Do one of the following:
 - If you will be using the Disk to Disk to Tape Option, click the Staging tab, click the Enable Staging check box, and then choose a staging group.
 - Click the Destination tab to choose the group where you want to back up your data.
5. Click the Schedule tab, and select Use Rotation Scheme to use one of the pre-designed backup schemes.
You can choose a five or seven day schedule using incremental, differential, or full backups.
6. To modify a rotation scheme, highlight the day you want to change and click the Modify button.
For example, you might want to change a routine to initiate a full backup on Saturday.
7. Make the necessary modification to your schedule, and click OK.
8. Use the calendar to review the backup plan you selected. Click the Calendar View tab to see a calendar view of your rotation scheme.
9. Select the Start Date and Execution Time as required.

10. In the Media Pool Used field, enter the name of the media pool that you want to use for the rotation..
11. After you finish revising your backup schedule, click Start on the toolbar to submit the job.

Note: You can also make or view changes to your backup schedule by clicking the Exceptions tab. To make additional exceptions to your schedule, click the Add button to open the Exceptions dialog. Click the Date drop-down menu to open a calendar from which you can select the date you want to change.

Back Up Remote Servers

Before you can back up a remote machine, you must have CA ARCserve Backup installed and running on your server, and you must install the appropriate agent (in this case, the Client Agent for Windows) on the remote machine.

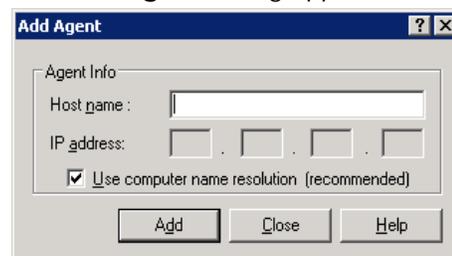
To back up remote servers

Note: The scenario that follows describes how to back up a server running Windows Server 2003.

1. From the Backup Manager, select the **Windows Systems** object. Right-click, and select **Add Machine/Object** from the pop-up menu.

Note: Alternately, you can use **Auto Discovery** to find machines with the selected agents installed.

The **Add Agent** dialog appears.



2. Enter the host name of the remote machine in the **Host Name** field.

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.

Check the **Use Computer Name Resolution** check box or specify the IP address of the computer. Click **Add** to include the remote server for backup, and click **Close**.

Note: CA ARCserve Backup lets you treat the backup of multiple servers as one job. If you choose this method, CA ARCserve Backup automatically submits the tasks in the job queue as one job and backs up the servers one after the other. Alternatively, you can select the **Schedule** tab and specify when each job should run to have CA ARCserve Backup back up each machine as a separate job.

3. Select the remote machine, and click the **+** to the left of it. The **Security** dialog appears, prompting you for security and agent information.

Enter your user name and password. You must supply this information to verify that you have sufficient rights to browse the machine and perform a backup. Click **OK**.

Note: CA ARCserve Backup does not support logging in to systems with passwords that are greater than 23 characters. If the password on the system you are attempting to log in to is greater than 23 characters, you must modify the password on the agent system such that it is 23 characters or less, and then you can log in to the agent system.

4. Repeat Steps 1, 2, and 3 for each machine you want to add.
5. Choose the sources and a destination for each machine you want to include in the backup.

Before you click **Start** to submit the backup job, you can set up an Alert to send you notification after the job runs.

Backup Staging Methods

CA ARCserve Backup provides two methods to backup to a staging area and then migrate (or copy) this data to a final destination (usually a tape).

- The disk staging method utilizes a disk as the staging area and is commonly referred to as Backup to Disk to Tape (D2D2T).
- The tape staging method utilizes a tape library or a virtual tape library as the staging area and is commonly referred to as Backup to Tape to Tape (D2T2T).

Each staging method contains specific options to control the behavior of CA ARCserve Backup during the backup process.

How to License the Disk to Disk to Tape Option

To successfully use the CA ARCserve Backup Disk to Disk to Tape Option, you must fulfill the following requirements:

- You must license the CA ARCserve Backup Enterprise Module to submit disk staging (D2D2T) backup jobs consisting of more than two simultaneous streams of data. This capability lets you process disk staging jobs efficiently, enabling backups of up to 32 streams of data. Additionally, you must license the Enterprise Module to submit backup to tape (VTL) to tape (D2T2T) jobs.
- You must issue all licenses on the primary server or a stand-alone server.
- Ensure that you have a sufficient number of licenses to support your environment.

Example: How to License the Enterprise Module for Disk to Disk to Tape Backups

The following example describes how count-based licensing works with the Disk to Disk to Tape Option:

- Your environment consists of a primary server and two member servers. You require the capability to perform staging operations on both member servers. You must purchase and issue two Enterprise Module licenses on the primary server.
- Your environment consists of a primary server and three member servers. You require the capability to perform staging operations on two ARCserve servers. You must purchase and issue two Enterprise Module licenses on the primary server.

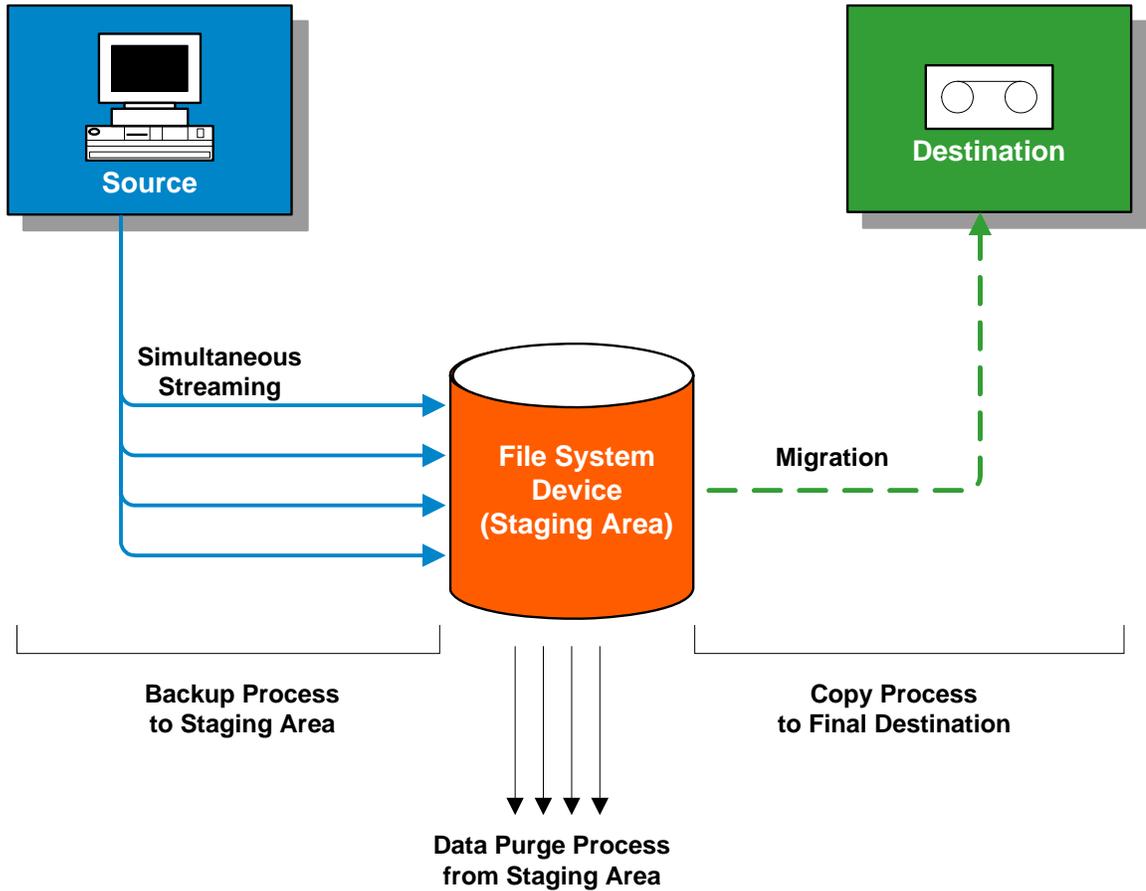
In the event you submit a D2D2T backup job on the third ARCserve server, the job will fail due to an insufficient number of licenses. To correct the error, you must issue a third Enterprise Module license and then resubmit the job.

How Backup to Disk to Tape Works

The Disk to Disk to Tape Option allows you to back up data to a temporary data storage location (staging area), and then based on selected policy options, migrate (copy) the data to the final destination (which could be a tape or disk) or automatically purge the data from the staging area after a specified duration time. When necessary, the Disk to Disk to Tape Option also allows you restore data directly from the staging area.

The Disk to Disk to Tape Option is basically a two-part data backup process.

- **Backup Process**--Backs up data from the source to the staging area.
- **Copy Process**--Copies or migrates the backed-up data from the staging area to the final destination.



How to Use Disk Staging to Manage Backup Data

The following list describes how you can use staging to manage backup data.

- Using the Disk to Disk to Tape Option to back up data, you can back up data to a file system device (FSD) that is used as a temporary staging area. A staging job can divide your backup job into several subjobs that run simultaneously. The Disk to Disk to Tape Option lets you use simultaneous streaming to send multiple streams of data to the FSD. Since the data is split among several different streams, backup jobs with simultaneous streaming enabled can be completed significantly faster than regular backup jobs.

- You can then migrate (copy) the data from the FSD to a final storage media (or from disk to tape). As a result, the tape drive can be kept streaming, thereby minimizing the shoeshine effect (starting, stopping, and repositioning the tape), and increasing both the life expectancy and efficiency of the tape drive. While the backup image is still on the FSD, data can be restored directly from it. The restore time is significantly reduced because restoring data from disk is generally faster than restoring from a tape (no delays due to tape load and seek latency).
- During the backup-to-FSD process, if the FSD gets full or reaches the specified maximum threshold, the Disk to Disk to Tape Option allows you to create makeup jobs which would then back up the data directly to the final destination after the staging backup job fails. This increases the success rate of backups. In addition, if there are any errors during the copy-to-final destination process, the Disk to Disk to Tape Option also allows you to create makeup jobs.

Note: Under disk full conditions, the makeup job created to back up the data to tape will always try to use a blank tape or a media from a scratch set. It will never try to append to an existing media.

- The backup images are kept on the FSD until the retention time expires (as determined by the specified purge policy). At that time, the Disk to Disk to Tape Option automatically purges the data from the FSD, and reclaims valuable disk space so that additional backups can continue.
- For rotation jobs or GFS rotation jobs, the Disk to Disk to Tape Option allows you to specify policies to disable staging for any particular day. This feature is helpful in situations where the FSD is full, is scheduled for maintenance, or has a problem.

More information:

[How to Use Tape Staging to Manage Backup Operations](#) (see page 226)

Disk to Disk to Tape Option Capabilities

In addition, the Disk to Disk to Tape Option provides the following capabilities:

- **File System Device Capacity Management**--The Disk to Disk to Tape Option allows you to specify minimum capacity and maximum capacity thresholds of the file system device. The maximum threshold can be represented as either an absolute value or as a percentage of the capacity of the volume.
- **Ensures that CA ARCserve Backup does not use the full capacity of a disk**--A backup job will fail when writing to a file system device if the total disk space used exceeds the maximum threshold.

Important! File System Devices (FSD) that are part of a staging group cannot be erased or formatted using the corresponding utility from the Device Manager window. To prevent accidental erasing or formatting of an FSD prior to the staged data being migrated to a final destination media, the Erase and Format toolbar buttons on the Device Manager window are disabled. If you want to erase or format the FSD, you can either use the command line (`ca_devmgr`) or disable the staging option for the selected FSD.

- **Increases your overall backup success rate**--You can define staging policies that let you create makeup jobs that back up directly to tape if an exceeds maximum threshold condition occurs or to create a makeup job on hold if a data migration failure occurs.
- **Pause Data Migration**--The Disk to Disk to Tape Option allows you to pause the migration of data from the FSD to the final destination (tape) by enabling the Pause Data Migration option. This feature allows you to continue backing up to the FSD, but pause the migration from the FSD to the final destination in case the tape library is scheduled for maintenance or has hardware problems.
- **Simultaneous Streaming**--Simultaneous streaming is a process that divides your backup jobs into several subjobs that run simultaneously. The Disk to Disk to Tape feature allows you to utilize the simultaneous streaming feature to send multiple streams of data to the temporary staging device (FSD) at the same time. Since the work is split up among several different streams (for concurrent writing to the FSD), simultaneous streaming-enabled backup jobs can be completed significantly faster than regular backup jobs. Simultaneous streaming also provides the capability to restore data while backup jobs are running.

Note: Disk to disk to tape is no longer a separately-licensed option. It is now part of the Enterprise Module. You can still perform disk to disk to tape backups without licensing the Enterprise Module, however, the maximum number of streams for such jobs is two. To submit more than two streams in disk to disk to tape backups, you must license the Enterprise Module.

- **SnapLock Support**--SnapLock™ is technology from Network Appliance that provides non-erasable, non-rewritable, Write Once Read Many (WORM) data protection. The Disk to Disk to Tape Option allows you to enable SnapLock protection on the backup operation. When you back up data with SnapLock protection enabled, you cannot purge or over-write the backed up data until the specified retention time elapses. This ensures that the data on the FSD can not be deleted by any user, thus providing WORM support on disk with a retention time out. The retention time for the enabled SnapLock protection is determined by the specified settings for the staging purge policies.

Note: The device must support SnapLock technology. If you enable SnapLock on a device that does not support SnapLock WORM protection, CA ARCserve Backup write-protects the data, however, the data can be deleted from the device.

- **Copy Image Tracking**--CA ARCserve Backup provides the capability to track copied images on different media. As a result, the merging of catalogs only has to be performed one time, and then all sessions which are copies of each other would point to the same catalogs.
- **Flexible Restore Options**--During the time period that the backed-up data is located both on the final destination media (tape) and on the FSD (prior to purging), the Disk to Disk to Tape Option provides you with a choice for selecting the source for restoring the data. If the backup image is located on both the FSD and the final destination, you can choose where to restore it from.
- **Smart Restore**--CA ARCserve Backup provides a transparent Smart Restore feature, which is further enhanced by the Disk to Disk to Tape Option feature of providing multiple locations for the backed-up data. If during the restore process from either the FSD or from the final destination, a media or drive error occurs, CA ARCserve Backup internally finds the alternate media and starts restoring the data from the alternate media. This increases the success rate of restores in the event of any hardware problems.
- **Optimize Restore Option**--If, during a restore operation, CA ARCserve Backup discovers duplicate backup sessions, where one session resides on tape media and another session resides on a file system device, the Optimize Restore option directs CA ARCserve Backup to restore the data from the session that resides on the file system device.
- **Command Line Support**--CA ARCserve Backup allows you to create backups to an FSD using either the graphical user interface (GUI) or the command line utility. In the event that a copy-to-tape operation fails, you can use the Query tool to analyze the file and session contents on the FSD. If you need to purge sessions from the FSD, you can use the Purge tool to remove data and free extra space on the FSD.

- **Disk to Disk to Tape Option Reports**--CA ARCserve Backup provides the capability to generate additional reports dedicated to the Disk to Disk to Tape Option. Using these reports you can find the backup to disk status of every session, whether a session was copied, when the session was copied, where the session was copied, whether the session was SnapLocked, when the session will be purged from the FSD, and other valuable information.

How to Manage Backup Data Using Staging

The following sections provide information about how to protect data using disk staging (B2D2T and B2T2T) operations.

More information:

[How to Manage Backup Data Using Tape Staging](#) (see page 223)

Staging Operations

The operations and tasks associated with the Disk to Disk to Tape feature include the following:

- Specify and configure file system devices, tape libraries, and virtual tape libraries.
- Configure devices as a staging group and configure staging group policies.
- Submit backup jobs to a staging group.
- Define policies for managing backup, data migration, data security, data purge, alert messages, and postscript operations.
- Perform simultaneous backup operations to devices in a staging group.
- Disable staging in rotation and GFS rotation backup jobs on any specified day of the week.
- View the status of master and child jobs in the Job Status Manager. The Job Status Manager displays a tree view of all master jobs and their corresponding child jobs for backup and migration operations.
- View the Activity Log (in Windows) displaying the logs of all the child jobs and migration jobs, and the purging activities of the master job in a tree format.
- Restore data from a staging device. If the data from a backup job resides in two locations (on the file system device and on the final destination media), you can restore the data from either location.

- Run command line tools that can analyze and purge data stored on a FSD in a staging group.
- Access reports using the Report Manager to capture information about purge and migration activities on FSDs.

Note: Disk to disk to tape is no longer a separately-licensed option. It is now part of the Enterprise Module. You can still perform disk to disk to tape backups without licensing the Enterprise Module, however, the maximum number of streams for such jobs is two. To submit more than two streams in disk to disk to tape backups, you must license the Enterprise Module.

How the Max Number of Streams Option Affects Backup and Restore Operations

Simultaneous streaming is a process that divides your backup jobs into several subjobs that run simultaneously. The Disk to Disk to Tape feature lets you use the simultaneous streaming feature to send multiple streams of data to a device in a staging group. Since the work is split up among several different streams, simultaneous streaming-enabled backup jobs can be completed significantly faster than regular backup jobs.

CA ARCserve Backup provides you with the capability of streaming multiple jobs simultaneously to the FSD. The base product allows you to write a maximum of two streams per job simultaneously, as well as two streams per staging group simultaneously. Licensing the Enterprise Module enables you to increase the simultaneous streams to 32 (for each job and each staging group).

When you back up data using the Disk to Disk to Tape Option, a backup job can spawn child jobs. Each child job employs one stream of data. The actual number of child jobs that the parent job can spawn varies depending upon whether the backup job is a node-level or a volume-level backup job. However, the number of child jobs will never exceed the number of streams specified for staging.

Note: If a job spawns child jobs and you do not specify a number of streams to use, the child jobs will be created and backed up in one continuous stream.

For a node-level backup job, the number of child jobs spawned depends upon the number of agents specified in the backup job. Similarly, for a volume-level backup job, the number of child jobs spawned depends upon the number of volumes specified in the backup job.

Example: Staging Backup Jobs with Multiple Streams

If a backup job consists of backing up four nodes and the backup level is at the node level, the parent job can spawn a minimum of four child jobs. In this example, if you specify three streams, the master job can stream three child jobs simultaneously and start the fourth child job as one of the three previous child jobs end. After all child jobs are complete, the parent job is considered finished.

Staging Tab

To access the information and options on the staging tab, start the Backup Manager and select the Staging tab.

The Staging tab contains the following options and informational fields:

Enable Staging

Click the Enable Staging check box to enable or disable staging backup operations for a particular group.

Group Field

Displays the name of the group selected for this job.

Note: A staging group must be selected in a staging job. Specifying a "*" group is not allowed for staging.

Policy

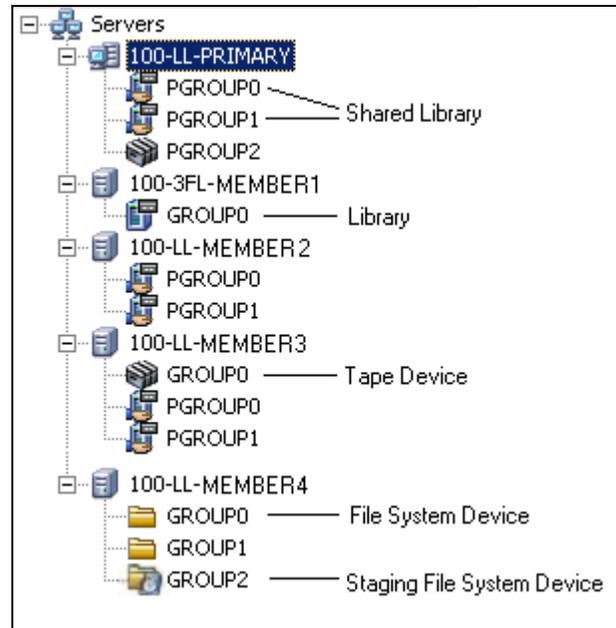
Opens the Staging Policy dialog. Using the Staging Policy dialog, you can specify staging policies for full, incremental, and differential backup operations. Staging policies allow you to specify copy policies, purge policies, enabling SnapLock protection, and other miscellaneous policies.

Max Number of Streams

Specifies the maximum number of simultaneous data streams that this job would be allowed to use while writing to the FSD in the staging group. For example, if the maximum number of streams is specified at 4, this means that at any point of time this staging job will have no more than 4 child jobs writing to the FSD simultaneously. To specify more than two streams, you must license the Enterprise Module.

Staging Groups Directory Tree

Displays the names of the groups which were configured as staging groups.



Properties View

From the properties view in the Backup Manager, you can perform the following tasks:

- Configure Groups-Click this option to open the Device Group Configuration dialog.
- Configure File System Device Groups-Click this option to open the File System Device Group Configuration dialog.

How to Configure the Disk to Disk to Tape Option to Perform Disk Staging Backups

If you plan to back up your data to disk, then it is recommended that you use the Disk to Disk to Tape Option, rather than just backing up to a file system device. The Disk to Disk to Tape Option allows you to do the following:

- Back up to disk and then copy the data to a final destination and delete the data on the staging device by creating staging groups.
- Create flexible policies that determine when you want to copy and delete data.
- Reduce the backup window when a single job breaks into multiple simultaneous streams while writing to a disk staging area. The number of simultaneous streams can be controlled according to your disk network throughput capabilities.

Before you can back up data using the Disk to Disk to Tape Option, you must perform the following tasks:

- Create the staging devices. First, you must specify the devices in your environment that you will use for staging operations.

Important! Staging backup operations can quickly consume a large amount of free disk space on file system devices. Due to the maximum file size limitations of FAT 16 and FAT 32 file systems, you should not use these file systems on file system devices designated for staging operations.

- Configure the staging groups. After specifying the devices in your environment, you must configure the device group to function as a staging group.
- Configure the staging policies. To perform backup operations using staging, you must define the copy and purge policies that CA ARCserve Backup will use to manage data stored on staging devices.

The following sections provide you with information about how to configure the Disk to Disk to Tape Option.

More information:

[How to Create File System Devices](#) (see page 337)

[Configure Device Groups to Use Staging](#) (see page 201)

[Modify Staging Groups Settings](#) (see page 204)

[Specify Copy and Purge Policies for Disk Staging Backups](#) (see page 205)

[Specify Miscellaneous Options for Disk Staging Backups](#) (see page 208)

[Specify Alert Options for Disk and Tape Staging Backups](#) (see page 210)

[Specify Postscripts Options for Disk and Tape Staging Backups](#) (see page 213)

Configure Device Groups to Use Staging

This section describes how to configure device groups for staging operations.

Note: Before you can configure device groups, you must specify the devices that you will use for staging operations. For more information, see [How to Create File System Devices](#) (see page 337).

To configure device groups to use staging

1. From the Administration menu in the Navigation Bar on the CA ARCserve Backup Manager Console, click Device Group Configuration.
Device Group Configuration opens.
2. Click Next.
The Login Page dialog opens.
3. Complete the required fields on the Login Page dialog and click Next.
The Options dialog opens.
4. From the Options dialog, select the server that you want to configure, click the **Configure Staging Groups** option, and then click Next.

5. From the **Groups** list, select the group that you want to configure. To enable staging for the selected group, click the **Enable Staging** option and then modify the following options as needed:

Max Threshold

Lets you specify the maximum amount of used space on a disk that CA ARCserve Backup will use for staging backups. When CA ARCserve Backup detects that the amount of used disk space exceeds the Max Threshold, CA ARCserve Backup pauses the backup job and purges the oldest migrated sessions from the FSD until the amount of used disk space is equal to or less than the Purge to Threshold.

Default value: If % is specified, 80%; if GB is specified, 8 GB; if MB is specified, 4000 MB.

The Max Threshold can be represented as either the total number of MB or GB used, or as a percentage of the total capacity used on the FSD. If the Max Threshold value is set as a percentage of the capacity of the FSD, the Max Threshold value must be equal to or less than 100% and the Purge to Threshold value must be greater than 0%.

Note: The Max Threshold must be greater than the Purge to Threshold. If you specify an absolute value (for example, MB or GB), the value must be equal to or greater than 1 MB.

Purge data when the used disk space exceeds the Max Threshold

Lets CA ARCserve Backup purge migrated sessions from the FSD when the amount of used disk space exceeds the Max Threshold.

Note: To ensure that the purge mechanism starts in a timely manner, best practice is to specify a Max Threshold value that is at least 100 MB less than the total disk space.

Purge to Threshold

Lets you specify the amount of used space on a disk when CA ARCserve Backup stops purging the oldest migrated sessions from the disk.

Default value: If % is specified, 60%; if GB is specified, 6 GB; if MB is specified, 3000 MB.

CA ARCserve Backup automatically specifies the units specified in the Max Threshold value (for example, %, MB, or GB). The Purge to Threshold value must be less than the Max Threshold value. If you specify an absolute value (for example, MB or GB), the value must be equal to or greater than 1 MB.

Example: The capacity of an FSD is 100 GB. The amount of used disk space is 75% (75 GB). The Max Threshold is 80% (80 GB) and the Purge to Threshold is 50% (50 GB). The administrator submits a job totalling 10 GB. CA ARCserve Backup detects that the job, when complete, will be greater than the Max Threshold. CA ARCserve Backup pauses the job and purges the oldest migrated sessions from the FSD until the amount of used disk space is equal to or less than the Purge to Threshold - in this example, 50% (or 50 GB). CA ARCserve Backup then continues the backup job.

Note: If CA ARCserve Backup purges all of the migrated sessions from the disk, but the amount of used continues to exceed the Purge to Threshold, CA ARCserve Backup restarts the job and attempts to complete the job using the available disk space.

Max # Streams

Lets you specify the maximum number of simultaneous streams to the selected file system device group. If you have licensed the Enterprise Module, you may specify up to 32 streams, otherwise, the maximum number is 2.

Note: If a job spawns child jobs, the number of child jobs spawned will not exceed the number of streams specified for the job. However, if a job spawns child jobs and you do not specify a number of streams to use, the child jobs will be created and backed up in one continuous stream.

Enable SnapLock for this group

Lets you enable SnapLock WORM protection on the file system device.

Note: This option is not available for libraries. To use this option, the file system device must support SnapLock technology. If you enable SnapLock on a device that does not support SnapLock WORM protection, CA ARCserve Backup write-protects the data, however, the data can be deleted from the device.

Pause data migration

Lets you pause the data migration operation.

6. Repeat Step 5 as necessary to configure other groups.
7. Click Next and then click Finish.

The options are applied to the job.

More information:

[How to Configure the Disk to Disk to Tape Option to Perform Disk Staging Backups](#) (see page 200)

Modify Staging Groups Settings

Use the following procedure to modify staging group settings.

To specify staging groups settings

1. From the Backup Manager window, click the **Staging** tab.
2. From the groups list, right-click a group and select **Configure File System Device Groups** from the pop-up menu.

The **Staging Group Configuration** dialog opens.

Note: You can also open the File System Device Group Configuration dialog by clicking the Configure File System Device Groups link located in the Properties view on the Staging or Destination tab.

3. Select the desired group and click the **Enable staging** check box.
4. In the **Max Threshold** field, specify the maximum file system device threshold. From the drop-down list, choose MB, GB, or %.
5. Click the **Purge data when the used disk space exceeds the Max Threshold** option if you want CA ARCserve Backup to automatically purge migrated sessions from the FSD when the amount of used disk space is greater than the Max Threshold

In the **Purge to Threshold** field, specify the amount of used space on a disk when CA ARCserve Backup stops purging the oldest migrated sessions from the disk.

6. When you enable disk staging, multiple streaming is enabled by default. If you:
 - Did not license the Enterprise Module, you can specify up to two simultaneous streams.
 - Licensed the Enterprise Module, you can specify up to 32 simultaneous streams.
7. If the file system device supports SnapLock, and you want to WORM-protect the backed up data, click the **Enable SnapLock** option.
8. Click **OK**.

After you complete these steps, the newly created file system device group appears in the Groups directory tree on the staging tab.

Note: Device groups identified as staging device groups do not appear in the Destination tab of the Backup Manager.

More information:

[How to Configure the Disk to Disk to Tape Option to Perform Disk Staging Backups](#) (see page 200)

[Configure Device Groups to Use Staging](#) (see page 201)

Specify Copy and Purge Policies for Disk Staging Backups

After CA ARCserve Backup completes the backup to disk phase, copy policies let you specify when to copy the data to its final destination media.

The following information describes how to set policies for Full and Differential/Incremental backups to a file system device or a deduplication device (B2D2T). For information about how to set policies for Full and Incremental/Differential backup policies to a library or virtual library, see [How to Configure the Disk to Disk to Tape Option to Perform Tape Staging Backups](#) (see page 227).

Note: The copy and purge policies specified for disk staging backups apply to file system devices and deduplication devices.

To specify copy and purge policies for disk staging backups

1. Open the Backup Manager and select the **Staging** tab.

Browse to and select the staging group that you want to configure and click the **Policy** button.

The **Disk Staging Policy** dialog or the **Deduplication Staging Policy** dialog opens.

Note: Click the **Full Backup** tab to set policies for full backup jobs or select the **Differential/Incremental Backup** tab to set policies for differential and incremental backup jobs.

2. From the **Full Backup** tab or the **Differential/Incremental Backup** tab, specify the following **Copy Policies**, as required, for the job:
 - **Do not copy data option**--Choose this option if you do not want to copy the backup sessions to final destination media. For example, consider differential and incremental backup operations. Operations of this type tend to have short retention periods and are small with respect to overall size. If you do not copy the incremental and differential backups to final destination media, the need for tapes to store your backups diminishes.

- Copy data **After** option--Choose this option to direct CA ARCserve Backup to start the copy from disk to final destination media operation after specified length of time elapses. CA ARCserve Backup starts the copy to media operation based upon the occurrence of one of the following events:

- **After job starts option**--Choose this option if you want to start the copy to media operation at a fixed point in time after the backup to disk operation starts.
- **After job ends option**--Choose this option if you want to start the copy to media operation after the backup to disk operation ends.

Due to variations in the overall size of backup jobs and the length of time needed to complete backup to disk operations, simultaneous read and write operations to the disk staging device can occur. This option prevents simultaneous read and write operations to disk staging devices.

- **After each session is finished option**--Choose this option if you want to start the copy to media operation immediately after the backup to disk operation for the session is complete.

Most backup jobs consist of several sessions. When you specify this option, you can direct CA ARCserve Backup to copy backup sessions to their final destination immediately after the backup job is finished. This option manifests simultaneous backup and copy operations. By performing backup and copy operations simultaneously, you can reduce the overall backup window and copy window.

Because this option induces simultaneous read and write operations on the FSD, you should only specify this option if you are using a high-speed device that can process many read and write operations simultaneously.

Note: For all Copy data after options, CA ARCserve Backup will not migrate sessions to their final destination media until after the backup job for the session is complete. This capability includes scenarios when the copy retention period expires before the backup operation is complete.

- Copy data **At** Option--Choose this option to direct CA ARCserve Backup to start the copy to media operation at a specific time of day. When you use this option you can direct CA ARCserve Backup to start the migration process at a specific time on a daily basis.
 - Select the Or after the job is finished whichever happens later option if you suspect or anticipate the backup to disk operation to end after the specified start time for the copy to final destination operation. This option prevents CA ARCserve Backup from copying sessions from disk to tape while the backup operation is in progress.
 - **Copy data for monthly backups only**--Choose this option if you want the monthly full backup jobs to be migrated but not the weekly full backup jobs. No migration job is generated for sessions backed up by the weekly full backup job.
- Important!** This option only affects GFS rotation jobs.
3. From the **Full Backup** tab or the **Differential/Incremental Backup** tab, specify the following **Purge Policies**, as required, for the job:
 - Purge data **After** option--Choose this option to direct CA ARCserve Backup to start the purge operation after specified length of time elapses. CA ARCserve Backup starts the purge operation based upon the occurrence of one of the following events:
 - **After job starts option**--Choose this option to direct CA ARCserve Backup to start the purge data from disk operation at a specified time after the backup to staging device operation starts.
 - **After job ends option**--Choose this option to direct CA ARCserve Backup to start the purge data from disk operation at a specified time after the backup to staging device operation ends.
 - Purge data **At** option—Choose this option to direct CA ARCserve Backup to start the purge data from disk operation at a specific time of day. Use the spin box to specify the time of day that you want the operation to start.
 4. If you want to enable SnapLock protection, click the **Enable SnapLock** check box.

Note: To use this option, the device must support SnapLock protection. If you select this option and the device does not support SnapLock protection, the files are stored on the FSD in a read-only state.

Specify Miscellaneous Options for Disk Staging Backups

To perform disk to disk to tape (B2D2T) backups, you can optionally specify policies that control how CA ARCserve Backup processes backup job data.

Note: The miscellaneous options specified for disk staging backups apply to file system devices and deduplication devices.

To specify miscellaneous options for disk staging backups

1. Open the Backup Manager and select the Staging tab.

Browse to and select the staging group that you want to configure and click Policy.

The Disk Staging Policy dialog or the Deduplication Staging Policy dialog opens.

2. Click the Miscellaneous tab and specify the options that follow that you require for the job:

Miscellaneous Options

- **Purge canceled sessions from disk immediately**--Use this option to direct CA ARCserve Backup to delete sessions from the staging device immediately after a backup to staging device is canceled.

This option helps to reclaim free disk space on the staging device as quickly as possible.

- **Purge failed sessions from disk immediately**--Use this option to direct CA ARCserve Backup to delete sessions from the staging device immediately after a backup to disk staging device fails.

This option helps to reclaim free disk space on the staging device as quickly as possible.

- **Create makeup jobs to back up data directly to final destination under disk full conditions**--Use this option to direct CA ARCserve Backup to back up data directly to its final destination media if there is insufficient free space on the file system device in a staging group.

A backup operation will fail if there is insufficient free disk space on the staging device. To remedy this situation, CA ARCserve Backup can divert the backup operation from the file system device in a staging group directly to the final destination media. A makeup job searches for blank media and media from a scratch. As such, specifying this option can increase the overall success rate of your backup operations when a "disk full" condition exists.

- **Schedule makeup jobs for failed data migration jobs**--Use this option to direct CA ARCserve Backup to create makeup jobs on HOLD if data migration (copy to tape) jobs fail.

A data migration job can fail if a media or tape drive error occurs during the copy to tape operation. Use this option to create a makeup job with a HOLD status that you can change to a Ready status after correcting the tape drive or media errors. If an error condition exists, this option minimizes the need to create tapecopy jobs.

Consolidate Data Across Jobs While Copying Options

Lets you consolidate backup data during the migration operation.

- **Copy Method**--Specify a copy method (Append or Overwrite) that you want to use for the consolidation operation. The method that you specify must be the same for all jobs that you want to consolidate.
 - If you have a requirement to consolidate data across multiple jobs and ship the tapes on a daily basis, you should choose the Overwrite option.
 - If you have a requirement to consolidate data across multiple jobs (for daily backups) for the whole week to a single tape and ship the tapes on a weekly basis, you should choose the Append option.
- **Limitations and Considerations**
 - To use consolidation, ensure that the Disk to Disk to Tape Option is licensed.
 - To consolidate data across multiple jobs to the same tape, you should run the backup jobs on the same machine.
 - If the backup is a rotation or a GFS backup, you must specify the prefix of the target media and the prefix of the media pool that you want to use for consolidation on the Destination tab. The screen that follows illustrates the fields that you must complete:



Note: For more information about consolidation options and examples, see [Consolidation During Migration](#) (see page 397).

3. Click OK.

Specify Alert Options for Disk and Tape Staging Backups

CA ARCserve Backup lets you use the alert notification system to send messages about migration events that occur during the course of staging operations. For more information about setting up alerts, see [Using the Alert Manager](#).

Note: The alert options specified for disk staging backups apply to file system devices and deduplication devices.

To specify alert options

1. Open the Backup Manager and click the **Staging** tab.

From the **Staging Groups** tree, select the group for which you want to specify alerts.

Check the **Enable staging** check box, if it is not checked.

Click the **Policy** button.

The **Disk Staging Policy**, **Deduplication Staging Policy**, or **Tape Staging Policy** dialog opens.

2. Click the **Alert** tab.

The Alert options display.

3. From the **Event** list, select one of the following migration events for which you want to send an alert notification:

- **Migration job complete**--All sessions in the current migration job migrated successfully.

Example:

A backup job can consist of one or multiple migration jobs. This event will occur after each individual migration job is complete.

- **Migration job incomplete**--One or more sessions in a migration job did not complete successfully.

Example:

A session was skipped during the migration job. You can configure Alert to send an email to a system administrator with instructions to investigate the problem.

- **Migration job canceled**--A migration job was canceled by a user while it was in an Active, Ready, or Hold status. A makeup job was not created.

- **Migration job failed**--One or more sessions in a migration job failed.

- **Makeup of migration job created**--A migration job failed and CA ARCserve Backup created a makeup job.

- **All sessions migrated**--All sessions corresponding with a staging job migrated successfully.

Example:

A backup job consists of multiple migration jobs. The migration jobs consist of several sessions each. All sessions in all of the migration jobs for the backup job migrated successfully. To ensure that the media is not overwritten, you can configure Alert to send a pager message to a librarian to eject the media from the library after the copy phase is complete.

4. From the **Methods & Recipients** field, you can accept the default options, or create a custom alert for the event. The <Default> configuration means that you will use the alert options configured using the Alert Manager.

To create custom alerts, click the **Configure** button.

The **Methods & Recipients Configuration** dialog opens. You can specify one or more of the defined alert configurations. CA ARCserve Backup provides the following defined alert configurations:

- Broadcast
- Pager
- SMTP
- SNMP
- Event
- Printer
- Email
- Lotus Notes
- Unicenter NSM

Note: Pager options are not supported on Japanese versions of CA ARCserve Backup.

5. To add a new Methods & Recipients configuration, click the **New** button.

The **Configuration Name** dialog opens. Specify a name for the configuration and click **OK**.

A new configuration tree displays in the browser at the left of the dialog. The new configuration tree contains one branch for all available notification methods. You must now add recipients to the methods branches of your tree. For example, if you want to use the **Printer** notification method, you must add an available printer to the tree.

6. To add a recipient to a configuration, you must first select a method (for example, Broadcast) from the configuration tree and then click the **Add** button.

The appropriate Add Recipient dialog opens for the selected configuration. Configure the new recipient in this dialog. For more information about the different Recipient dialogs, click the **Help** button.

After you configure the new recipient, it is added to the tree.

Note: You can not add recipients for the Unicenter TNG alerts. If you click on Modify, the Unicenter TNG Event Map dialog opens. You can then have messages sent to the Unicenter console or the World View repository when an alert is generated.

7. To modify a Methods & Recipients configuration, select the configuration from the **Configuration** drop-down list.

The selected Configuration tree displays in the browser. You can add, modify, or delete recipients from the configuration tree by clicking the **Add**, **Modify**, or **Delete** button.

To delete a configuration, select the configuration from the **Configuration** drop down list and click the **Delete** button.

To rename a configuration, select the configuration from the **Configuration** drop down list, and click the **Rename** button.

8. Click **OK**.

The alert options are applied and the Staging Policies or Tape Staging Policies dialog closes.

Specify Postscripts Options for Disk and Tape Staging Backups

CA ARCserve Backup lets you specify postscripts that run based on particular migration events that occur during the course of staging operations.

A script is a set of instructions that are stored in user-defined files that can be created in any format, such as .bat and .exe. Scripts can be executed before or after an event occurs. A postscript is a set of instructions that you can run or execute after an event occurs, such a migration event. Postscripts are not limited to CA ARCserve Backup-based scripts.

Note: The postscript options specified for disk staging backups apply to file system devices and deduplication devices.

To specify postscripts options

1. Open the Backup Manager and click the **Staging** tab.

From the **Staging Groups** tree, select the group for which you want to specify postscripts options.

Check the **Enable staging** check box, if it is not already checked.

Click the **Policy** button.

The **Disk Staging Policy**, **Deduplication Staging Policy**, or **Tape Staging Policy** dialog opens.

2. Click the **Postscripts** tab.

The Postscripts options display.

3. From the **Event** list, select one of the following migration events for which you want to run a postscript:

- **Migration job complete**--All sessions in the current migration job migrated successfully.

Example:

A backup job can consist of one or multiple migration jobs. This event will occur after each individual migration job is complete.

- **Migration job incomplete**--One or more sessions in a migration job did not complete successfully. For example, a session was skipped during the migration job.
- **Migration job canceled**--A migration job was canceled by a user while it was in an Active, Ready, or Hold status. A makeup job was not created.
- **Migration job failed**--One or more sessions in a migration job failed.
- **Makeup of migration job created**--A migration job failed and CA ARCserve Backup created a makeup job.
- **All sessions migrated**--All sessions corresponding with a staging job migrated successfully.

Example:

A backup job consists of multiple migration jobs. The migration jobs consist of several sessions. This event will occur when all sessions in all migration jobs for the backup job migrated successfully.

4. Click in the **Postscripts** field adjacent to the selected event and do one of the following:

- Enter the path to script that you want to run after the event occurs.
- Click the ellipsis button  to browse to the script that you want to run after the event occurs.

Note: You can specify one postscript per migration event.

5. From the **Run As** section, complete the following fields:

- User name
- Password
- Confirm password

Note: You must provide Windows credentials to run postscripts.

6. Repeat Steps 3, 4, and 5 to specify postscripts for other migration events.
7. Click **OK**.

The postscripts options are applied and the Staging Policies or Tape Staging Policies dialog closes.

How to Submit a Disk Staging Backup Job

The following sections provide you with information about how to submit a disk staging backup job.

More information:

[Options You Can Specify on the Backup Manager Destination Tab](#) (see page 136)

Licensing Requirements for Staging Backups

To successfully submit a disk staging backup job, ensure that the following licensing requirements are fulfilled.

- To be able to utilize the full capabilities of CA ARCserve Backup B2D2T backups, you must license the CA ARCserve Backup Enterprise Module.
For example, if you do not license the module, you cannot consolidate data from different jobs to one tape when you are copying data to final destination media.
- You must license the CA ARCserve Backup Enterprise Module to enable the following functions:
 - Encrypt data during the migration phase of a backup job.
 - Enable the use of more than one stream of data when you use multistreaming to process backup data.
 - Enable the use of more than four streams of data when you use multiplexing to process backup data.
- You must license the CA ARCserve Backup Tape Library Option to back up data to a tape library that contains more than one tape drive.

Back Up Data Using Disk Staging

Prior to performing a backup job using the disk staging (B2D2T), you must have already configured the staging groups. If you did not configure CA ARCserve Backup to use the Disk to Disk to Tape Option, see [How to Configure the Disk to Disk to Tape Option to Perform Disk Staging Backups](#) (see page 200).

CA ARCserve Backup provides you with the capability to submit a backup job using either the Backup Manager or the command line utility. This information describes how to perform a disk staging backup job using the Backup Manager. For information about how to submit a staging backup job using the command line, see the *Command Line Reference Guide*.

Note: Before you can back up data using disk staging, ensure that all preconfiguration tasks are complete and licensing requirements are fulfilled. For more information, see [Licensing Requirements for Staging Backups](#) (see page 215).

Back up data using disk staging

1. Open the Backup Manager, click the Source tab, browse to and select the source objects that you want to back up.

2. Click the Staging tab and expand the Staging Servers object.

Browse to and select the staging group that you want to use for the backup job. If you wish to enable deduplication, choose a deduplication device group from the Staging tab.

Check the Enable staging check box and click the Policy button.

The Disk Staging Policy dialog opens.

3. Click the Full Backup tab and specify the Copy and Purge policies for full backups required for the job.

Click the Incremental/Differential Backup tab and specify the Copy and Purge policies for incremental and differential backups required for the job.

For more information, see [Specify Copy and Purge Policies for Disk Staging Backups](#) (see page 205).

Click the Miscellaneous tab and specify the Miscellaneous policies required for the backup job. For more information, see [Specify Miscellaneous Options for Disk Staging Backups](#) (see page 208).

Click the Alert tab and specify the Alert policies required for the backup job. For more information, see [Specify Alert Options for Disk and Tape Staging Backups](#) (see page 210).

Click the Postscripts tab and specify the Postscript policies required for the job. For more information, see [Specify Postscripts Options for Disk and Tape Staging Backups](#) (see page 213).

Click OK.

The Disk Staging Policy dialog closes and the policies specified for the job are applied.

- To use multistreaming, check the Multistreaming check box. To modify the number of simultaneous streams during the backup operation, use the spin box to change the Max # Streams.

Note: Disk to disk to tape is no longer a separately-licensed option. It is now part of the Enterprise Module. You can still perform disk to disk to tape backups without licensing the Enterprise Module, however, the maximum number of streams for such jobs is two. To submit more than two streams in disk to disk to tape backups, you must license the Enterprise Module.

- Click the Destination tab and expand the Servers object.

Browse to and select the destination device you want to use for the backup job. If desired, you may choose a deduplication device group as the final destination provided it is not the same deduplication device group selected as the staging group.

- Click the Schedule tab and specify the schedule that you want to use for the backup job.
- Click the Options toolbar button.

The Options dialog opens.

- Select the Encryption/Compression tab and complete the following fields for the backup job, provided you are not using deduplication devices:

- **Session/Encryption password**--Specify a Session/encryption password to restore this data from media.

Important! If you specify a Session/Encryption password, you must provide this password to restore the session.

- **Encrypt data**--Use this option to encrypt the backup data. You can specify one of the following options:
 - **At agent**--Select this option to encrypt the backup data prior to the actual backup process. For more information about this option, see [Data Encryption at the Agent Server](#) (see page 104).
 - **At backup server during backup**--Select this option to encrypt the backup data at the backup server during the backup process. For more information, see [Data Encryption During Backup](#) (see page 106).
 - **At backup server during migration**--Select this option to encrypt the backup data during the migration phase of a staging backup job. For more information, see [Data Encryption During Migration](#) (see page 107).

- **Compress data**--Use this option to compress the backup data. You can specify one of the following options:
 - **At agent**--Select this option to compress the backup data on the system where the agent is installed and running.
 - **At backup server**--Select this option to compress the backup data at the CA ARCserve Backup server during the backup process. Using this option directs CA ARCserve Backup to compress files before backing them up using a software compression algorithm.

Note: When you use data compression at the backup server before data encryption, the amount of space required to store the data on the staging device can be two times the size of the source files. Because of this limitation, we discourage the use of compression before encryption when backing up to disk.

Click OK.

The Options dialog closes and the specified encryption and compression options are applied.

Be aware of the following:

- If you want to apply other options that affect the migration job, you should do so at this time. For example, to eject the tape from a library after the migration job is complete, click the Operation tab on the Global Options dialog and select the Eject Media option.
- If you specify encryption and compression options, and the backup destination is a drive that does not support compression, or is a file system device (FSD), CA ARCserve Backup encrypts the backup data and does not compress the backup data.
- Encryption and compression are not supported on deduplication devices. However, if you select a regular FSD for either the staging or final destinations, you may enable encryption or compression, as needed. For more information, see the topic, [Compression and Encryption with Deduplication](#) (see page 687).

9. Click Start on the toolbar to submit the backup job.

More information:

[Submit a Backup Job](#) (see page 129)

[Modify Pending Data Migration Jobs](#) (see page 299)

Modify a Staging Rotation Scheme

If you are using rotation or GFS rotation disk staging jobs, CA ARCserve Backup provides you with the flexibility to disable staging on any specified day of the week.

To modify staging when using a rotation scheme

1. Open the Backup Manager and select the Schedule tab.
2. Select the Use Rotation Scheme option, and then select the scheme name from the Scheme Name drop-down list.
3. Click the Rotation Rules tab.

The Staging column displays the current status of staging as it applies to your rotation scheme.

4. Select the Day Of Week for which you want to modify staging, and then click the Modify button.

The Configuration dialog opens.

5. From the Staging drop-down list, select Enable or Disabled.
6. Click OK.

Note: To disable staging for a staging group, see [Disable Staging](#) (see page 220).

More information:

[Modify Pending Data Migration Jobs](#) (see page 299)

Pause Data Migration

The Pause Data Migration option lets you temporarily stop the process of migrating data from the FSD to its final destination media.

Example

You need to take a tape library offline to perform maintenance on the library. You can pause the data migration process, complete the maintenance tasks, bring the library back online, and then restart the migration process.

To pause data migration

1. From the **Staging Groups** tree on the **Staging** tab, select the group that you want to pause.
2. Do one of the following:
 - Right-click the group name and select **Configure File System Device Groups** from the pop-up menu.
 - Click the **Configure Staging Group** option in the Properties view.

The **Staging Group Configuration Dialog** opens.

3. Check the **Pause Data Migration** option and click **OK**.

Note: To restart the data migration operation, repeat Steps 1 and 2, then clear the checkmark from the Pause data migration check box and click OK.

Disabling Disk Staging Rotations

When you back up data using regular or GFS rotation rules, CA ARCserve Backup provides you with the capability to suspend or disable staging in the backup jobs on any specified day of the week, bypassing the FSD, and backing up your data directly to its final destination media.

Example: When You Should Disable a Staging Backup Job

If you discover that your FSD in a staging group is approaching or has exceeded its storage capacity threshold, backup jobs can fail. You can modify the staging job to disable staging on that day so that the data is backed directly to the final destination.

To verify whether staging for rotation and GFS rotations is disabled or enabled, open the Backup Manager, select the Schedule tab, and select the Rotation Rules tab. The Staging column in the Rotation Rules schedule displays the current status of all rotations and GFS rotations. To modify a rotation rule, click the Modify button below the schedule.

Disable Staging

CA ARCserve Backup provides you with the capability to disable (or bypass) backup to FSD operations. When you use this option, data is backed up directly to its final destination media, rather than being backed up to the FSD.

There are two methods that you can use to perform this task:

- From the Rotation Rules tab on the Schedule tab of the Backup Manager.
- Using File System Device Group Configuration.

Backup Manager - Schedule Tab

To disable backup to staging device operations from the Backup Manager, perform the following steps:

1. Open the Backup Manager window and click the **Schedule** tab.
2. Select the **Scheme Name** from the drop-down list.
3. Click the **Rotation Rules** tab and select the rotation that you want to disable.
4. Click the **Modify** button.

The **Configuration** dialog opens.

5. From the **Staging** drop-down list on the **Configuration** dialog, select **Disabled**.
6. Click OK.

File System Device Group Configuration Dialog

To disable back up to staging device group operations using Device Group Configuration:

1. Open the Backup Manager window and click the **Staging** tab.
2. Right-click the group that you want to disable and select **Configure File System Device Groups** from the pop-up menu.

The **File System Device Group Configuration** dialog opens, displaying all groups in your environment that are specified as file system device groups.

Note: The groups that are enabled for staging display with a corresponding dark blue flag. The groups that are not enabled for staging display with a corresponding light blue flag.

3. Select the group that you want to disable.
4. Clear the check mark from the **Enable Staging** check box.
5. Click **OK**.

How You Can Manage Staged Data When the Database Fails

When you use the Disk to Disk to Tape Option to back up data, the information about the backup jobs, sessions, staging policies, and so on is stored in the CA ARCserve Backup database. If the database fails, and you need to recover the CA ARCserve Backup database, the staging policies for the data residing on the staging device (for example, a file system device or a library) that specify when to copy the data to the final destination media and, if file system device (FSD), when to purge the data from the staging device are no longer available.

If this situation occurs:

- CA ARCserve Backup cannot copy (migrate) the data on staging device to its final destination media.
- CA ARCserve Backup cannot purge data from a file system device (FSD) to reclaim disk space. As a result, future backup jobs will probably fail due to an insufficient amount free disk space on the staging device.

To remedy this situation and retain all of the backup data that is stored on the staging device, you can use the `tapecopy` command line utility to copy all the backup data from the staging device to final destination media. (When you use this approach, media rotation rules, such as Friday tape or Monday tape may not be adhered to.) Then, you can use the `-purge` option from the Device Manager command line utility (`ca_devmgr`) to delete the data from the FSD and reclaim disk space.

How to Reclaim Disk Space

This section provides examples of how you can quickly reclaim disk space using the **Purge Data At** and **Purge Data After** options.

Example 1

You have a high-performance disk with a limited amount free disk space. You can quickly reclaim disk space by specifying a short length of time under the Purge data After option and select the After job starts option. This approach ensures that the purge operation starts shortly after the copy to final destination media operation starts, as opposed to the using the After job ends option, which starts the purge operation after the copy to final destination media operation ends.

Example 2

You have a backup job rotation or a GFS rotation scheme that starts at the same time daily and your high-performance disk maintains a limited amount of unused space. Using the Purge data At option to schedule the purge operation to start before the next backup operation starts. This approach helps to ensure that you have freed enough disk space to prevent the backup job from failing.

Important! If you specify that the data is to be copied to final destination media, CA ARCserve Backup does not start the purge operation until after the copy to final destination media operation is finished.

More information:

[Modify Pending Data Migration Jobs](#) (see page 299)

How to Manage Backup Data Using Tape Staging

The following sections provide information about how to protect data using backup to tape to tape operations.

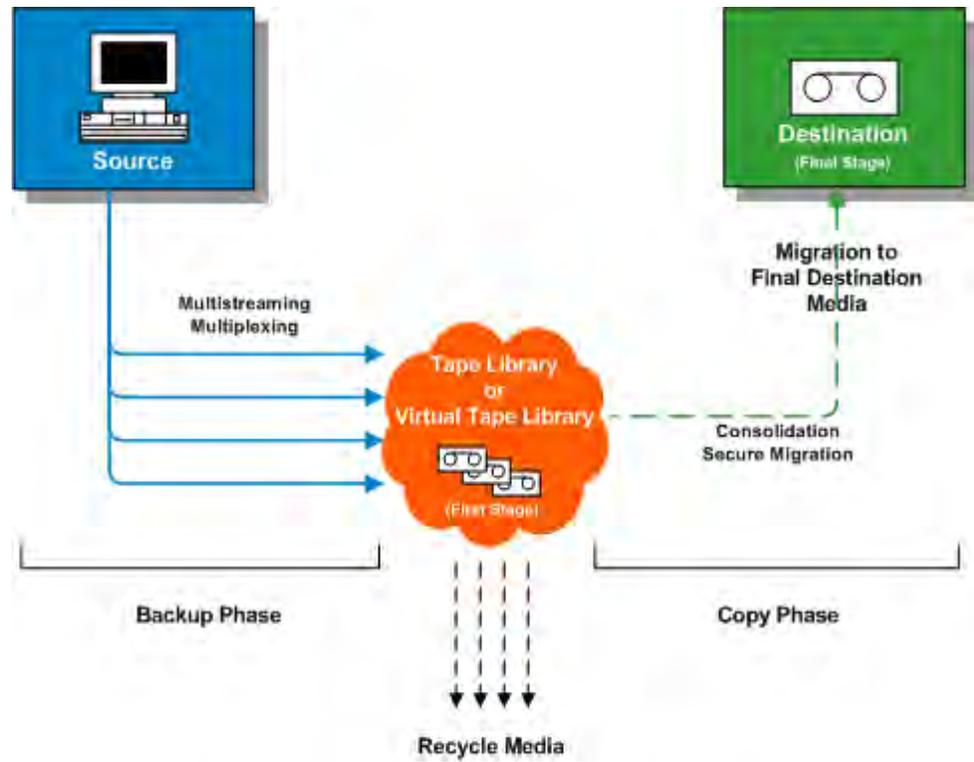
More information:

[How to Manage Backup Data Using Staging](#) (see page 196)

How Backup to Tape to Tape Works

CA ARCserve Backup lets you to back up data to a tape library or a virtual tape library, and then copy the data to a different tape library or other type of device. Copy operations, also known as migration, are governed by user-specified copy policies.

The following diagram illustrates the flow of data from the source to the first stage tape library (or virtual tape library) and then on to the final destination.



When you use backup to tape to tape (B2T2T) to protect data, the backup to tape to tape operation consists of two phases:

Backup Phase

CA ARCserve Backup backs up data from the source to the tapes in the first stage, based on user-specified policies.

- Backup jobs can consist of full, incremental, or differential backups.
- During the backup job, global options, media selection rules, media pool usage, rotation rules, GFS rotation rules, Alert messages, Export options, and so on are identical to that of backing up directly to tape.

Note: Various global backup options do not apply to backup phase operations.

- Multiplexing and multistreaming can be used to transmit and save data to first stage media.

Note: The Multiplexing option can be used for backup operations to all tape devices, with the exception of file system devices. The Multistreaming option can be used for backup operations to tape libraries that contain two or more drives.

Copy Phase

CA ARCserve Backup copies data from the first stage to the final destination based on user-specified policies.

- CA ARCserve Backup copies data from the first stage media to the final destination media one session at a time. Multiple sessions cannot be copied to a single tape simultaneously.
- If you need to copy data from more than one first stage media to one final destination media, CA ARCserve Backup copies each session in succession until all the sessions are copied to the final destination media.
- CA ARCserve Backup sessions associated with different jobs can be consolidated during migration. You can activate this capability using the consolidation option.
- If a hardware error occurs during the process of copying data to final destination, the job stops and CA ARCserve Backup creates a **Makeup Job On Hold**. After you correct the hardware error, you can status the job to **Ready**, and the job resumes.

How to Use Tape Staging to Manage Backup Operations

The following are common scenarios that describe how you can use Backup to Tape to Tape operations (B2T2T) to manage backup operations:

- If you need to store two copies of backup data, one copy on site and one copy at an off-site storage location, B2T2T lets you back up data directly to tape. After the backup job is complete, you can use CA ARCserve Backup copy utilities to automate and create copies of the backup tapes, and then ship the tapes to an off-site storage location.
- B2T2T lets you encrypt backup data when you are copying the data to its final destination media. This capability is beneficial when you are copying data from a virtual tape library or a library that does not support encryption to a library that supports encryption. This capability ensures that your backups are as fast as possible and the tapes that you need ship to an off-site storage location are encrypted.
- While backup operations are in progress, you may have many jobs that are backing up data to many different tapes. This can result in media that is not being used to its full capacity. B2T2T operations let you consolidate backups to ensure that media is being used to capacity when copying data to final destination. This capability helps to reduce the cost of media because you are using fewer tapes for final destination media, off-site storage, or both.
- If you need to reduce the length of time required to back up data and copy the data from a staging area to final destination, you can use virtual tape libraries (VTL) in your environment to manage backup operations.

A VTL is a temporary storage location, such as a disk drive, that is configured to behave like a library. Since most backup data is transmitted across a network, CA ARCserve Backup lets you use multiplexing to reduce the backup window. When you use a VTL to store backup data, you can quickly read data from a multiplexing formatted data in a VTL because your operations do not encounter tape positioning overhead. As a result, the processes of backing up data to a VTL, reading from a VTL (disk), and copying the data to final destination media is fast. CA ARCserve Backup lets you automate the process of copying to final destination media when you use a VTL to stage your backup data.

How to Configure the Disk to Disk to Tape Option to Perform Tape Staging Backups

Before you can back up data using the Disk to Disk to Tape Option, you must perform the following tasks:

- Create the staging devices.

If you plan to use a virtual library, open the Device Manager to confirm the the library is properly configured. CA ARCserve Backup automatically configures libraries when you stop and restart the Tape Engine. If a library is not properly configured, you can run Device Configuration to manually set up libraries and virtual libraries for staging operations.

Note: For more information about using Device Configuration to set up libraries and virtual libraries, see [Tape Library Configuration](#) (see page 329).

- Specify device groups as staging groups.
- Configure staging policies.

Note: To perform backup operations using staging, you must define the migration policies that CA ARCserve Backup will use to manage data stored on staging devices. For more information, see [Back Up Data Using Tape Staging](#) (see page 230).

More information:

[Specify Alert Options for Disk and Tape Staging Backups](#) (see page 210)

[Specify Postscripts Options for Disk and Tape Staging Backups](#) (see page 213)

[Specify Migration Policies for Tape Staging Backups](#) (see page 227)

[Specify Miscellaneous Options for Tape Staging Backups](#) (see page 228)

Specify Migration Policies for Tape Staging Backups

Copy policies let you specify when to copy backup data to its final destination media after CA ARCserve Backup completes the backup to a tape staging device (for example, a library, a virtual library, a tape drive, an FSD, and so on).

The following information describes how to set policies for Full and Differential/Incremental backups for tape staging devices.

To specify migration policies for tape staging backups

1. Open the Backup Manager and select the Staging tab.

Browse to and select the staging group that you want to configure, check the Enable staging check box, and then click the Policy button.

The Tape Staging Policy dialog opens.

Note: Click the Full Backup tab to set the migration policies for full backup jobs or select the Differential/Incremental Backup tab to set migration policies for differential and incremental backup jobs.

2. Specify when you want to copy the backup data to final destination media by doing one of the following:

- Click the Do not copy data option if you do not want to copy the backup data from the staging location to final destination media

Note: If you select this option, you can skip to the next step.

Specify the number of Weeks, Days, Hours, and Minutes that must elapse before migration operation starts.

3. Click the Copy data for monthly backups only option to copy only the monthly full backups in a GFS rotation to final destination media.

With this option specified, CA ARCserve Backup will not migrate the weekly full backups and the first full backup in the GFS rotation to final destination media.

Note: If you specify a GFS rotation, CA ARCserve Backup considers the last weekly full backup in a GFS rotation job a monthly backup. For more information, see [Rotation Schemes](#) (see page 287).

Specify Miscellaneous Options for Tape Staging Backups

To perform tape staging backup operations, you can optionally specify policies that control how CA ARCserve Backup processes backup job data.

To specify miscellaneous options for tape staging backups

1. From the **Backup Manager** window, select the **Staging** tab, and select a **Tape Staging** group.

Note: A library is distinguished by .

Check the **Enable staging** check box and then click the **Policy** button.

The **Tape Staging** dialog opens.

2. Click the **Misc** (Miscellaneous) tab and specify any or all of the following miscellaneous options:

- **Create a makeup job on hold if a data migration job fails**--Use this option to direct CA ARCserve Backup to create makeup jobs on HOLD if data migration (copy to tape) jobs fail.

A data migration job can fail if a media or tape drive error occurs during the copy to tape operation. Use this option to create a makeup job with a HOLD status that you can change to a READY status after correcting the tape drive or media errors. If an error condition exists, this option minimizes the needs to create tapecopy jobs.

- **Schedule a makeup job for a data migration job if it cannot proceed because the source group or tape is not available**--Use this option to direct CA ARCserve Backup to schedule a makeup job when the source group or tape is not available.

The source may not be available do to a variety of reasons. For example, the backup phase for the job is not complete, or a hardware problem exists in the tape library or virtual tape library.

- **Reschedule after**--Specify how many minutes must elapse before the makeup will be rescheduled.

3. To consolidate the backup data during the migration operation, click the **Consolidate data across jobs while copying** option and complete the following fields.

Note: If you want to consolidate data across multiple jobs to the same tape, you should run the backup jobs on the same machine.

Important! To use Consolidation, ensure that the Disk to Disk to Tape Option is properly licensed.

- **Copy Method**--Specify a copy method (Append or Overwrite) that you want to use for the consolidation operation.

The method that you specify must be the same for all jobs that you want to consolidate.

- If you have a requirement to consolidate data across multiple jobs and ship the tapes on a daily basis, you should choose the "Overwrite" option.
- If you have a requirement to consolidate data across multiple jobs (for daily backups) for the whole week to a single tape and ship the tapes on a weekly basis, you should choose the "Append" option.

Note: For more information about consolidation options and examples, see [Consolidation During Migration](#) (see page 397).

How to Submit a Tape Staging Backup Job

The following sections provide you with information about how to submit a tape staging backup job.

More information:

[Options You Can Specify on the Backup Manager Destination Tab](#) (see page 136)

Licensing Requirements for Tape Staging Backups

To perform successful backup to tape to tape backup (B2T2T) operations, ensure that the following licensing requirements are fulfilled.

- To be able utilize the full capabilities of CA ARCserve Backup B2T2T backups, you must license the CA ARCserve Backup Enterprise Module.
For example, if you do not license the module, you cannot consolidate data from different jobs to one tape when you are copying data to final destination media.
- You must license the CA ARCserve Backup Enterprise Module to enable the following functions:
 - Encrypt data during the migration phase of a backup job.
 - Enable the use of more than one stream of data when you use multistreaming to process backup data.
 - Enable the use of more than four streams of data when you use multiplexing to process backup data.
- You must license the CA ARCserve Backup Tape Library Option to back up data to a tape library that contains more than one tape drive.

Back Up Data Using Tape Staging

Prior to performing a backup job using tape staging (B2T2T), you must have already configured the staging groups. For more information, see [How to Configure the Disk to Disk to Tape Option to Perform Tape Staging Backups](#) (see page 227).

CA ARCserve Backup provides you with the capability to submit a backup job using either the Backup Manager or the command line utility. This information describes how to perform a tape staging backup job using the Backup Manager. For information about how to submit a staging backup job using the command line, see the *Command Line Reference Guide*.

Note: Before you can back up data using tape staging, ensure that all preconfiguration tasks are complete and all licensing requirements are fulfilled. For more information, see [Licensing Requirements for Staging Backups](#) (see page 215).

Back up data using tape staging

1. Open the Backup Manager, click the Source tab, browse to and select the source objects that you want to back up.

2. Click the Staging tab and expand the Staging Servers object.

Browse to and select the Staging group that you want to use for the backup job.

Check the Enable staging check box and click the Policy button.

The Tape Staging Policy dialog opens.

3. Click the Full Backup tab and specify the Migration policies for full backups required for the job.

Click the Incremental/Differential Backup tab and specify the Migration policies for incremental and differential backups required for the job.

Note: For more information see [Specify Migration Policies for Tape Staging Backups](#) (see page 227).

Click the Misc (Miscellaneous) tab and specify the Miscellaneous policies required for the backup job.

Note: For more information, see [Specify Miscellaneous Options for Tape Staging Backups](#) (see page 228).

Click the Alert tab and specify the Alert policies required for the backup job.

Note: For more information, see [Specify Alert Options for Disk and Tape Staging Backups](#) (see page 210).

Click the Postscripts tab and specify the Postscript policies required for the job.

Note: For more information, see [Specify Postscripts Options for Disk and Tape Staging Backups](#) (see page 213).

Click **OK**.

The Tape Staging Policy dialog closes and the policies specified for the job are applied.

4. Click the Destination tab.

Specify the final destination device group for the job by doing one of the following:

- If the staging device contains two or more drives, you can select any device group on the Destination tab.

Example: You are required to stage your backup data to a virtual tape library and ship the final media to an off-site storage facility. To manage a backup of this type, you can specify a group that corresponds with a virtual library on the Staging tab, and then specify a group that corresponds with a tape library on the Destination tab.

- If the final destination device contains one drive (for example, an FSD or a single-drive library), you must select a device group on the Destination tab that is different from the device group specified on the Staging tab.

5. Click the Schedule tab and specify the schedule that you want to use for the backup job.

Note: For more information, see [Rotation Schemes](#) (see page 287) and [Custom Schedules](#) (see page 297).

6. To use multistreaming, check the Multistreaming check box. Use the spin box to change the Max # Streams.

Note: The CA ARCserve Backup base product lets you stream one job per available device or available library drive. You must license the CA ARCserve Backup Enterprise Module to use multistreaming to stream multiple jobs simultaneously to multiple devices and library drives. With the Enterprise Module, the multistreaming option lets you stream one job for each available device or library drive.

7. Click Options on the toolbar.

The Options dialog opens.

8. Select the Backup Media tab and complete the following fields, as required, for the backup job:

- **Session/Encryption password**--Specify a Session/encryption password to restore this data from media.

Important! If you specify a Session/Encryption password, you must provide this password to restore the session.

- **Encrypt data**--Use this option to encrypt the backup data. You can specify one of the following options:
 - **At agent**--Select this option to encrypt the backup data prior to the actual backup process. For more information about this option, see [Data Encryption at the Agent Server](#) (see page 104).
 - **At backup server during backup**--Select this option to encrypt the backup data at the backup server during the backup process. For more information, see [Data Encryption During Backup](#) (see page 106).
 - **At backup server during migration**--Select this option to encrypt the backup data during the migration phase of a staging backup job. For more information, see [Data Encryption During Migration](#) (see page 107).
- **Compress data**--Use this option to compress the backup data. You can specify one of the following options:
 - **At agent**--Select this option to compress the backup data on the system where the agent is installed and running.
 - **At backup server**--Select this option to compress the backup data at the CA ARCserve Backup server during the backup process. Using this option directs CA ARCserve Backup to compress files before backing them up using a software compression algorithm.

Click OK.

The Options dialog closes and the specified encryption and compression options are applied.

Be aware of the following:

- If you want to apply other options that affect the migration job, you should do so at this time. For example, to eject the tape from a library after the migration job is complete, click the Operation tab on the Global Options dialog and select the Eject Media option.
- If you specify encryption and compression options, and the backup destination is a drive that does not support compression, or is a file system device (FSD), CA ARCserve Backup encrypts the backup data and does not compress the backup data.

9. Click Start on the toolbar to submit the backup job.

More information:

[Submit a Backup Job](#) (see page 129)

[Modify Pending Data Migration Jobs](#) (see page 299)

Submit a Tape Staging Backup Job Using a Rotation Scheme

This section topic describes how to set up tape staging (D2T2T) backup jobs using a rotation or GFS rotation scheme. A rotation scheme lets you determine the type of backup (full, differential, and incremental), when to run a backup job, and where to save the backup data (media).

To submit a tape staging backup using a rotation scheme

1. Open the Backup Manager and select the Staging tab.
2. On the Staging tab, check the Enable staging option.

Specify the values that you require to submit the backup job in the following fields:

- Media Pool or Media pool (prefix)

Note: The name of the media pool or the media pool prefix that you specify in this field is the name (or prefix) of the media pool that you will use for the staging phase of the job.

- Group

3. Select the Schedule tab, and select the Use Rotation Scheme option.

A list of available schemes display in the Scheme Name drop-down list.

- From the Scheme Name drop-down list, select the scheme that you require for your backups.

From the Media Pool Used drop-down list, select the media pool or media pool prefix that you will use for the backup.

Note: The name of the media pool or media pool prefix that you specify in Media Pool Used drop-down list is the name (or prefix) of the media pool that you will use for the final destination media, without consolidation. If you specify use consolidation during migration, the name of the media pool or media pool prefix assigned on the Tape Staging policy dialog overwrites the value specified in the Media Pool Used field on the Schedule tab.

The following screen illustrates the Backup Manager window. The Schedule tab and the Rotation Rules tab are selected. The Scheme Name is 5-day weekly incremental backup, full backup on Friday.

The screenshot shows the Backup Manager window with the following configuration:

- Source | Staging | Destination | Schedule** (selected)
- Custom Schedule Use Rotation Scheme
- Scheme Name: <5-day weekly incremental backup, full backup on Friday> [Save as...] [Remove]
- Start date: 1/27/2009
- Execution Time: 4:28:55 PM
- Enable GFS Append Media
- Daily Backup Method:
 - Full
 - Incremental
 - Differential - Archive Bit
- Use WORM Media
 - Daily WORM
 - Weekly WORM
 - Monthly WORM
- Rotation Rules | Calendar View | Exceptions | Media** (selected)
 - Overwrite Append
 - Table:

Day of Week	Media Name	Method	Mode	Exec. Time	Staging
Sunday	SUNDAY	Off			
Monday	MONDAY	Incremental	Overwrite	<Default>	
Tuesday	TUESDAY	Incremental	Overwrite	<Default>	
Wednesday	WEDNESDAY	Incremental	Overwrite	<Default>	
Thursday	THURSDAY	Incremental	Overwrite	<Default>	
Friday	FRIDAY	Full	Overwrite	<Default>	
Saturday	SATURDAY	Off			
 - [Modify]

- Click Submit on the toolbar.
The Submit Job dialog opens.
- Complete the required fields on the Submit Job dialog and click OK.

Disaster Recovery

To ensure against data loss, maintain current backups of all your servers and workstations. If you do not have these backups, CA ARCserve Backup is limited in its ability to recover data. Be sure to create a media rotation scheme and a schedule to maintain current backups.

By default, the CA ARCserve Backup server always generates or updates disaster recovery information for all full backup systems, even when the CA ARCserve Backup Disaster Recovery Option is not installed. This ensures that the latest backup information is always available if the CA ARCserve Backup Disaster Recovery Option is installed a later time.

Note: To disable the CA ARCserve Backup server from generating or updating the disaster recovery information, create and set the following registry key value to 1 on the CA ARCserve Backup server machine:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Computer Associates\CA ARCserve  
Backup\Base\Task\backup\SkipDRSession
```

For more information, see the *Disaster Recovery Option Guide*.

Back Up BrightStor ARCserve Backup for Laptops & Desktops Data

If you use BrightStor ARCserve Backup for Laptops & Desktops, you can use CA ARCserve Backup to back up your BrightStor ARCserve Backup for Laptops & Desktops data to media to protect yourself against the possibility of a disaster on your BrightStor ARCserve Backup for Laptops & Desktops server.

To back up a BrightStor ARCserve Backup for Laptops & Desktops server

Note: All BrightStor ARCserve Backup for Laptops & Desktops data on the BrightStor ARCserve Backup for Laptops & Desktops server is backed up.

1. Add the computer running the BrightStor ARCserve Backup for Laptops & Desktops server as a Client Agent. Perform the following steps:
 - a. Right-click the Windows Systems object in the Source directory tree.
 - b. Select Add Machine/Object from the pop-up menu.
 - c. Enter the required information in the Add Agent dialog. For help with the Add Agent dialog, click the Help button.

2. Expand the BrightStor ARCserve Backup for Laptops & Desktops server computer's node in the Source tree and select the BrightStor ARCserve Backup for Laptops & Desktops server box (it will turn green).
3. Submit the backup job as you would any other.

Note: After you have added the computer running the BrightStor ARCserve Backup for Laptops & Desktops server as a Client Agent, you can use the Backup Wizard to submit your backup job.

Migrated Files Management

To help manage the space on backup servers, BrightStor ARCserve Backup for Laptops & Desktops administrators have the option of migrating old backup data to a CA ARCserve Backup server. The administrator defines criteria for old backup data—such as size and the date the file was last modified—on the BrightStor ARCserve Backup for Laptops & Desktops server. Migrating old backup data helps conserve space on the BrightStor ARCserve Backup for Laptops & Desktops server and provides a safe way to archive these files.

Over time, however, some of these file can become obsolete or expired. This can happen when:

- The BrightStor ARCserve Backup for Laptops & Desktops server restores the file to its local storage area, returning the file to the BrightStor ARCserve Backup for Laptops & Desktops server.
- The BrightStor ARCserve Backup for Laptops & Desktops server submits a newer version of a file; older versions of the file with the same name on the tape become obsolete and can no longer be used.
- The BrightStor ARCserve Backup for Laptops & Desktops client to whom the files belong is completely deleted from the server storage area.

In all cases, these files are marked “expired” in the CA ARCserve Backup database.

This expiration of files results in a situation in which parts of the data stored on the BrightStor ARCserve Backup for Laptops & Desktops-dedicated tape are no longer needed, and the tape can be reused and placed in the CA ARCserve Backup scratch set. The following are guidelines for reusing such CA ARCserve Backup media:

- If all files on a tape are no longer being used, the tape can be reused.
- If there are only a few files on the tape, the CA ARCserve Backup administrator can query the files, submit a restore, and free up the tape.

Note: Data Growth Restores cannot be performed on the session level.

Chapter 4: Restoring Data

CA ARCserve Backup provides you with various tools and options that you can use to restore data. This section includes information about how you can safely and efficiently restore data.

This section contains the following topics:

[Restore Manager](#) (see page 239)

[How to Find Files That You Want to Restore](#) (see page 241)

[Restore Manager Markers](#) (see page 250)

[Restore Manager Location Options](#) (see page 252)

[Restore Job Schedules](#) (see page 252)

[Specify Run as Administrator on Windows Server 2008 Systems](#) (see page 253)

[Global Restore Options](#) (see page 254)

[System State Restore Options](#) (see page 263)

[Restoring Data Scenarios](#) (see page 264)

[Restore BrightStor ARCserve Backup for Laptops & Desktops Data](#) (see page 282)

Restore Manager

The aim of running a successful restore job is to quickly identify the data you need and to retrieve it from the appropriate backup media.

CA ARCserve Backup allows you to restore data to most machines attached to your Windows network. Each restore job requires a source and destination. The files selected as your source must originate from backup media created by CA ARCserve Backup, and the destination must be a hard drive. The Restore Manager provides three tabs to customize your restore job:

- Source
- Destination
- Schedule

The optional CA ARCserve Backup Client Agents allow you to communicate with remote workstations in various environments to restore data to non-Windows systems, such as NetWare or UNIX.

Similarly, the optional Backup Agents allow CA ARCserve Backup to restore online databases and applications such as Microsoft Exchange, Microsoft SharePoint, Microsoft SQL Server, Lotus Domino, Oracle, and IBM Informix.

For procedural information on how to submit a basic restore job, see the online help.

If Unicenter NSM is already installed, you can use the monitoring agent to monitor CA ARCserve Backup. This agent can be used to start and stop services, monitor the status of the CA ARCserve Backup processes and media, and report on the failure of backup jobs. For more information, see the section Unicenter Monitoring Agent.

More information:

[Monitor Activity Using the Unicenter Monitoring Agent](#) (see page 631)

How to Find Files That You Want to Restore

CA ARCserve Backup makes it easy to find the files you want to restore. Because your requirements and circumstances can vary, CA ARCserve Backup provides you with the following methods for selecting the data (the source) you want to restore:

Restore by Tree

Lets you restore a specific directory or drive from a display of files and directories that were backed up with CA ARCserve Backup. Use this method when you do not know which media contains the data you need, but you know the machine from which the back up originated.

The Restore by Tree view displays only the last instance of a backup. To view and access all other instances, select the object that you want to restore and click the Version History button. If there are multiple partial backups of the same drive, the Restore by Tree view displays only the last backup. However, if there is a full volume backup of the drive available, the last full backup is displayed, instead of the last partial backup.

The Computer Name field allows you to filter based on partial name searching. You can enter any part of the name and a list of relevant items are returned. For example, if there are some computers whose computer name contains 'BB', you can enter 'BB' in the Computer Name field and click the Update button. Relevant computers are found. The Computer Name field also supports full name searching and wildcard searching.

Note: The Restore Manager cannot display file paths that exceed 512 bytes. For single-byte languages, this equates to approximately 500 characters. For multi-byte languages with a combination of single, mixed, and multi-byte characters, 512 bytes equates to 250 to 500 characters. For multi-byte languages with all multi-byte characters, 512 bytes equates to approximately 250 characters. If a file path exceeds 512 bytes, truncation occurs. To restore data from a truncated directory, you must submit the restore job from the last directory in the path whose name was not truncated.

Search button

Click the Search button to search your backups for a specific file or group of files with a similar file name. CA ARCserve Backup lets you specify file names up to 255 characters, including the file extension, in the Search for field. If you do not know the complete file name, you can simplify the results of the search by specifying the wildcard characters "*" and "?" in the Search for field.

Examples:

1. Drive D:\ contains two directories that are backed up on a weekly basis—D:\Temp and D:\Documents. D:\Temp and D:\Documents were both backed up on April 21 and April 28. A full backup of drive D:\ was performed on April 1.
2. The Restore Manager displays instances relating to the full backup of Drive D:\ performed on April 1.
3. To restore the April 28 instance of D:/Documents, select the D:/Documents directory in the Restore by Tree view and click the Version History button. From the Version History dialog, select the April 28 instance and then click the Select button.

Note: This restore method will not work if the Database Engine is stopped.

Restore by Session

Lets you select the session, the files, and directories you want to restore. Use this method when you know the media name, but are not certain about the session you want to restore.

This restore method will not work if the Database Engine is stopped.

Deduplication devices are supported by Restore by Session but will likely contain thousands of sessions. You will be prompted to choose a display option to manage the volume.

The Media Name field allows you to filter based on partial name searching. You can enter any part of the name and a list of relevant items are returned. For example, if there are some sessions whose media name contains 'BB', you can enter 'BB' in the Media Name field and click the Update button. Relevant sessions are found. The Media Name field also supports full name searching and wildcard searching.

Note: The Restore Manager cannot display file paths that exceed 512 bytes. For single-byte languages, this equates to approximately 500 characters. For multi-byte languages with a combination of single, mixed, and multi-byte characters, 512 bytes equates to 250 to 500 characters. For multi-byte languages with all multi-byte characters, 512 bytes equates to approximately 250 characters. If a file path exceeds 512 bytes, truncation occurs. To restore data from a truncated directory, you must submit the restore job from the last directory in the path whose name was not truncated.

Restore by Query

Lets you restore files based on the search pattern used to locate the names of the files or directories. Use this method when you know the name of the file or directory you want to restore, but do not know the machine it was backed up from or the media it was backed up to.

Restore by query is not a case-sensitive operation.

CA ARCserve Backup lets you specify file names up to 255 characters, including the file extension, in the File Name field. If you do not know the complete file name, you can simplify the results of the query by specifying the wildcard characters "*" and "?" in the File Name field.

Note: This restore method will not work if the Database Engine is stopped.

Restore by Backup Media

Lets you restore a complete backup session from a specified media in a storage device. All files in the session are restored to the destination, unless filters are added to the restore job. Use this method when media was created by a different version of CA ARCserve Backup or if the database does not recognize it.

Important! If you cannot see the items that you would like to restore, the corresponding records may have been pruned from your database. You can repopulate your restore source selection by running the Merge utility. For more information about the Merge utility, see the section Merge Utility.

If you installed the CA ARCserve Backup Enterprise Module, you will also have Restore by Image/Serverless available. Use this method when you need to read and restore blocks of data quickly by bypassing the file system.

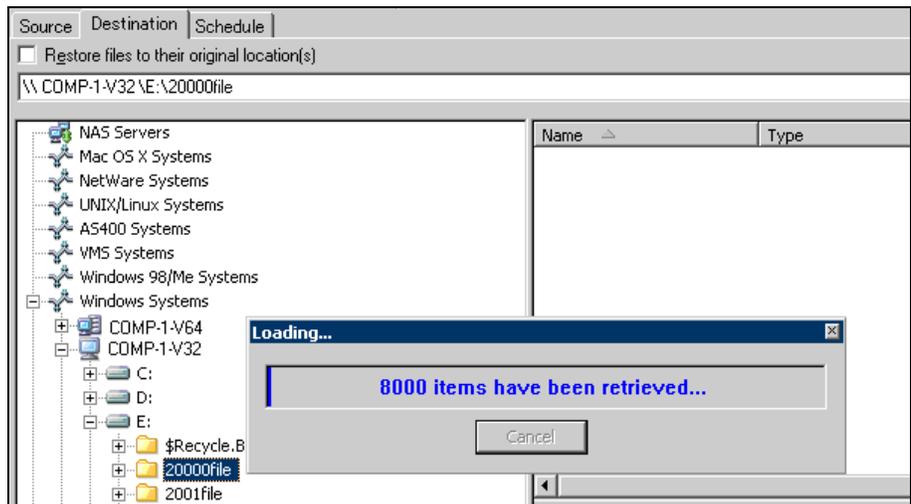
Note: For more information on how to submit a restore job using each of these methods, see the online help.

How CA ARCserve Backup Lets You Browse a Large Number of Items in the Restore Manager

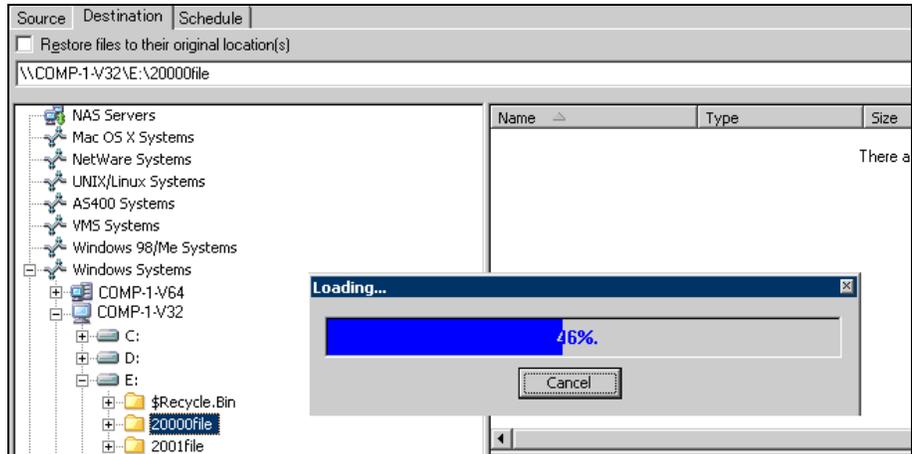
CA ARCserve Backup lets you pause the process of loading items in the Restore Manager when you browse a large number of directories, files, and so on. You can pause the loading process when you click the Destination tab, clear the check mark from the Restore files to their original location(s) option, and browse items on the Destination tab.

The steps that follow describe how CA ARCserve Backup lets you browse a large number of items in the Restore Manager window.

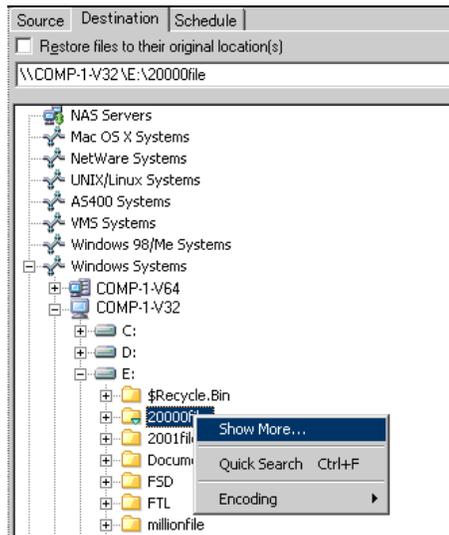
1. When you select an item in from the directory tree in the Restore Manager, Destination tab, CA ARCserve Backup displays a Loading dialog to inform you that a large number of items need to be retrieved and loaded into the Restore Manager window. You cannot click Cancel while CA ARCserve Backup is retrieving the list of items to display in the Restore Manager window.



- After CA ARCserve Backup retrieves the list of items to display in the Restore Manager Manager window, the Loading dialog then displays the percentage of items that are loaded into the Restore Manager. You can click Cancel to pause the operation.



- After you pause the Loading operation, you can continue the Loading operation by right-clicking the target directory and selecting Show More from the pop-up menu.



- If you pause the loading process, the icon for the target directory displays as follows:



5. You can pause and continue the loading process as often as necessary. To load more items, right-click the target directory and click Show More from the pop-up menu.
6. When the loading process is complete, the icon for the target directory displays as follows:



Browse a Large Number of Files in the Restore Manager

Use the following procedure when you need to browse a directory that contains a large number of items in the Restore Manager.

To browse a large number of files in the Restore Manager

1. Open the Restore Manager and click the Destination tab.
On the Destination tab, clear the check mark from Restore files to their original location, and then browse to and specify a target directory from the directory tree.
The Loading message box appears.
2. From the Loading message box, click Cancel to stop the loading process.
If CA ARCserve Backup did not load all items, the To show more objects, right-click the target directory and select Show More from the pop-up menu warning message appears.
Note: The message only appears the first time you click Cancel on the Loading message box.
3. From the directory tree, right-click the target directory and click Show More from the pop-up menu.
The Loading message box appears and CA ARCserve Backup continues loading the items.
4. You can pause and continue the loading process as often as necessary until CA ARCserve Backup loads all items in the target directory.
If you pause the loading process, the icon for the target directory displays as follows:



When the loading process is complete, the icon for the target directory displays as follows:



Restore Manager Considerations on 64-bit Windows Platforms

If the CA ARCserve Backup server is running on a 64-bit Windows platform, the following considerations apply:

- Information about objects backed up from the local server using the Client Agent for Windows appears under the Windows Systems object in the source directory tree. The objects can include files, folders, drives, System State files, the Windows Registry, and Volume Shadow Copy Service writer backups.
- Local database agent objects backed up using network-based communication appear in the Local Server branch the Restore Manager Source directory tree.
- Remote database agent objects backed up using network-based communication appear in the Microsoft Windows Network branch of the Restore Manager Source directory tree.

Version History

If you have backed up a volume, directory, or individual files on a node more than once, the path displays only once in the graphical tree, but you can still restore any version of your data in the database. Use the Version History button to view all the versions that you backed up and select the one that you need. Each version is identified by modification date, file size, media name, backup time, session number, type, and method.

Note: You can view the Version History when you use Restore by Tree as your source view.

Duplicate Backup Sessions

When you use the Disk to Disk to Tape Option to back up data or copy media using the `tapecopy` command line utility, duplicates of backup sessions can exist in multiple locations. For example, you can define your staging copy and purge policies such that backup sessions remain on the file system device used for staging for a period of time after the copy to final destination media operation occurs. If the backup session was not purged from the file system device, data will reside on the file system device and the final destination media. If this situation presents itself, you can quickly restore the session by using data that resides on the file system device.

When you copy media, duplicate backup sessions exist on multiple media. If one media remains on site and the other media was vaulted, you can direct CA ARCserve Backup to use the media that is on site to facilitate the restore operation.

To search for duplicate sessions, click the Duplicates button on the Version History dialog. The Duplicates Sessions dialog displays the original backup session and all of its copies. If duplicates for a session exist, you can direct CA ARCserve Backup to use the session that allows you to restore the session as quickly as possible.

Smart Restore

CA ARCserve Backup provides a transparent Smart Restore feature that can increase the overall success rate of your restore operations. If a media read error or a hardware error occurs during a restore job, CA ARCserve Backup searches for an alternate media to use to complete the restore job. Consider the following scenario:

During a restore job, the restore source media jams and disables the library. CA ARCserve Backup then searches for duplicates of the backup session. If a duplicate of the session exists, regardless of whether it exists on a file system device or another media, the restore operation continues without user intervention.

Note: If a second media error occurs during the restore job, the job will fail.

Restore Data by Query on UNIX and Linux Platforms

The Restore by Query method of restoring data lets you search for and restore files based on the search criteria used to locate the names of the files or directories stored in your backup data. On UNIX and Linux platforms, the syntax that you use to query the ARCserve database based on the Look in Directory (file location) option is different from that of Windows platforms. The following procedure describes the syntax that you will use to restore data by query on UNIX and Linux platforms.

To restore data by query on UNIX and Linux platforms

1. From the Restore Manager, select Restore by Query from the Source view drop-down list.

The Restore by Query fields appear.

2. To specify your search criteria, complete the following fields:

Computer Name

Lets you specify the name of the computer that you want to search. You can specify a specific computer name or select <<ANY>> from the drop-down list to search all computers in your ARCserve environment.

File Name

Lets you specify a wild card or specific file name search. On UNIX and Linux platforms, CA ARCserve Backup uses the standard 8.3 file naming convention. For example, if you specify *.txt, all files with a .txt file extension appear in the query results.

Note: Do not specify leading or trailing spaces in this field.

Look in Directory

Lets you specify the directory that you want to search. You must specify an exact string match, starting with the drive letter, in this field.

UNIX and Linux platforms regard the backward slash character "\" as a separator. For example, \root\dir1\text.txt.

Examples:

If the mount point is "/", use the following search string:

```
/\root\dir1\text1
```

If the mount point is "/root", use the following search string:

```
\root\dir1\text1
```

Note: Do not specify leading or trailing spaces in this field.

Include Subdirectories

Lets you search the subdirectories of the directory specified in the Look in Directory field.

3. Click Query.

CA ARCserve Backup queries the ARCserve database and returns the files that meet your search criteria.

4. Select the files and directories you want to restore by double-clicking the name of the file or directory.

A green light appears when a file or directory is selected.

Restore Manager Markers

Each object displayed in the Restore Manager window has a green or gray box to its left called a marker.

Green marker

Lets you control the extent of the restore for an object directly. Click a marker to exclude an object from a restore or to indicate that you want the restore for the object to be full or partial. As you click the marker, you fill or empty the marker of color, indicating the extent of the restore.

Gray marker

These markers are associated with objects that are not real and that you cannot restore. Typically, these items serve as placeholders under which other objects are grouped and displayed. As you click the green markers under a gray marker item, the fill proportion of the gray marker changes automatically from empty to partial to full depending on the proportion of files you have chosen to restore.

The following table describes the different marker configurations and corresponding restore levels:

Marker	Configuration	Description
	Completely filled center.	Full restore.
	Partially filled center.	Partial restore.
	Empty center.	Do not restore.

Note: Gray marker configurations follow the same pattern as green marker configurations, but reflect the proportion of files under them that are selected for restore.

The fill proportion of a marker at a higher level of the directory tree depends on the fill proportions of the markers of the objects at the lower levels.

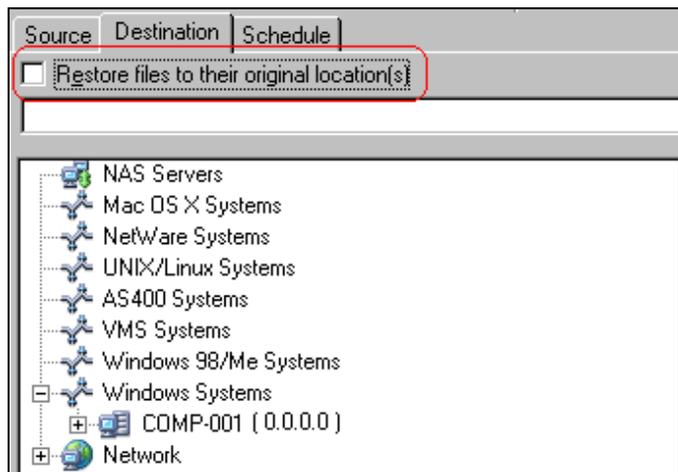
- If all the markers at the lower levels are completely filled, then the marker at the higher level is also automatically completely filled.
- If the markers at the lower levels are a mix of completely filled and partially filled, then the marker at the higher level is automatically partially filled.
- If you click a marker at a higher level so that it is completely filled, then all the markers at the lower levels are automatically filled completely.

Restore Manager Location Options

CA ARCserve Backup provides you with two methods for selecting the location that you want to restore the data to:

- Restore files to their original location
- Restore to user-shared directories and drives

Note: The default method is to restore files to their original location. If you deselect this check box, you are presented with a list of machines, directories and files. You can select your specific destination from this list.



For information on how to select a destination, see the online help.

Restore Job Schedules

Jobs can be submitted so that they repeat as follows:

- **Once**--Do not repeat this job.
- **Every n frequency**--Repeat this job every specified number of Minutes, Hours, Days, Weeks, or Months.
- **Day(s) of the Week**--Repeat this job on the days that are checked off.
- **Week(s) of the Month**--Repeat this job on the weeks that are checked off.
- **Day of the Month**--Repeat this job on the specified day.
- **Custom**--Repeat this job on the month, day, hour, or minute specified.

Note: If you select the Run Job Now option when your storage device is busy, CA ARCserve Backup reports that the storage device is busy and the job is not submitted to the job queue. You should schedule your job, keeping the current date and time. This way, when CA ARCserve Backup discovers that the storage device is busy, it automatically retries the job until the drive becomes free.

For a description of detailed job scheduling features, see the chapter “Customizing Jobs” or the online help.

Specify Run as Administrator on Windows Server 2008 Systems

On Windows Vista and Windows Server 2008 operating systems, a security feature prompts you to provide or confirm administrator credentials (user name and password) each time you attempt to launch an executable or application. To bypass the continuous prompting you can specify to run each executable or application as an administrator.

For example, if you want to run the Windows Command Prompt, locate the Command Prompt icon (from the Start menu), right-click the icon, and select the Run as administrator from the pop-up menu. After your administrator privileges have been established for the Command Prompt console, all subsequent Command Prompt invocations can be launched without any further prompts until you close the Command Prompt console.

Note: This task should be performed on all CA ARCserve Backup executables and applications. For example, ca_auth , ca_backup, ca_restore, cabatch, and so on.

To specify Run as Administrator on Windows Server 2008 systems

1. From Windows Explorer, locate the executable or application that you want to specify as Run as administrator.

Right-click the executable or application and select Run as administrator from the pop-up menu.

Windows prompts you to provide administrator credentials (a user name and a password).

2. Do one of the following when you are prompted to provide administrator credentials:
 - If you are not logged in as an administrator, enter the administrator user name and password.
 - If you are logged in as an administrator, click Continue.
3. Follow the prompts and complete the required fields to complete this task.

More information:

[Authentication Levels for CA ARCserve Backup Services, Components, and Applications](#) (see page 484)

Global Restore Options

This section describes the global restore options you can select when submitting your restore job. To access the global options dialog, click the Options button in the Restore Manager. The available options are as follows:

- [Backup Media options](#) (see page 254).
- [Destination options](#) (see page 255).
- [Operation options](#) (see page 258).
- [Pre/Post options](#) (see page 260).
- [Job Log options](#) (see page 261).
- [Virus options](#) (see page 261).
- [Alert options](#) (see page 262).

Restore Manager Backup Media Options

The Restore Manager supports the following backup media options:

Timeout Options

You can specify a timeout period that CA ARCserve Backup will wait to provide the media you need to restore your data. Available media options are:

- **Timeout for First Backup Media**--Period of time that CA ARCserve Backup waits for the first media required for your restore job. If the time expires, the job fails.
- **Timeout for Additional Backup Media**--Period of time that CA ARCserve Backup waits for any additional media to become available.

Optimize Restore

If, during a restore operation, CA ARCserve Backup discovers duplicate backup sessions, where one session resides on tape media and another session resides on a file system device, the Optimize Restore option directs CA ARCserve Backup to restore the data from the session that resides on the file system device.

The Optimize Restore option is a global setting that is applied to all restore operations, and is enabled by default.

Under most circumstances, restoring data from a file system device is faster than restoring from tape media. However, you may wish to consider disabling the Optimize Restore option if you are using tape media or a library with high-speed reading capabilities, or there is a known problem with your file system device.

To disable the Optimize Restore option, clear the check mark from the Optimize Restore check box.

Restore Manager Destination Options

The Destination options determine how the directory structure is created on the destination when files are copied or restored. They also determine which files (if any) can be overwritten.

Directory Structure Options

Select one of the following methods CA ARCserve Backup should use to create directories on your destination.

- **Do Not Create the Base Directories**--(default) Do not create the base directory on the destination path, but create all subdirectories below the source base directory. A base directory is considered the first directory selected in the source path.
- **Create Directories from the Base**--Create the destination path beginning from the base directory.
- **Create Entire Path from the Root**--Create the entire source path (except the root drive or volume name) on the destination. No files from any parent directories are restored. Only the directory path to the base directory is created on the destination.

File Conflict Resolution Options

Select the method CA ARCserve Backup should use when there are files on the destination disk that have the same name as files being copied from the source. The default is Overwrite All Files.

- **Overwrite All Files**--Restore all source files to the destination regardless of conflicting file names. The files from the source overwrite existing files on the destination.
- **Rename Files**--Copy the source file to the destination with the same file name but a different extension. The format of the renamed extension will vary based upon the file system that is present on the target partition.

- **Restoring files to local NTFS partitions**--If the length of the file name is less than or equal to 251 characters, CA ARCserve Backup appends '.__0' to the file name after the first restore. For all subsequent restores, CA ARCserve Backup appends '.__1', '.__2', and so on to the file name. This rule applies to file names with and without a file extension.

If the length of file name is more than 251 characters, CA ARCserve Backup truncates the file name at 251 characters and appends '.__0' to the file name, after the first restore. For all subsequent restores, CA ARCserve Backup appends '.__1', '.__2', and so on to the truncated file name.

- **Restoring files using the Windows Client Agent and to local or remote FAT, FAT32, and NTFS partitions**--If the length of the file name is less than or equal to 251 characters and has a file extension, CA ARCserve Backup replaces the last character of the file extension with the character 1 (for example, filename.tx1). For subsequent restores, CA ARCserve Backup replaces the last character of the file extension with the character 2, 3, and so on. After the 10th restore, CA ARCserve Backup replaces the last two characters of the file extension with 10, 11, 12, and so on (for example, filename.t10). After the 100th restore, CA ARCserve Backup replaces the last three characters of the file extension with 100, 101, 102, and so on (for example, filename.100). After the 999th restore, CA ARCserve Backup cannot rename the file extension, which causes the restore to fail. If the length of the file name is less than or equal to 251 characters, and it does not have a file extension, CA ARCserve Backup appends '.__0' to the end of the file name. If CA ARCserve Backup appends '.__0' to the file name after the first restore, the renaming process appends two characters after the 10th restore (for example, filename.__10), and after the 100th restore, the renaming process appends three characters to the file name (for example, filename.__100). After the 999th restore, CA ARCserve Backup cannot rename the file name, which causes the restore to fail.

If the length of file name is more than 251 characters, CA ARCserve Backup renames the file using the same rules as restoring to local NTFS partitions.

- **Skip Existing Files**--Do not restore a source file if a file with the same name already exists on the destination.
- **Overwrite with Newer Files Only**--Only restore source files whose modification date is later than the modification date of the file with the same name on the destination. Source files whose modification date is earlier are not copied to the destination.
- **Confirm Overwrites (for Run Now only)**--A user prompt must confirm the restore of source files with the same name on the destination.

Note: This option is used for local restore jobs on x86 operating systems but does not display on Vista or Windows Server 2008 operating systems.

VMS File Version Options

The following options indicate how CA ARCserve Backup should act when restoring VMS files that have the same names and version numbers as the files in the target restore directory.

- **Create New File Version**--CA ARCserve Backup will restore all files as new versions of the original. The files in the target directory will not be affected.
- **Replace Current File Version**--If a file in the target directory has the same name and version number as a file in the restore data, CA ARCserve Backup will overwrite the file.
- **Restore File Version**--If a file in the target directory has the same name and version number as a file in the restore data, CA ARCserve Backup will not restore the file. All other files will be restored with their original names and version numbers.

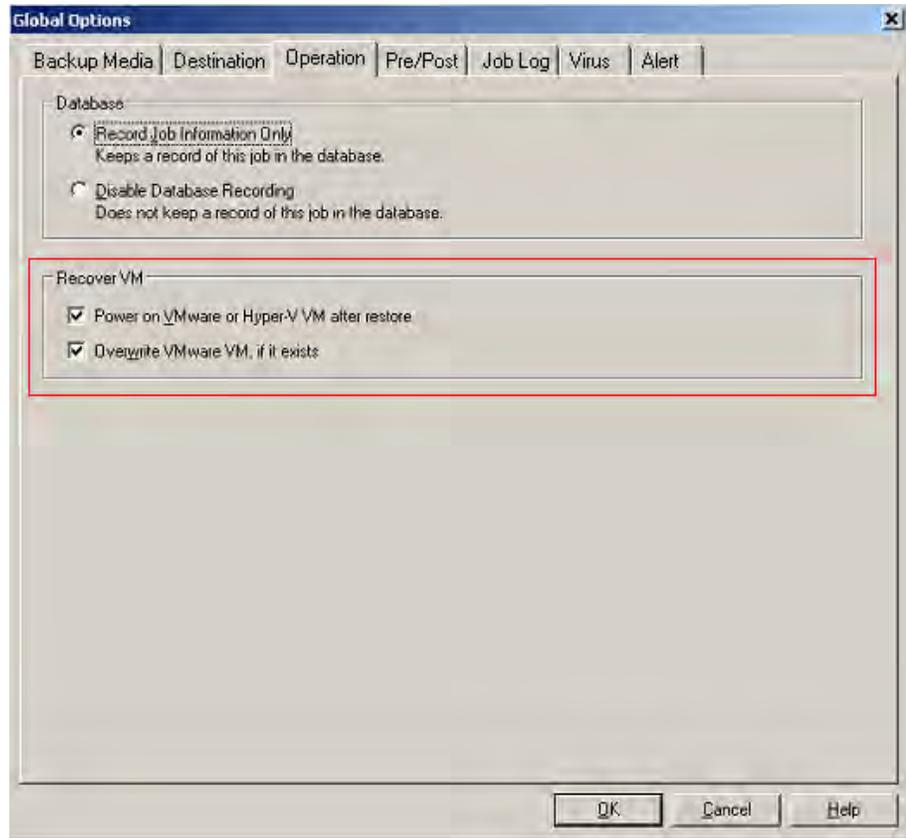
Restore Manager Operation Options

Operation options let you determine the actions or related action that you want to perform while a job is in progress or after a job completes, and the level of detail that is recorded in the CA ARCserve Backup database.

The options that follow affect the CA ARCserve Backup database:

- **Record Job Information Only**--Record job information.
- **Disable Database Recording**--Do not record job information.
- **Restore and Preserve Directory Attributes and Security Information**--Restore the existing directory attributes (such as Read Only, Archive, and Hidden) and security data to the machine.
- **Restore and Preserve File Attributes and Security Information**--Restore the existing file attributes (such as Read Only, Archive, and Hidden) and security data to the machine.
- **Restore Registry Files and Event Logs**--Restore registry files and event logs to the restore target machine if the sessions selected for restore have the registry files and event log files.

The options that follow affect VM restores and appear on the Operation tab only if the restore method selected is Recover VM:



- **Power on VMware or Hyper-V VM after restore**--Powers on the VM after the restore job is complete.

Default value: Enabled.

- **Overwrite VMware VM, if it exists**--Lets you overwrite the VM, if the VM exists.

When you restore a VMware VM, CA ARCserve Backup detects the VMs that reside in the host system. If the VM exists in the host system, this option lets you overwrite the VM using the existing UUID of the VM.

Default value: Enabled.

Note: For Hyper-V VMs, the agent always overwrites the VM, if the VM exists in the Hyper-V host.

The option that follows affects CA XOsft scenarios:

- **Continue the restore job even when the scenario cannot be stopped--**Lets you restore a CA XOsft scenario while you are backing up the scenario.

When you attempt to restore a CA XOsft scenario while you are backing up the scenario, by default, the restore job will fail. With this option specified, CA ARCserve Backup will complete the restore job while a backup is in progress.

Note: The above option appears on the Global Options dialog only when you integrate CA ARCserve Backup with CA XOsft.

Restore Manager Pre/Post Options

The Pre/Post options let you run a command on your system before or after the job is executed.

For example, you can use the Pre option to stop the application that owns the data you are backing up, and then use the Post option to start it the application after the backup is complete.

Note: Commands with executables on remote systems are not supported.

- **Run Command Before Job--**Select the following options to run a command on your machine before the job is executed:
 - Enter the path to, and name of, the file to be executed on the machine before the job starts.
 - **On Exit Code--**CA ARCserve Backup detects exit codes of other programs. For a specified exit code, you can choose to run the job immediately, skip the job, or skip post application.
 - **Delay in Minutes--**Specify the delay that CA ARCserve Backup waits before running a job when the specified exit code is detected.
- **Run Command After Job--**Enter the path to, and name of, the file to be executed on the machine after the job is completed.
- **Do Not Run Command If--**Specify that a command will not run if CA ARCserve Backup detects the following events:
 - **Job Fails--**If a job fails, then the command will not run.
 - **Job is Incomplete--**If a job is not completed, then the command will not run.
 - **Job is Complete--**If a job is completed, then the command will run.

- **Run Before/After Command As--**Specify the User Name and Password that corresponds to that of the Local Host server selected, and is required to check the system privileges on that server. The user name and password entered into these fields should not be confused with the CA ARCserve Backup User Name and Password.

Restore Manager Job Log Options

Using this option, you can determine the level of detail that is included in the log report for the restore job. You can view the log report in the Job Queue or Database Manager window (Job View). The log options are:

- **Log All Activity--**Record all of the activity that occurs while the job is running.
- **Log Summary Only--**Record summary information of the job (including source, destination, session number, and totals) and errors.
- **Log Disabled--**Do not record any information about this job in the job log.

Restore Manager Virus Options

Since CA Antivirus is bundled with CA ARCserve Backup, you can automatically scan for viruses during the job using the virus scanning options.

Enable Virus Scanning

Select this option to enable virus scanning and the following options:

- **Skip--**Do not back up the infected file.
- **Rename--**If CA Antivirus detects an infected file (for example filename.com), it renames the file and appends 0.AVB to the file name (for example filename.com.0.AVB). If filename.com.0.AVB already exists, eTrust renames the file to filename.com.1.AVB, filename.com.2.AVB, filename.com.3.AVB and so on.
- **Delete--**Delete the infected file.
- **Cure--**Attempts to cure the infected file.
- **Scan Compressed Files--**Check each file in compressed archives individually. Selecting this option might affect the performance of the backup but provides increased virus protection.

Restore Manager Alert Options

You can use the Alert notification system to send messages about events that appear in the Activity Log during your restore operation. Choose one or more of the following events for which you want to be notified:

- **Job Completed Successfully**--All of the nodes and drives/shares were processed.
- **Job Incomplete**--Some nodes, drives, or shares were missed.
- **Job Canceled by User**--The user canceled the job.
- **Job Failed**--The job was started but could not be completed.
- **Virus Detected**--A virus was detected in one of the files to be backed up. See Virus options (Backup, Copy, Count)
- **Customized Event**--A customized event occurred. To specify this type of event, enter an error, warning, or notification code in the space below the Event drop-box.

Choose one or more of the defined Alert configurations. The <default> configuration means that you will use whatever is configured in Alert Manager. Click Configure to define further configurations. CA ARCserve Backup provides the following defined Alert configurations:

- Broadcast
- Pager
- SMTP
- SNMP
- Event
- Printer
- E-Mail
- Lotus Notes
- Unicenter TNG

Select **Attach Job Log** to include the job log information in the Alert message. (This option applies for Trouble Tickets and Mail only.)

Note: The list you create using Alert Options is saved with the Job Script and the configuration defined using the Configuration button.

System State Restore Options

Right-click the system state session to access the restore option context menu. The following options are available:

Make the Restored Copy of the Active Directory Authoritative

Forces the restored copy to become the “authoritative” version of Active Directory on the system. This means that, even if the restored replica set is older than the current replicas, the older data is replicated to all of its replication partners. Authoritative restore is typically used to restore a system to a previously known state.

When Restoring replicated data sets, mark the data as primary for all replicas

Forces the restored File Replication service data to be replicated to other servers. If this option is not enabled, the replicated data sets may not be replicated to other servers because the restored data will appear to be older than the data on other servers.

Stop the Cluster if necessary to Restore the Cluster Database

Gives permission to stop a cluster service to restore the cluster database. This applies only to cluster machines. If this option is not enabled and the cluster service is running, CA ARCserve Backup dumps the cluster database files into the %SYSTEMROOT%\clusbkup folder, but does not load them. CA ARCserve Backup provides a utility program (caclurst.exe) that lets you load the cluster database files at a convenient time.

Enable Quorum Drive Selection when Quorum Location Changes (Non-Windows Server 2008 Cluster only)

Lets you to set the drive of the quorum resource that a cluster currently uses. If a cluster system was reconfigured to use a different quorum drive since the last system state backup, use this option to provide the new quorum drive. Otherwise, the backup copy of the quorum drive will be used which will cause the cluster database restore to fail.

Select the drive letter in the case the quorum location changed since this backup

Lets you specify a drive letter to restore data to when the location of the quorum changed since the backup was performed.

Authoritative Restore Cluster Database (Windows Server 2008 Cluster only)

Lets you perform an authoritative restore on Windows Server 2008 clusters. An authoritative restore lets you to restore the cluster database across all nodes. You should enable this option when you want to roll back the cluster configuration to the previous version.

Note: If the node that you want to restore is corrupt or not operational, you must perform a node restore before you perform an authoritative restore. To perform a node restore, do not enable this option..

Do not Stop World Wide Web Service

Lets you continue the www service while the certificate server is being restored. The IIS Publishing Service may be using the certificate service dynamic files at the time of certificate server restore. For this reason, by default, WWW service will be stopped during certificate server restore. If you do not want it to stop, use this option.

Restoring Data Scenarios

The following sections describe how to restore data in specific scenarios.

Restore Data Backed Up Using Staging

The process for restoring data that was backed up using the Disk to Disk to Tape Option is identical to the process of restoring data that was backed up to any other type of storage media. However, staging provides you with the option to restore data from the location that is most suitable to your needs.

When you perform backup operations using the Disk to Disk to Tape Option, and the backed up data has been copied to its final destination media, the data can reside in two locations (the staging device and its final destination media). If you need to perform a restore operation and the data resides in two locations, you can restore the data directly from the staging device. Restore operations from staging devices are usually faster than tape-based restores.

To restore data that was backed up using staging

1. Open the Restore Manager and select the Restore by Tree method.
2. In the left pane of the Restore Manager, select the volume, drive, directory, or file you want to restore.
3. Click the Version History button.

CA ARCserve Backup searches the databases and the Version History dialog opens displaying a list of all backed up versions of this file, directory, drive, or volume.

Note: When using disk or tape staging, ensure that the staging tape is not offlined without formatting or erasing the staging tape. This will allow you to view the session details from the destination (migration) tape.

4. From this list, select the version you want to restore.

CA ARCserve Backup presents you with a list of all duplicates for the session. Duplicates exist when clones of the session reside on the multiple media which might have happened because of staging backup jobs or tape copies.

Note: If the staging device is an FSD, restoring data from a disk is generally faster than restoring from a tape. When you restore data from a disk, there are no delays caused by tape load and seek latency. If you need to restore data that exists in two locations (disk and tape), you can reduce the restore time by restoring directly from the disk rather than retrieving it from a tape.

- If you want to restore directly from the final destination, click OK to start the restore process.
- If you want to restore from a different location rather than from the final destination, click the Duplicates button.

The Duplicate Sessions dialog opens displaying any sessions which are duplicates or clones of each other (including the original session). If the selected session has no duplicates, the Duplicates field will be blank.

For each copy of the selected session, the Duplicate Sessions dialog displays the Modified Date, Size, Media Name, Backup Time, Session #, Type, and Media Type to help you decide the location from where you want to restore from.

After you select the session and click OK, the restore process will start.

Restore a Remote Agent on a System without the Disaster Recovery Option

This section describes how to restore a remote agent on a system without the CA ARCserve Backup Disaster Recovery Option.

Before proceeding, ensure that the following prerequisite tasks are complete:

- Verify that there is one full backup of the remote agent machine, and verify that the backup media is available.
- Record the disk partition/volume configuration, including all volume drive letters and volume mount points, when the system is up and running.
- Record the network configuration when the system is up and running.
- Ensure the operating system CD, the device drivers, and the CA ARCserve Backup installation media are available.

To restore a remote agent on a system without the Disaster Recovery Option

1. Start the computer you want to recover, using the Windows operating system CD.
2. Create partitions which are necessary for installing the operating system. Other disk partitions/volumes can be restored manually after the operating system is installed. For dynamic disk configuration, it must be restored after the operating system is installed.
3. Install the operating system and verify that the host name is the same as the original system.
4. Restore the remaining disk/volume configuration, disk partition layout, dynamic disk volumes, etc.
Note: The volume drive letter should be the same as the original system.
5. Install the device drivers which are not included on the operating system CD. This includes SCSI/RAID/FC drivers and network adapter drivers.
6. Configure the network and verify that all configurations are the same as the original system.
7. Apply the operating system patch. This is necessary when the system is going to be connected to the network.
8. Install the same antivirus software as backup time, and update to the latest patch. This is necessary when the system is going to be connected to the network.
9. Install CA ARCserve Backup Client Agent.

10. Add this machine to the source node list of the ARCserve backup server if it is not on the existing node list.
11. Select restore by tree in the CA ARCserve Backup Restore Manager and submit the restore job.

Restore CA ARCserve Backup Member Servers without the Using the Disaster Recovery Option

This section describes how to restore CA ARCserve Backup member servers without using the Disaster Recovery Option.

Important! This procedure does not apply to restoring CA ARCserve Backup primary servers and stand-alone servers.

Prerequisite Tasks:

Before proceeding, ensure that the following prerequisite tasks are complete:

- Ensure that there is at least one full backup of the system and the backup media is available.
- Record the disk partition/volume configuration, including all volume drive letters and volume mount points, when the system is up and running.
- Record the network configuration when the system is up and running.
- Ensure that the operating system CD, the device drivers, and the CA ARCserve Backup installation media are available.

To restore CA ARCserve Backup member server without using the Disaster Recovery Option

1. Start the computer you want to recover, using the Windows operating system CD.
2. Create the partitions that are necessary for installing the operating system. Other disk partitions/volumes can be restored manually after the operating system is installed. For dynamic disk configuration, it must be restored after the operating system is installed.
3. Install the operating system and verify that the host name is the same as the original system.
4. Restore the remaining disk/volume configuration, disk partition layout, dynamic disk volumes, and so on.

Note: The volume drive letter should be the same as the original system.

5. Install the device drivers which are not included on the operating system CD. This includes SCSI/RAID/FC drivers and network adapter drivers.
6. Configure the network and verify that all configurations are the same as the original system.
7. Apply the operating system patch.
Note: This step is necessary when the system is going to be connected to the network.
8. Install the same antivirus software that was running when the last backup completed and update to the latest patch.
Note: This step is necessary when the system is going to be connected to the network.
9. Install all applications same as original system.
10. Install CA ARCserve Backup, agents, and options into the same directories as the original installation.
11. Open the Restore Manager and click the Options toolbar button.
The Options dialog opens.
Click the Operation tab, select the Restore Registry File and Event Log option and click OK.
The restore options are applied.
12. From the Restore Manager, specify the Restore by tree restore method and submit the restore job to restore the system.
Restart the system after the restore job is complete.
If the system is not a domain controller, go to Step 17.
13. When restarting the system press the F8 key to start the Windows Server 2003 Expansion Option Menu.
14. When prompted, select Directory Service Restore Mode to start the system in the restore mode.
15. Restore the System State using the following options:
 - Specify the System State as the source.
 - From the ARCserve server, specify the Global Options for restoring data (see Step 10).
16. Restore the system.

17. After the job is complete, restart the system.
18. Based on one of the following scenarios, confirm that the system has been restored successfully after the system restarts.
 - If the operating system detects that the backed up registry information does not reflect the currently-used hard disk device, you may need to change the drive letter assignment. If this occurs, re-assign the proper drive letter.
 - If a file is required for the system, in addition to the system drive, you may need to restart the system after the drive letter is re-assigned. If other drives are data only, restarting the system is not necessary. If you are not sure of the types of data that reside on the other drives, you should restart the system after re-assigning the drive letter.

Best Practices - How to Recover a Stand-alone Server from a Disaster Using the Disaster Recovery Option

The following scenario describes how to leverage the Disaster Recovery Option to protect an CA ARCserve Backup server that is hosting SQL Server databases.

Server Specifications

The CA ARCserve Backup server is configured as follows:

- The ARCserve Stand-alone Server installation option is installed on the server.
- The ARCserve database is hosted using Microsoft SQL Server 2005 Express Edition.
- The stand-alone server is hosting various Microsoft SQL Server databases.

Software Specifications

The following applications are installed on the CA ARCserve Backup server:

- Microsoft Windows Server
- Microsoft SQL Server
- Microsoft SQL Server 2005 Express Edition as the CA ARCserve Backup database
- CA ARCserve Backup for Windows
- CA ARCserve Backup Client Agent for Windows
- CA ARCserve Backup Agent for Microsoft SQL Server
- CA ARCserve Backup Disaster Recovery Option

Note: Microsoft SQL Server and Microsoft SQL Server 2005 Express reside on the same node. The CA ARCserve Backup installation routine installed the Microsoft SQL Server 2005 Express application.

Use the following guidelines to recover an CA ARCserve Backup server that is hosting SQL Server databases from a disaster:

1. During the backup operation, ensure that you do not status the SQL Server and SQL Server 2005 Express instances as offline.
2. Perform a full backup of the machine. The backup should be successful.
3. Create the Disaster Recovery Boot Kit.

Note: For information about creating a Disaster Recovery Boot Kit, *Disaster Recovery Option Guide*.

4. Perform Disaster Recovery restore. The restore should be successful.

During the restore operation, the Disaster Recovery Option recovers the master and model databases in the CA ARCserve Backup database (Microsoft SQL 2005 Express).

5. When prompted, restart the CA ARCserve Backup server.

After you restart the CA ARCserve Backup server, the disaster recovery process continues recovering the CA ARCserve Backup database. After the CA ARCserve Backup database is recovered, you can start CA ARCserve Backup normally.

6. Restore the disaster recovery element sessions for the SQL Server database instances.

Note: For more information, see the *Agent for Microsoft SQL Server Guide*.

7. Restart the SQL instances.
8. Restore the data to each of the SQL instances.

Best Practices - How to Recover a CA ARCserve Backup Server from a Disaster Without Using the Disaster Recovery Option

CA ARCserve Backup lets you perform a full disaster recovery of a CA ARCserve Backup server without installing the Disaster Recovery Option. To enable this capability, you must complete the steps described in Recover the CA ARCserve Backup server described below. If the CA ARCserve Backup server that you are recovering is a primary or stand-alone server, you must also complete the steps in Recover the CA ARCserve Backup Database below.

The procedure consists of the following tasks:

1. Perform a full backup and restore of the CA ARCserve Backup server.
2. Recover the CA ARCserve Backup server.
3. Recover the CA ARCserve Backup database.
4. Reactivate the existing CA ARCserve Backup database (optional).
5. Recover the Job Queue Session.

Important! You must restore the Job Queue to the ARCserve primary or stand-alone server. Do not restore the Job Queue to a member server of any ARCserve domain.

6. Recover the Active Directory.

Note: This task applies only to CA ARCserve Backup servers that function as a domain controller.

7. Confirm CA ARCserve Backup licenses, if needed.

Note: During and after the recovery process, you will encounter error messages in the system log and CA ARCserve Backup log. These messages are normal under recovery circumstances and will not result in a loss of data or functionality problems.

To recover the CA ARCserve Backup server

Important! You must have performed at least one full backup of the CA ARCserve Backup server before you can recover the CA ARCserve Backup server.

1. (Optional) If the CA ARCserve Backup server is a domain controller, Windows File Replication Service must be installed on the backup server before you can restore the system state to the backup server.
2. Reinstall the operating system on the CA ARCserve Backup server.
Ensure that the hard disk partitions, hardware, and the operating system (version, edition, and service pack) configurations are identical to the configurations that were backed up.
3. Reinstall CA ARCserve Backup, agents, and options into the same directories as the original installation.
4. After you install CA ARCserve Backup, open the Merge utility and merge the media used for the last full backup.
5. After the merge is complete, open the Restore Manager, and ensure that the Restore files to their original location(s) option is checked.

Locate the full backup sessions.

Select the backup sessions for the machine, excluding all of the following CA ARCserve Backup-specific sessions:

- Disaster Recovery session
- ARCserve Job Queue session
- ARCserve Database session
- SQL Server Disaster Recovery Elements session

Note: If the CA ARCserve Backup Catalog database session was selected during the restore, you must close the CA ARCserve Backup Manager Console after you submit the restore job (CA ARCserve Backup enables the catalog database by default). This approach lets the restore process overwrite the catalog database. You can reopen the Job Status Manager or Job Monitor to monitor the status of the job, however, you must not open the Restore Manager or Database Manager until the job is complete.

6. Click the Options toolbar button.
The Restore Manager, Options dialog opens.
Click the Operations tab, click Restore Registry Files and Event logs, and click OK.
The Options dialog closes.
7. Click the Start toolbar button to submit the restore job.
The Session User Name and Password dialog opens.

8. On the Session User Name and Password dialog, complete the fields that follow, as required, and then click OK.
 - **User Name**--Specifies the user name for the target CA ARCserve Backup server.

Note: You must complete this field on Windows Server 2003 64-bit systems and on Windows Server 2008 systems.
 - **Password**--Specifies the password for the target CA ARCserve Backup server.

Note: You must complete this field on Windows Server 2003 64-bit systems and on Windows Server 2008 systems.
 - **Session Password**--Specifies the password for encrypted backup sessions.
 - **IP Address**--Specifies the IP address of the target CA ARCserve Backup server.

On the Session User Name and Password dialog, click Edit to modify the User Name, Password, and IP address for the selected session.

The Enter User Name and Password dialog opens.

9. On the Enter User Name and Password dialog, specify the User Name and Password for the CA ARCserve Backup server, click the Apply [User Name and Password] to All Rows check box to apply the user name and passwords specified to all sessions.

Note: When you are editing IP addresses and passwords, you must edit the individual IP address and session password for each individual session.

Click OK.

The Enter User Name and Password dialog closes.

10. Click OK to close the Session User Name and Password dialog.

Note: After you click OK, a message box labeled CA ARCserve Backup may open and prompt you to specify the IP addresses for the sessions that require authentication to submit the restore job. If the CA ARCserve Backup dialog opens, you must specify all the IP address for all sessions to submit the job, and then click OK.

The restore job is submitted.

11. When the restore job is complete, restart the computer.

Be aware of the following behavior:

- When you log in to the operating system, you may receive an error message asking why the computer was unexpectedly shut down. This is expected behavior caused by the System State Recovery. If needed, you should select the appropriate response from the drop-down list and continue.
- You may also see the message, "At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details." In addition, the service SQL Server (ARCSERVE_DB) cannot start, thus resulting in the error. This is normal behavior because the SQL Server service does not recover during this step. This error will be corrected when you complete the steps in the section Recover the CA ARCserve Backup database.

12. After the computer restarts, the SQL Server service (ARCSERVE_DB) will not start. Access the current Microsoft SQL 2005 Express Edition instance data directory. By default, the instance is located in the following directory:

32-bit platforms

c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data

64-bit platforms

c:\Program Files\Microsoft SQL Server(x86)\MSSQL.1\MSSQL\Data

Note: If there are other instances of Microsoft SQL Server or Microsoft SQL Express on the same machine, this directory may vary from above path. To find the correct folder containing the CA ARCserve Backup database, go to the Windows Services manager and double-click SQL Server (ARCSERVE_DB) to open its properties. The Path to Executable field specifies the location of the service program.

13. Right-click the Data folder and select Properties from the pop-up menu.

The Properties dialog opens.

14. Click the Security tab and then click Advanced.

The Advanced Security Settings for Data opens.

Note: On Windows Server 2008 systems, click Edit on the Data Security Detailed Settings screen.

15. Click the Permissions tab and select the Replace permission entries on all child objects shown here that apply to child objects option and click OK.

Note: On Windows Server 2008 systems, click the Replace the existing inheritable permissions on all descendants with inheritable permissions from this object option.

If the CA ARCserve Backup Database is configured such that the database data files are stored in a different directory, repeat Steps 9, 10, and 11 on this folder to change its security attributes.

16. Open the Windows Services Manager and start the SQL Server service (ARCSERVE_DB).
17. Do one of the following:
 - If the SQL Server service is started, continue to the next task, **To recover the CA ARCserve Backup database**.
 - If the SQL Server service is not started and you cannot start the SQL Server service, continue to the next step
18. Open the Windows Computer Management Console, click Local Users, and then click Groups.

The following group name should appear:

```
SQLServer2005MSSQLUser$MACHINENAME$ARCSERVE_DB
```

Note: The value of MACHINENAME should be the name of your computer.

19. Record this Group name.

Return to the Data folder (see Step 8).

Right-click the Data folder and select Properties from the pop-up menu.

The Properties dialog opens.
20. Click the Security tab and then click Add.

The Select Users, Computer, and Groups dialog opens.
21. Click Locations and then click Local Machine.

Add the Group that you recorded in step 14 and click OK.

The Select Users, Computer, and Groups dialog closes.
22. Click the Advanced tab and then click the Permissions tab.

Select the Replace permission entries on all child objects shown here that apply to child objects option and click OK.

Note: If the CA ARCserve Backup database is configured such that the database data files are stored in a different directory, repeat Steps 8 to 11 on this folder to change its security attributes.
23. Open the Windows Services Manager and start the SQL Server service (ARCSERVE_DB).

To recover the CA ARCserve Backup database

Important! CA ARCserve Backup will not be available until you recover the database. Error messages may appear in the CA ARCserve Backup Activity Log that you can ignore.

1. Open the Windows Services Manager and start the CA ARCserve Database Engine service.

2. Open the Restore Manager.

From the restore methods drop-down list, select Restore by Session.

Locate and select the CA ARCserve Backup Database session as the restore source.

Click the Destination tab and ensure that the Restore files to their original location(s) option is selected.

Note: If the CA ARCserve Backup database you are recovering is stored in an independent local SQL Server instance, you should select the "master" database to restore before restoring the CA ARCserve Backup "asdb."

3. Open the Restore Options by clicking Options on the toolbar.

Click the Operation tab, select the Disable Database Recording option, and click OK.

The Options dialog closes.

4. Right-click the ARCserve Database session and select Agent Option from the pop-up menu.

5. Click the Restore Options tab, select the Force Restore over existing option, and click OK.

Note: If you do not choose this option, the restore job may fail, and the Database Engine will not start. For troubleshooting assistance, see the steps under the section To Reactivate the existing CA ARCserve Backup database.

6. Click Start on the toolbar to submit the restore job.

Note: After you click Start on the toolbar to submit the restore job, you must specify a user name and password on the DBAgent tab on the Session User Name and Password dialog.

During the restore process, the Database Engine service may pause or stop and the Manager Console may respond slowly. Since the Database Engine is unavailable during the recovery process, clients cannot connect to it. Therefore, Error E1516 [Staging] may be recorded in the Activity Log: "Cannot inquiry the database (Error=4294967293)." This behavior is normal during the database recovery process.

After the restore job completes successfully, the Database Engine will automatically resume and CA ARCserve Backup will return to normal operations.

To reactivate the existing CA ARCserve Backup database

This is an optional task. If the restore job fails because the correct options were not selected in the previous steps, the database may have been in an offline state while the restore job was in progress. As a result, the Database Engine could not access the CA ARCserve Backup database during the restore. The following steps describe how to reactivate the CA ARCserve Backup database.

1. Browse to the CA ARCserve Backup Home directory and locate `asdbe_start.bat`.
2. Execute `asdbe_start.bat`.

Note: The script uses a Microsoft SQL CLI utility "sqlcmd" to run a series of commands that will bring the CA ARCserve Backup database online.

After you execute the script, the Database Engine service resumes.

3. Repeat the steps in the section To recover the CA ARCserve Backup database.

Note: Ensure that you specify the Disable Database Recording and Force Restore over existing options before you start the job.

To Recover the Job Queue Session

1. After the CA ARCserve Backup server starts, open the Restore Manager, locate, and select the Job Queue session.

Note: When you select this session, CA ARCserve Backup requires a merge job of the Job Queue session.

Click Yes to continue the recovery of the Job Queue session.

2. From the Destination tab, specify an alternate location to restore the Job Queue session.
3. Click Start on the toolbar to submit the job to restore the Job Queue session to an alternate location.

Note: Ensure that the alternate location is an empty directory.

4. After the Job Queue session is restored to the alternate location, open the Server Admin and do the following:
 - a. Locate the CA ARCserve Backup primary server or stand-alone server.
 - b. Right-click the CA ARCserve Backup server and select Stop all services from the pop-up menu.

All CA ARCserve Backup services stop.

5. Access the alternate location and copy all Job Queue files under the folder that you restored to the following directory:
`ARCSERVE_HOME\00000001.qsd`

6. From the Server Admin, restart all CA ARCserve Backup services by doing the following:
 - a. Locate the CA ARCserve Backup primary server or stand-alone server.
 - b. Right-click the CA ARCserve Backup server and select Start all services from the pop-up menu.

All CA ARCserve Backup services start.

Note: The status of the backup job that you used for restoration is in a "crashed" state. When the Job Queue was backed up, that job was in an active state, but the corresponding process was not running. Therefore, that job is now in a crashed state and error message E1311 is written to the Activity Log: Job has crashed. This behavior is normal while the Job Queue is being restored.

7. If the CA ARCserve Backup is not a domain controller, go to the section, **Confirm CA ARCserve Backup product licenses**. Otherwise, continue to **Recover the Active Directory**.

Recover the Active Directory

1. Re-start the system.

After the system restarts, press F8.

The Advanced Option Menu appears.

2. Select Directory Service Restore Mode and start the system in the Restore mode.

Start CA ARCserve Backup.

Error message E3073 occurs:

Unable to logon as user, user =Administrator,EC=Logon Failure or W3073 Unable to logon as user, user =Administrator,EC=Logon Failure

3. Open the Restore Manager and select the Source tab.

From the Restore methods drop-down list, select Restore by Session.

Locate and select the System State session.

Do one of the following:

- To perform a **Non-authoritative Restore**, go to Step 5.
- To perform an **Authoritative Restore**, right-click the System State session and select Local Options from the pop-up menu.

The System State Restore Options dialog opens.

Continue to Step 4.

4. On the System State Restore Options dialog, click Make the Restored Copy of the Active Directory Authoritative and click OK.

5. Click Options on the Toolbar.
The Global Options dialog opens.
6. Click the Operation tab.
Click Restore Registry Files and Event logs and click OK.
The Global Options are applied.
7. Click Start on the toolbar to submit the restore job.
After the restore job is complete, restart the system.

Note: To restore the active directory data in Authoritative mode, CA ARCserve Backup executes NTDSUTIL.exe on the CA ARCserve Backup server. However, NTDSUTIL.exe executes asynchronously with the restore job and may not complete at the same time as the restore job. If this behavior occurs, restart the system after NTDSUTIL.exe completes. To ensure that NTDSUTIL.exe is complete, open Windows Task Manager, click Processes, and search for NTDSUTIL.exe. If NTDSUTIL.exe does not appear in the Windows Task Manager, NTDSUTIL.exe is complete and you can restart the system.

Confirm CA ARCserve Backup product licenses

You should confirm the product license after full restore is complete. The current CA ARCserve Backup license is restored back to the original state when you perform a full backup. If you have applied new licenses after a full backup, or the licenses were dynamically assigned to other servers, it is possible to encounter license errors. You should register or adjust product licenses accordingly.

Error Messages

After you recover the CA ARCserve Backup server, you may discover errors, warnings, and failure audits in the system Event Log similar to the error messages listed below, depending on how your system is configured. Such messages are caused by the intermediate state of recovery, or are related to the startup order in which CA ARCserve Backup and the SQL Server services started.

CA ARCserve Backup may report the following errors during the intermediate state of recovery.

Error 8355

This error message is reported when a "service broker" disabled setting is detected in the MSDB that was recovered. You can safely ignore this error because this is the default behavior of a system database recovery that is limited to SQL Server 2005 Express Edition. SQL Server 2000 and SQL Server 2005 are not affected by this behavior.

You can suppress this error by doing the following:

1. Open a Windows Command Line window.
2. Connect to the CA ARCserve Backup database (ARCSERVE_DB) by executing the following sqlcmd:

```
SQLcmd -S <machine name>\<Instance name>
```

For example:

```
C:\Users\Administrator>sqlcmd -S localhost\ARCSERVE_DB
```

3. Confirm the value of service_broker on msdb is 0:

```
select name,is_broker_enabled from sys.databases  
go
```
4. Execute the command using the following arguments:

```
alter database msdb set enable_broker  
go
```
5. Confirm the value of service_broker on msdb is 1:

```
select name,is_broker_enabled from sys.databases  
go  
Quit
```

Close the Command Line window.

CA ARCserve Backup corrects the following error conditions after the recovery process is complete:

Error 615

This error message is reported when the 'master' database is restored during recovery without using the CA ARCserve Backup Disaster Recovery Option and SQL Server is hosting a single CA ARCserve Backup database. This error may not occur when SQL Server 2005 Express Edition hosts the CA ARCserve Backup database.

The CA ARCserve Backup Agent for Microsoft SQL Server will not back up the tempdb database even when a full instance is selected. Tempdb is also excluded by the CA ARCserve Backup server and file system agent when the normal file system is backed up. However, tempdb is recorded as an existing database in the SQL Server master database, so when the master is restored, the SQL Server service reports that it cannot find tempdb.

Error 15466

This error message is reported when the system state is restored during recovery without using the CA ARCserve Backup Disaster Recovery Option. Either SQL Server 2005 Express Edition or SQL Server can host the CA ARCserve Backup database.

When you recover the CA ARCserve Backup server without using the Disaster Recovery Option, the Windows operating system and SQL Server are reinstalled, and the Service Master Key (SMK) of SQL Server is created. The Service Master Key (SMK) is used to encrypt all database master keys and all server-level secrets such as credential secrets or linked server login passwords.

The key is a 128-bit 3DES key. The SMK is encrypted using DPAPI and the service account credentials. When the system state is restored but SQL Server sessions have not yet been restored, the system state is overwritten by the restore operation. However, the SQL Server instance is not yet overwritten. The SMK is in the system state, so it has been recovered to the old one, which is therefore inconsistent with the SQL Server instance. At this time, the recovery procedure requires that you restart the operating system.

During the restart, SQL Server reads the SMK and checks it against the SQL database. Since the SMK and SQL Server database are inconsistent, the error occurs.

Error 17113

This error message is reported when the user permission settings for either the file or its containing folders are incorrect. Using the procedures described in this topic, you will adjust these permissions. The error will be corrected after you adjust the permissions.

Errors not related to the recovery process

If the CA ARCserve Backup services and SQL Server services do not start in the proper sequences, SQL Server error messages may appear in the system log. This behavior is a known issue. For more information, see the readme file.

Restore BrightStor ARCserve Backup for Laptops & Desktops Data

Since CA ARCserve Backup backs up all the for Laptops & Desktops data on your BrightStor ARCserve Backup for Laptops & Desktops server, you can only restore your BrightStor ARCserve Backup for Laptops & Desktops data to a fresh installation of the BrightStor ARCserve Backup for Laptops & Desktops server.

To restore BrightStor ARCserve Backup for Laptops & Desktops data

1. Ensure that a fresh copy of the BrightStor ARCserve Backup for Laptops & Desktops server has been installed on the computer to which you are restoring the data.
2. Ensure that the BrightStor ARCserve Backup for Laptops & Desktops server is not running on the target computer. To do so:
 - a. From the Control Panel, select Administrative Tools, then Services.
 - b. Select the BrightStor ARCserve Backup for Laptops & Desktops service in the right-hand pane.
 - c. From the Action menu, select Stop.
3. Open the Restore Manager, select the Source tab, and select Restore by Session from the drop-down list.
4. Select the BrightStor ARCserve Backup for Laptops & Desktops backup session that you want to restore.
5. Click the Start toolbar button to submit the job.

Restore Migrated Files

To reclaim CA ARCserve Backup tapes that contain BrightStor ARCserve Backup for Laptops & Desktops data, administrators can force the restoration of BrightStor ARCserve Backup for Laptops & Desktops files, regardless of whether these files are expired.

Forcing the restore returns these files to the BrightStor ARCserve Backup for Laptops & Desktops server and frees the CA ARCserve Backup tape for use with other data. For information on how to force the restore of BrightStor ARCserve Backup for Laptops & Desktops files, see the online help.

Chapter 5: Customizing Jobs

This section contains the following topics:

[How You Can Customize Jobs](#) (see page 285)

[Rotation Schemes](#) (see page 287)

[How Job Filters Work](#) (see page 291)

[Schedule Custom Jobs](#) (see page 296)

[Custom Schedules](#) (see page 297)

[Tasks You Can Perform Using the Job Status Manager](#) (see page 298)

[How Save Node Information Works](#) (see page 315)

[How to Use the Job Scheduler Wizard to Schedule Jobs](#) (see page 322)

[Job Scripts](#) (see page 323)

[Job Templates](#) (see page 324)

[Windows-Powered NAS and Storage Server 2003 Device Configuration](#) (see page 325)

How You Can Customize Jobs

CA ARCserve Backup provides a number of methods to customize your jobs to suit your needs. This chapter discusses the following customization methods in further detail.

- **Rotation schedules** let you to define standard and consistent intervals at which to rotate and retire backup media.
- **Filters** allow you to select the files and directories to be included in, or excluded from, your backup and restore jobs, based on a wide variety of criteria.
- **Scheduling options** provide you with the ability to schedule your jobs to run immediately, later, or on a regular basis.
- The **Job Scheduler Wizard** is a powerful tool that allows you to quickly and easily schedule and submit any job that can be entered at the command line.
- The **Job Status Manager** is a graphical tool that helps you centrally manage CA ARCserve Backup servers enterprise-wide.
- **Job scripts** allow you to save the options, filters, and scheduling information you define for your job as a file, so you can re-use, copy, or efficiently resubmit jobs with these settings.
- **Job templates** let you use preconfigured settings to submit jobs on any machine running CA ARCserve Backup without having to repeat the set up detail tasks for each job. The job template copies your configured backup schedule settings to be used again in the future on any machine.

Dynamic Job Packaging

If you click the box next to an item and the box turns completely green, this item is packaged dynamically. Dynamic job packaging means that the content of your selection is determined when the job runs. For example, if you choose to back up an entire server and the volumes listed on that server change between the time you scheduled the job and the time the job runs, the volumes from the time the job actually runs are backed up.

When you dynamically select a parent item, all of its associated (or child) items are automatically packaged dynamically as well.

Explicit Job Packaging

If you click the box next to a child item and its parent's box appears half green, the parent item is packaged explicitly. If you explicitly select the entire server, the volumes included in the backup are determined at the time the job is packaged. Explicit job packaging means that, in a parent object, you select only certain child items to include in your job. As a result, the content of what is packaged from the parent item is determined when you schedule the job rather than when the job runs.

When a parent item is explicitly selected, it applies only to its child items (the level that immediately follows). It does not apply to any selection you may make in the child items (for example, if you choose to back up only certain files within your child items).

For example, if you back up only the C and E drives on your server, the server is explicitly packaged. If you add another drive to your server between the time you scheduled your job and the time it runs, the new drive is not included in this job. In contrast, if you dynamically back up your C and E drives, any changes to the contents of these drives between the time you scheduled your job and the time it runs are included in the job when the job actually runs.

Explicit job packaging is beneficial because it gives you the power to customize local backup options per volume. For example, if you back up the C and E drives on your server, you can select the option Compress Files before Backup on the C drive and the option Encrypt Files before Backup on your E drive.

Note: To customize volume or database options, a parent item must be explicitly selected.

Rotation Schemes

This section describes how to configure a rotation scheme for a backup job by using the CA ARCserve Backup default scheme or by specifying your own rotation parameters. To access the parameters for configuring a rotation scheme, select the Schedule tab in the CA ARCserve Backup Manager. The parameters that you can use are described below.

- **Scheme Name**--Select the type of rotation scheme you want, based on 5 or 7 days, and incremental, differential, or full backups. For more information on these standard schemes, see [Calendar View Tab](#) (see page 290) to modify your rotation scheme.
- **Start Date**--The date the backup will start.
- **Execution Time**--The time the backup will start.
- **Enable GFS**--CA ARCserve Backup allows you to select from pre-defined Grandfather-Father-Son (GFS) rotation schemes consisting of full weekly backup jobs combined with daily incremental and differential jobs. The GFS strategy is a method of maintaining backups on a daily, weekly, and monthly basis.

Accessible from the Backup Manager, the primary purpose of the GFS scheme is to suggest a minimum standard and consistent interval to rotate and retire the media. The daily backups are the Son. The last full backup in the week (the weekly backup) is the Father. The last full backup of the month (the monthly backup) is the Grandfather. GFS rotation schemes allow you to back up your servers for an entire year using a minimum of media.

GFS backup schemes are based on a five or seven-day weekly schedule beginning any day. A full backup is performed at least once a week. On all other days, full, partial, or no backups are performed. Using GFS rotation, you can restore data reliably for any day of the week by using the weekly full backup in conjunction with the daily incremental or differential backup jobs.

Note: A five-day GFS rotation scheme requires 21 media-per-year, while a seven-day scheme requires 23 media-per-year.

Although GFS rotation schemes are predefined, you can modify these schemes to suit your individual needs. You can deviate from your standard rotation scheme (for instance, if a holiday falls on Wednesday, your usual backup day).

- **Append Media**--If you specify the Enable GFS option, you can direct CA ARCserve Backup allow data from GFS rotation to append to existing jobs on the media.

- **Daily Backup Method**--The Daily Backup Method option lets you specify one of the following options for your daily backup jobs:
 - **Full**--All source files are backed up. This backup method clears the archive bit.
 - **Incremental**--Files that have changed since the last backup are backed up. This backup method clears the archive bit.
 - **Differential - Archive Bit**--Files that have changed since the last full backup job are backed up. This backup method does not change the archive bit.
- **Use WORM Media**--The Use WORM Media option lets you direct CA ARCserve Backup to use WORM media for all rotation rules. With this option enabled, you have the capability to use WORM media for daily, weekly, and monthly GFS backup jobs.

Important! CA ARCserve Backup does not support the use of WORM media for multiplexing and multistreaming backup jobs. As a result, when you enable the Multiplexing option or the Multistreaming option on the Destination tab of the Backup Manager, the Use WORM Media option is disabled.

More information:

[Calendar View Tab](#) (see page 290)

How You Can Manage GFS Rotation Jobs on File System Devices

CA ARCserve Backup supports using a GFS rotation scheme on File System Devices. A retention period for the media being used in the GFS rotation scheme can be determined using the following default retention cycle for a seven-day weekly rotation:

Frequency	Number of Media
Daily	6
Weekly	5
Monthly	12
Total	23

To run a rotation job beyond a year, a GFS rotation scheme requires 23 File System Devices to be created. These settings can be modified to meet your specific needs. Modifying the default values of the GFS rotation may change the number of FSDs required.

Note: Previously, only local disks were considered FSDs. You can now create FSDs that are accessible through a network share using a Universal Naming Convention (UNC) path.

Because a GFS rotation job may be using local disk drives and drive arrays, users must first make sure that there is enough space on the particular file system to store all the data being backed up for the entire retention period. Creating file system devices on a boot partition is not recommended because a boot disk that becomes full can cause the operating system to function abnormally.

Note: All file system devices need to be assigned to the same device group.

For more information on configuring a device group to be used by the GFS rotation scheme, or on how to set up a GFS rotation job, see the online help.

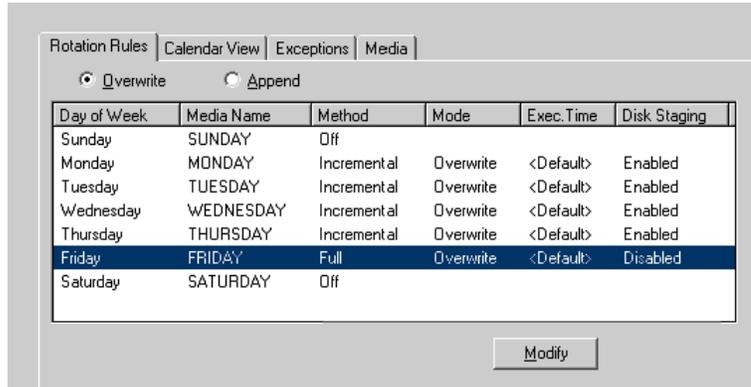
A configured GFS rotation job can run on a daily basis at a specified time. CA ARCserve Backup utilizes file system devices similar to a physical tape. As needed on a daily basis, CA ARCserve Backup moves tapes between the save sets and the scratch sets in the media pools, formats blank media, overwrites expired media, and tracks all operations in the database.

You can choose to duplicate backup data stored on the file system devices to physical tape media. The Job Scheduler Wizard and the Tapecopy utility provide the ability to automate the creation of the duplicate images.

The following sections describe the tabs available to customize your rotation job.

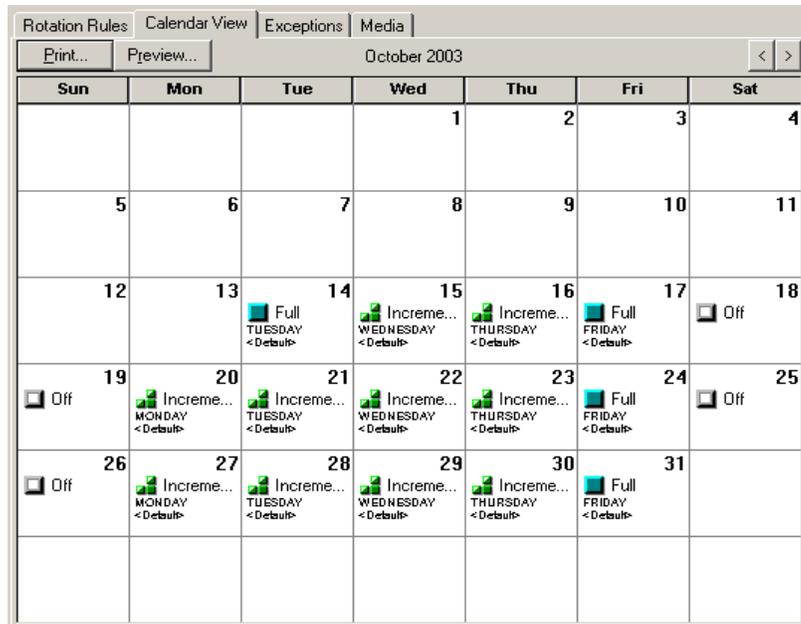
Rotation Rules Tab

You can modify the backup method or execution time for each day of the week.



Calendar View Tab

You can customize individual days. With GFS rotation either enabled or disabled, you can use the Calendar View feature to customize your rotation scheme according to the types of backups you want for particular days of the week or month, based on the calendar.



Note: This feature enables you to specify exceptions to the standard rotation scheme you are using.

Exceptions Tab

Define particular days on which the back up method and the execution time or date differs from the pre-existing schemes.

Media Tab

View information about the media pool you selected, including name, base serial number, next serial number, serial number range, minimum number of media, retention time, and prune retention time. You can also click the Daily, Weekly, or Monthly boxes to change the number of required media per year.

Media Pool Information		Preserve Media	
Pool Name	[Dropdown]	Daily	4
Base Serial Number	[Text]	Weekly	5
Next Serial Number	[Text]	Monthly	12
Serial Number Range	[Text]	Total Media	21
Min. # of Media	[Text]		
Retention Time (days)	[Text]		
Prune Retention Time (days)	[Text]		

Media Pool Specification

Specify a (non-shared) media pool to the rotation scheme. If necessary, you can append data to media and change the media name.

Backup Method Options

A combination of three different backup methods is available: full, differential, and incremental. See the section "Custom Schedules" in this chapter for detailed information about each of these methods.

How Job Filters Work

Filters allow you to include or exclude files and directories from your backup and restore jobs, as well as from the utilities, such as Copy, Count, and Purge.

For backup jobs, filtering can be performed on a per node basis. This means you can include a directory from one node and exclude the same directory from another node. A backup job can have node-level (local) and job-level (global) filters for the same job. Node-level filters apply to one specific node, not the entire job. If you want to add a filter that applies to the entire job, use a job-level, or global, filter. If you specify local (node-level) filters and global (job-level) filters for a backup job, CA ARCserve Backup applies the local filters and disregards the global filters.

You can include or exclude files based on the following criteria:

- Specific file names, patterns, attributes, and size.
- Specific directory names or patterns.
- Files accessed, modified, and created before, after, between, or within a specific date range.

CA ARCserve Backup uses wildcards or substitute characters, except when it detects that an absolute path is specified. If a valid absolute path is specified, CA ARCserve Backup will only exclude (or include) the absolute path specified, rather than excluding (or including) more directories, as it would for regular expression.

The wildcard characters supported for job filters based on file name or directory name are as follows:

- "*" --Use the asterisk to substitute zero or more characters in a file or directory name.
- "?" --Use the question mark to substitute a single character in a file or directory name.

Important! Exercise caution when specifying filters for your backup or restore operation. Incorrectly applied filters may not back up or restore the data you need, and can result in lost data and wasted time.

Examples: Back Up Data Using Wildcards

The following table describes examples of how you can use wildcards in conjunction with filters to back up data.

Note: The following examples assume that the source data resides in drive C:\.

Filter	Type and Criteria	Results
File	Include *.doc	CA ARCserve Backup backs up all files residing in drive C:\ that contain a .doc file extension.

Filter	Type and Criteria	Results
File	Exclude *.doc	CA ARCserve Backup backs up all files residing in drive C:\ that do not contain a .doc file extension.
File	Include ?.doc	CA ARCserve Backup backs up files that contain a single character file name and a .doc file extension. For example, a.doc, b.doc, 1.doc, 2.doc, and so on.
File	Include C:\myFolder\CA*.exe and Include C:\test\ms*.dll	CA ARCserve Backup backs up all of the following files: <ul style="list-style-type: none"> ■ Files residing in C:\myFolder that start with CA and contain an .exe file extension. ■ Files residing in C:\test that start with ms and contain a .dll file extension.
File	Exclude/Include C:\DOC\C*	CA ARCserve Backup restores all the files backed up in the 'C:\DOC\' folder except the files starting with 'C.'
Director y	Include m*t	CA ARCserve Backup backs up all directories residing in drive C:\ with directory names that start with m and end with t.
Director y	Exclude win*	CA ARCserve Backup backs up all directories residing in drive C:\ except directories that start with win.
Director y	Exclude C:\test\m* and Include C:\test\media*.gif	CA ARCserve Backup does not back up data. In this example, the exclude filter criteria directs CA ARCserve Backup to exclude all directories that reside in C:\test that start with m. As such, C:\test\media is excluded from the backup. Although the include filter directs CA ARCserve Backup to back up all files that reside in C:\test\media and contain a .gif file extension, CA ARCserve Backup will not back up any files because C:\test\media is excluded from the backup. Note: When you combine include filters with exclude filters, CA ARCserve Backup filters data based on

Filter	Type and Criteria	Results
		exclude criteria first, and then by include criteria.

Filter Options

You can access the filter options from the Backup Manager, Restore Manager, Copy, Count, Scan, Compare, and Purge Utility windows.

- **Exclude filters**--Exclusions always take precedence over inclusions. For example, if you add a filter to include files that have an .exe extension, and you add another filter to exclude your \SYSTEM directory, all .exe files in the \SYSTEM directory are excluded.
- **Include filters**--Results contain only those files that satisfy the filter specifications. For example, suppose you selected to back up your entire local hard drive, and you then set up a filter to include files in the \SYSTEM directory. The result would be that CA ARCserve Backup would only back up files from your \SYSTEM directory. No other files would be backed up.

Types of Filters

Filters are available which enable you to include and exclude files to suit your needs. For more information about how to apply filters, see the online help.

- **File Pattern Filter**--Use the File Pattern filter to include or exclude files from a job. You can specify a particular file name or you can use wildcards to specify a file pattern.

Note: Wildcards "*" (asterisk) and "?" (question mark) can be used in the file pattern filter.
- **Directory Pattern Filter**--Use the Directory filter to include or exclude specific directories from a job. You can enter an entire directory name or you can use wildcards to specify a directory pattern.

Note: Wildcards "*" (asterisk) and "?" (question mark) can be used in the directory pattern filter
- **File Attributes Filter**--Use the File Attributes filter to include or exclude specific types of files from a job. Select as many of the following types of file attributes as you want:
 - **Hidden**--Files not shown in a directory listing. For example, IO.SYS is a hidden file.
 - **System**--Files that are unique to the machine you are using.
 - **Archive**--Files whose archive bit is set.
 - **Read Only**--Files that cannot be modified.

- **File Modified Filters**--Use the files last modified attribute to include or exclude files, based on the time they were last changed. There are four options from which to choose:
 - **Before**--Files whose date matches, or whose date is earlier than this date, are included or excluded.
 - **After**--Files whose date matches, or whose date is later than this date, are included or excluded.
 - **Between**--Files whose date falls between the two dates are included or excluded from the job. You must specify two dates for this selection.
 - **Within**--Files whose date falls within the specified time are included or excluded from the job. You must specify the number of days, months, or years.

- **File Created Filters**--Use the files last created attribute to include or exclude files based on when they were created. There are four options from which to choose:
 - **Before**--Files whose date matches, or whose date is earlier than, this date is included or excluded.
 - **After**--Files whose date matches, or whose date is later than, this date is included or excluded.
 - **Between**--Files whose date falls between the two dates are included or excluded from the job. You must specify two dates for this selection.
 - **Within**--Files whose date falls within the specified time are included or excluded from the job. You must specify the number of days, months, or years.

- **File Accessed Filters**--Use the file last accessed attribute to include or exclude files based on when they were last accessed. There are four options from which to choose:
 - **Before**--Files whose date matches, or whose date is earlier than, this date is included or excluded.
 - **After**--Files whose date matches, or whose date is later than, this date is included or excluded.
 - **Between**--Files whose date falls between the two dates are included or excluded from the job. You must specify two dates for this selection.
 - **Within**--Files whose date falls within the specified time are included or excluded from the job. You must specify the number of days, months, or years.

- **File Size Filters**--Use the file size attribute to include or exclude files based on the specific size of the file. You can specify a size range from 0 to 9999999999 bytes, KB, MB, or GB. There are four options from which to choose:
 - **Equal to**--Files whose size matches the size range are included or excluded from the job.
 - **Greater than**--Files whose size matches or whose size is greater than the size range are included or excluded from the job.
 - **Less than**--Files whose size matches or whose size is less than the size range are included or excluded from the job.
 - **Between**--Files whose size falls between the two sizes are included or excluded from the job.
- **NDS Context & Object**--Lets you include or exclude certain NDS objects (NetWare Administrators and Directory Services) from your job.

Schedule Custom Jobs

All jobs can all be scheduled using the Schedule options available in each Manager. Jobs can be submitted with a repeat method. For information about repeat methods, see Rotation Schemes or Custom Schedules in this chapter.

If you select the Run Job Now option when your storage device is busy, CA ARCserve Backup reports that the storage device is busy and the job is not submitted to the Job Queue. You should schedule your job, keeping the current date and time. This way, when CA ARCserve Backup discovers that the storage device is busy, it automatically retries the job until the drive becomes free.

You should select the Run Job Now option when:

- The job you are submitting is a one time only job that you want executed immediately.
- You want to monitor the job as it runs.

You should schedule your job when:

- You are submitting a single occurrence job but and you want it to run at a specific time.
- You are submitting a single occurrence job, but you do not want to run it now. You want to submit the job on Hold, and start it manually at a later time.
- You are submitting a job that should run regularly. This is especially useful for setting up a media rotation scheme for your network.
- Your storage device is busy and you want to run a backup job as soon as the drive is free. To do this, schedule your backup job with the current date and time.

For details on how to specify a scheduling option, see the online help.

Important! All scheduled times for CA ARCserve Backup jobs are based upon the time zone where the CA ARCserve Backup server is located. If your agent machine is located in a different time zone than the CA ARCserve Backup server, you will need to calculate the equivalent local time that you want the job to be run.

Custom Schedules

You can select a custom schedule on the Schedule tab in the Backup Manager. A custom schedule enables you to run a backup job either once or on a repeating basis. You can specify the following parameter for a backup or restore job:

- **Repeat Method**--All jobs can be scheduled using the Schedule options available in each Manager. Jobs can be submitted with a repeat method of
 - **Once**--Do not repeat this job.
 - **Every n frequency**--Repeat this job every specified number of Minutes, Hours, Days, Weeks, or Months.
 - **Day(s) of the Week**--Repeat this job on the days that are checked off.
 - **Week(s) of the Month**--Repeat this job on the weeks that are checked off.
 - **Day of the Month**--Repeat this job on the specified day.
 - **Custom**--Repeat this at the specified interval, but exclude the days that are checked.

You can specify the following parameters for a backup job:

- **Backup Method**--This specifies what data will be backed up. Jobs can be submitted with a backup method of:
 - **Full (Keep Archive Bit)**--Performed each time the job is repeated and *keeps* the archive bit.
 - **Full (Clear Archive Bit)**--Performed each time the job is repeated and *clears* the archive bit.
 - **Incremental backup**--Backs up only those files whose archive bit have been set since the last full or incremental backup was performed. After each backup, archive bits are reset so that they are not backed up during the next incremental backup job.
 - **Differential backup**--Backs up only those files whose archive bits have been set since the last full backup was performed. Because differential backup jobs do not clear a file's archive bit, the files that were backed up in the last differential job are backed up again. Using this backup method, the backup jobs require more time to process than incremental backup jobs. However, this strategy requires less effort to restore servers and workstations because you will probably require fewer media to restore your machines.
- **Use WORM Media**--Directs CA ARCserve Backup to use WORM media when the backup job runs.

Tasks You Can Perform Using the Job Status Manager

The Job Status Manager is a graphical tool that helps you centrally manage CA ARCserve Backup servers across the enterprise.

You can use the Job Status Manager to:

- View all available CA ARCserve Backup servers, job history, job queues, and activity logs.
- Manage jobs--stop, add, run, delete, modify, reschedule jobs, and place jobs in a hold status.
- Monitor the progress of active jobs that are running on CA ARCserve Backup primary servers and member servers. You can view the real-time status of active jobs in the queue.
- View job detail and job log information about all the jobs that have been executed.
- View activity and media logs.
- Stop an active job.
- Modify user names and passwords associated with a job.
- Preflight Check the job.

Pop-up menus enable you to perform various operations with the Job Status Manager. These menus appear in both the left (server browser) and right (Job Queue) panels. To access a menu, right-click a selected item. When accessing a pop-up menu in the browser, the pointer must be on a selected group, server, or object. When accessing a pop-up menu in the Job Queue, a job must be selected.

Note: When you submit a job that spawns child jobs, the Job Queue tab displays details about the master job only. The Activity Log tab displays details about the master and child jobs. The Activity Log presents you with a description for the job.

Important! When you are executing a multistreaming, multiplexing, or disk staging job, the number of child jobs associated with a master job will never exceed the number streams specified for the job. However, if a job spawns multiple child jobs and the value specified for the Multiplexing Max # of Streams option is zero or one, the child jobs will be created and backed up in one continuous stream (the default Max # Stream is four).

More information:

[Preflight Checks for Your Backups](#) (see page 184)

Modify Pending Data Migration Jobs

Migration is the process of moving backup data from a temporary staging location (device or media) to final destination media.

A migration job is the CA ARCserve Backup task associated with migrating data, or copying data, from the staging location to the final destination media. The parameters for the migration job, such as the schedule, copy policies, and so on, are defined by the staging policies that you specified when you submitted the job.

To help you manage pending migration jobs, CA ARCserve Backup provides you with a tool called the Migration Job Status dialog. The Migration Job Status dialog displays a list of all backup sessions for a job in the Job Queue that are pending data migration. With the Migration Job Status tool you can reschedule migration and purge jobs, cancel migration jobs, and change the device group that contains the final destination media.

To modify pending data migration jobs

1. Open the Job Status Manager and select the Job Queue tab.

Job Name	Backup Se...	Job No.	Job ID	Status	Execution T...	Job Type	Last Result	MB Processed	Elapsed Time	MB/Minute
123 Data Migration Job	LIJY002-...	5	3	DONE	<Run Now>	Backup	Finished			
Data Migration Status	LIJY002-...	14	14	DONE	1/22/2009 ...	Migration	Finished			
221 Data Migration Job	LIJY002-...	7	15	DONE	1/22/2009 ...	Backup	Finished			
Data Migration Job	LIJY002-...	12	11	DONE	1/22/2009 ...	Migration	Finished			
Data Migration Job	LIJY002-...	16	17	DONE	1/22/2009 ...	Migration	Finished			
Data Migration Status	LIJY002-...									
333 Data Migration Job	LIJY002-...	9	9	DONE	<Run Now>	Backup	Finished			
Data Migration Job	LIJY002-...	13	12	DONE	1/22/2009 ...	Migration	Finished			
Data Migration Status	LIJY002-...									
Backup [Custom, Staging]	LIJY002-...	20	21	ACTIVE	Backup files...	Backup		0.00	3s	1.25
Data Migration Status	LIJY002-...									
Backup [Custom]	LIJY002-...	3	1	DONE	<Run Now>	Backup	Finished			
Database protection job	LIJY002-...	2		HOLD	1/22/2009 ...	Backup (Ro...				
Database pruning job	LIJY002-...	1	13	READY	1/23/2009 ...	DB Pruning	Finished			
eee	LIJY002-...	17	18	DONE	<Run Now>	Backup	Finished			

Locate the jobs with pending data migration jobs and click Data Migration Status.



The Migration Job Status <Backup Server Name> dialog opens as illustrated by the following screen.

No.	Backup Time	Copy Time	Purge Time	Num. of Sessions	Data Size(MB)	Status	Group Name	Tape Name
1	12/11/08 10:00 AM	12/11/08 1:01 PM	12/13/08 10:01 AM	1	290.04	Scheduled	PGRP1	*
2	12/11/08 12:00 PM	12/11/08 3:01 PM	12/13/08 12:01 PM	1	290.04	Scheduled	PGRP1	*

Note: The list doesn't display those sessions which have already been copied or were not supposed to be copied.
 * A Scheduled status indicates that the sessions have not been copied because the scheduled start times has not passed.
 ** A Pending status indicates that the sessions have not been copied although the scheduled start time has passed.

Buttons: Modify, OK, Cancel

2. Locate and click the sessions that you want to modify and click Modify.

The Migration Job Configuration dialog opens.

3. Specify the options that follow:

Copy Time

Lets you specify the date and time that you want to start the migration job.

Note: If you do not want to migrate the backup data to final destination media, clear the check box next to Do no copy data.

Purge Time

Lets you specify the date and time that you want to purge the backup data from the staging device.

Target

Lets you specify the group containing the final destination media.

Apply to the selected rows

If you selected more than one session on the Migration Job Status dialog, this option lets you apply the Copy Time, Purge Time, and Target options that you specified to all of the sessions selected on the Migration Job Status dialog.

4. Click OK.

More information:

[Back Up Data Using Disk Staging](#) (see page 215)

[Back Up Data Using Tape Staging](#) (see page 230)

[How to Reclaim Disk Space](#) (see page 223)

Update Multiple Jobs

In your CA ARCserve Backup environment, you can have several to many jobs listed in the Job Queue. If a situation arises where you need to change the READY or HOLD status on more than one job, you can update multiple jobs simultaneously. The updates that you can perform simultaneously include changing the job status from HOLD to READY, from READY to HOLD, and delete the job.

Note: When you select a job that contains child jobs, CA ARCserve Backup applies the update to the parent job and all of its child jobs.

To update multiple jobs

1. From the Job Status Manager, select the Job Queue tab.
2. Click to select the job that you want to update.
 - To select multiple adjacent jobs, press and hold the Shift key as you select the jobs.
 - To select multiple non-adjacent jobs, press and hold the Ctrl key as you select the jobs.
3. Right-click the selected jobs.
4. From the pop-up menu, select HOLD, READY, or Delete Job as warranted by the situation.

How to Manage Jobs Using the Job Queue Tab

The Job Queue tab on the right panel displays information about all jobs. Every time you run or schedule a job with the CA ARCserve Backup Manager, you submit it to the Job Queue. CA ARCserve Backup continuously scans the Job Queue for jobs that are waiting to execute. Select a job and right-click for the following options:

- **READY/HOLD**--Changes the job's status to HOLD or to READY (if it is currently on hold). HOLD signifies that the job is not scheduled to be executed, while READY means that the job can be executed.
- **Add Job**--You can quickly submit a job to the queue by using a previously saved script. (A script is a job that you saved to a file. It contains the original source, destination, option, and schedule information for the job.)
- **Modify Job**--Modifies a job. Allows you to add options or additional sources to an existing job, without having to create a new job.
- **Reschedule Job**--Quickly change a job's execution date, time, or status. It also allows you to resubmit a Done job that is still in the Job Queue. You may want to do this if your job was not successful when it first ran.

- **Run Now**--Available for jobs that have a Ready or Done status. This option is useful in the following scenarios:

- You want to run a job earlier than the time it is scheduled to run
- A scheduled job did not run because of a hardware problem and you want to run it immediately after the problem is fixed

If a device group is available, this option runs the job immediately. If you select Run Now and a device group is not available, the job stays in the queue and waits for a group to become available.

If you select the Run Now option for a repeating, rotation, or GFS rotation job, the following conditions apply:

- The job runs immediately and the existing schedule is not affected unless the time it takes to run the job overlaps with the next scheduled run. In this scenario, the scheduled run is skipped for that day. For example, if you have a job scheduled to run Monday through Friday at 9:00 p.m., you select Run Now at 6:00 p.m. and it does not finish till 10:00 p.m., the 9:00 p.m. scheduled run for that day is skipped.
- The backup method used for the job is the same backup method that will be used for the scheduled run that day. For example, if you have an incremental backup job scheduled for 9:00 p.m. and select Run Now at 6:00 p.m., the job that runs at 6:00 p.m. will be an incremental backup. If you select Run Now on a day that does **not** have a scheduled run, the backup method of the next scheduled job will be used. For example, if you have an incremental job scheduled to run Monday and you select Run Now on Saturday, the job that runs on Saturday will be an incremental backup.

- **Stop Job**--Cancels an active job from the CA ARCserve Backup queue and reschedules it for its next regular interval.

Note: If you stop a job, the Last Result field displays "Canceled."

- **Delete Job**--Cancels the job and deletes it from the CA ARCserve Backup queue completely.

You cannot use the Delete Job option on an active job. Use the Stop Job option if you want to delete an active job that repeats at intervals (determined when you create the job). Selecting the Delete Job button will interrupt and remove the job completely from the queue, and it will not be rescheduled. You will have to recreate the job if you did not save it to a script file.

For information about deleting the CA ARCserve Backup database pruning job, see the section "CA ARCserve Backup Database Pruning Jobs" in this chapter.

- **Modify User Name**--Modify the user name and password for server and source nodes.

- **Modify Encryption Password**--Modify the encryption password that was previously specified for a job.
- **Preflight Check**--Runs vital checks on the CA ARCserve Backup server and agents to detect conditions that may cause backup jobs to fail.
- **Sort By**--Jobs in the queue are listed in order of execution time. This option changes the order in which jobs are listed in the queue. Sorting the Job Queue is for informational purposes only. It does not affect the order in which jobs are processed. To sort jobs, click any of the following fields: Status, Execution Time, Job Type, Server, Last Result, Owner, Total Files, and Description.
Note: You can resize these columns by using the "drag and drop" method with the mouse. Place the cursor on the divider between columns, click and hold down the left mouse button, and then move the divider in either direction until the column is the size you want.
- **Properties**--Double-click to call up the Job Properties dialog when the job is processing.

For more information about using these menu options, see the online help.

Job Status Types

When a job is in the CA ARCserve Backup queue, it is listed with a status. The status can be one of the following:

Done

A no repeating job that was successfully executed and completed.

Ready

A new one-time or repeating job (a backup job that runs every Friday, for example) waiting to be executed.

Active

A job that is currently being executed.

Hold

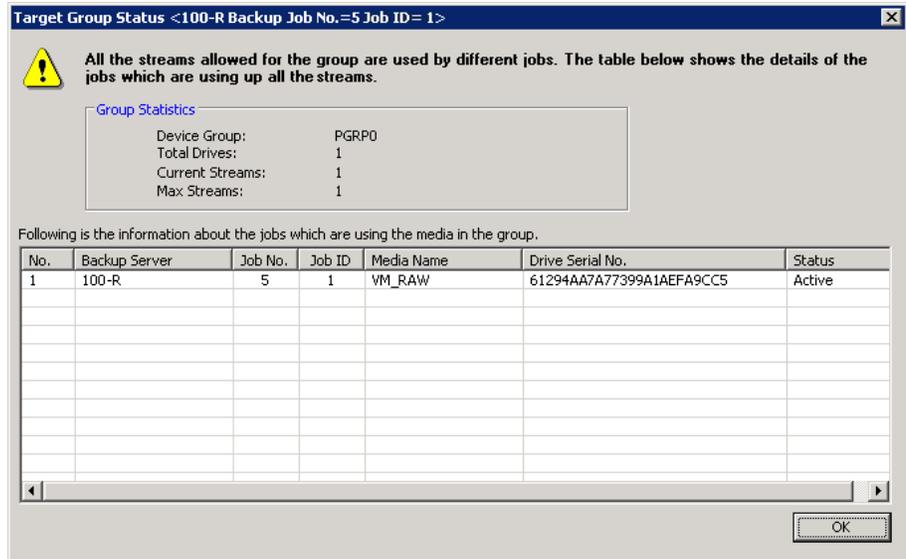
A job that is in the queue and was placed in a hold status.

Note: A job with a hold status will not execute until you remove the hold status.

Waiting for Target

A job that is ready to execute and is waiting for the target device, media, or both to become available. A device or media may not be available, for example, because it is busy with another job. To determine the specific reason why a job is waiting for a device, click the Waiting for Target hyperlink to open the Target Group Status dialog.

The Target Group Status dialog represents stream-based backups or device-based backups.



The Target Group Status dialog describes the information that follows:

- **Title bar**--Displays the name of the backup server, the job number, and the job ID of the job that you clicked in the Job Status Manager.
- The reason the job is waiting (for the device or media)
- **Group Statistics**--The Group Statistics field displays information about stream-based backups and device-based backups.

Stream-based Backups

- Device Group--The name of the target device group
- Total Drives--The number of drives included in the group
- Current Streams--The number of active streams in the group
- Max Streams--The number of active streams the group supports

Device-based Backups

- Device Group--The name of the target device group
- Total Drives--The number of drives included in the group
- Free Drives--The number of inactive drives in the group
- Reserved Drives--The number of drives in the group that are reserved for jobs

- **Backup Server**--The name of the backup server using the listed device
- **Job No.**--The job number that is using the listed device, if available
- **Job ID**--The job ID that is using the listed device, if available
- **Media Name**--The name of the media in the listed device, if available
- **Drive Serial No.**--The serial number of the listed device
- **Status**--The status of the job that is using the listed device

Waiting for source group

A migration job is waiting for a source group to be available.

Waiting for source tape

A migration job is waiting for the source tape to be available.

Waiting for target tape

A job that should be active, but it is not because it is waiting for the target device or media.

Positioning source tape

A migration job is waiting for the source tape to be positioned in the drive.

Positioning target tape

A migration job is waiting for the target tape to be positioned in the drive.

Copying

A migration job (copy to final destination media) is in progress.

Completed jobs remain listed in the Job Queue for a specified number of hours. This period of time is set up through the CA ARCserve Backup Server Admin. For more information, see Job Engine Configuration (see page 451).

More information:

[Job Engine Configuration](#) (see page 451)

How to Analyze Jobs Using the Last Result Field

The Last Result field on the Job History tab indicates whether your executed job was successful. If it was not successful, the information in this field helps you determine why the job may have failed. The Last Result field may contain the following one of the following statuses:

Finished

All of the nodes and drives and shares were processed.

Incomplete

The job was partially successful. Review the Activity log information to check the exact nature of what occurred to prevent job completion.

Canceled

The job was intentionally canceled. The following actions may have occurred:

- A user canceled the job from the Job Queue.
- Someone answered NO or CANCEL to a console prompt.
- The job required either a confirmation of OK, or media to be inserted before the time out was reached. (Time out is set in the media options in the Backup Manager window.)

Failed

The job failed to perform its designated task. This usually occurs if CA ARCserve Backup cannot back up any source nodes of a job (for example, if the agent is not loaded or an invalid password was entered) or if a hardware error occurs. If the job was started, but the Manager could not complete the job, you will receive "Run Failed" status. Review the Activity log information to check the exact nature of what occurred to prevent the job from completing.

Run Failed

The job was started, but the program that runs the job failed, because either there was not enough memory to run the job or a DLL file was not found.

Crashed

The job was started and a system error occurred which prevented CA ARCserve Backup from completing its task, such as a memory violation that caused CA ARCserve Backup or the operating system to be shut down. If a job has a status of Crashed, it can be retried after the Job Engine restarts. This can be set up through the CA ARCserve Backup Server Admin in the Job Engine Configuration tab.

Deleted CA ARCserve Backup Database Pruning Jobs

When you attempt to delete the CA ARCserve Backup database pruning job, a warning message opens. If you continue and delete a database pruning job, the following conditions apply:

- The job reconvenes the next time it is scheduled to run, if the CA ARCserve Backup database pruning job is scheduled to run daily. CA ARCserve Backup then prunes all records that were not pruned due to one or more deleted pruning jobs.
- Pruned records cannot be rolled back into the CA ARCserve Backup database.
- Use the CA ARCserve Backup Server Admin to restart the manually.

To submit the database pruning job manually

1. Start the CA ARCserve Backup Server Admin and click the Configuration toolbar button.

The Configuration dialog opens.

2. Select the Database Engine tab.
3. Check the Submit prune job option.

Note: The Submit prune job option is active only if the Database Pruning Job was deleted.

4. Click OK.

The database pruning job is submitted to the job queue and will run at the specified time.

View Job Details Using the Activity Log

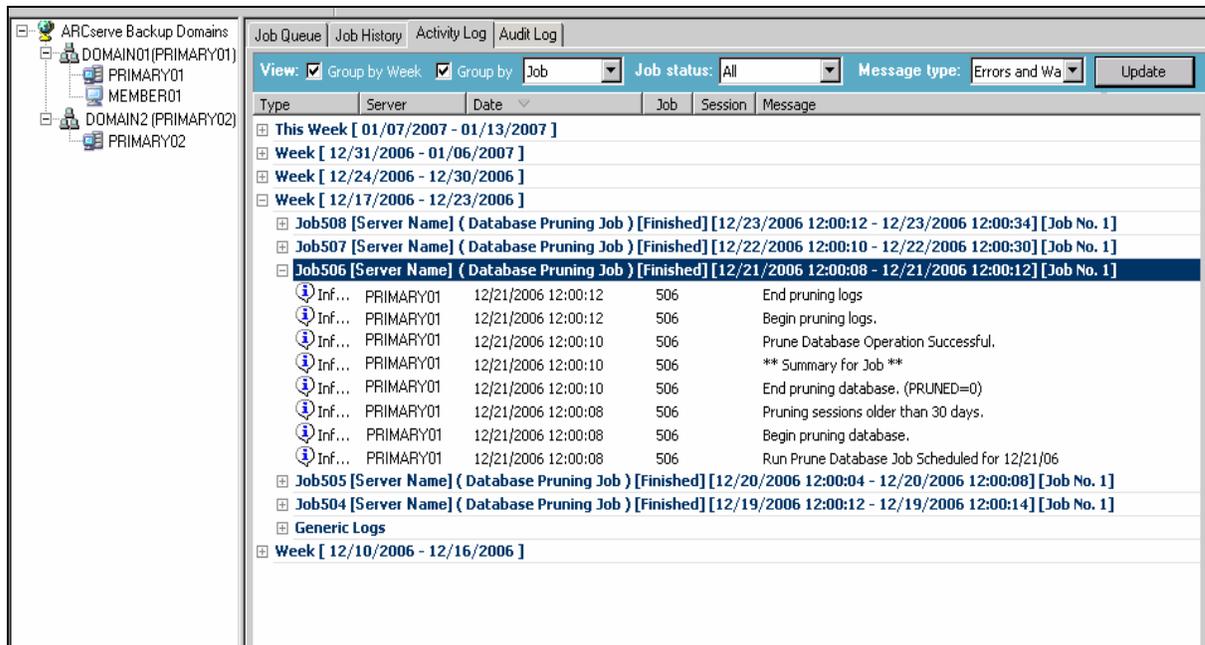
The Activity Log tab on the right panel contains comprehensive information about all the operations performed by CA ARCserve Backup.

The log provides an audit trail of every job that is run. For each job, the log includes the following information:

- Time the job started and ended
- Type of job
- Average throughput of the data
- Number of directories and files processed (backed up, restored, or copied)
- Job session number and job ID
- Result of the job
- Errors and warnings that occurred

When you install the Central Management Option, you can view Activity Log data as it relates to the domain primary server, a domain member server, or both.

The following diagram illustrates that the Central Management Option is installed, domain member server MEMBER01 is selected, and the activity log details for the MEMBER01 are displayed.



Group by Week (if checked) is always the first level group. The date comes from the operating system's setting.

The format for the week node is as follows:

Week[start date - end date]

The format for the job node is as follows:

JobID [Server Name](Job Name)[Job Status][Start time - End time][Job No.]

The Generic Log appears at the end of the master job list. It contains the logs that do not belong to any job.

Note: If you do not install the Central Management Option, the Activity Log displays data relating to the CA ARCserve Backup server that you are currently logged in to.

You can scan this log every day to see if any errors occurred. You can also use it to find a session number in case you need to restore a specific session. You can organize the Activity log view or print it to a file.

Delete Activity Log Files

To conserve file space, you can delete the entire Activity log file or unnecessary log records older than a specific time period.

To delete files in the Activity log

1. Open the Job Status Manager and select the Activity Log tab. Click the Delete toolbar button.

The Delete dialog opens.

2. Select the criteria you want to apply in the Delete dialog. Chose one of the following options:
 - **Entire Log**—Deletes all log file records.
 - **Partial**—Lets you select specific logs based on a time period. You can choose from the following criteria:
 - **days:** range 1-365
 - **weeks:** range 1-54
 - **months:** range 1-12
 - **years:** range 1-10

3. Click OK.
A caution dialog appears.
4. Click OK.
The Activity log files are deleted.

You can also use the command line interface to purge job logs (or any other log file) from the Activity log. Use the `ca_log -purge` command to delete logs older than a specified period of time from any log file. You can also use the `ca_log -clear` command if you want to delete all log data from log files with no specified time period.

Note: For more information about the `ca_log` command, see the *Command Line Reference Guide*.

Activity Log Pruning

To conserve file space, you can schedule log pruning.

More information:

[Database Engine Configuration](#) (see page 472)

Set Activity Log Queries

CA ARCserve Backup provides you with the capability to customize the type of information and how the information displays in the Activity Log.

The default activity log query values are as follows:

- View: Group by Week and Group by Job
- Job Status: All Message
- Type: All
- Date: All Time
- Job ID: blank
- Session: blank
- Keywords: Message

Note: To return to the default setting at any time click Reset.

To set Activity Log Queries

1. Open the Job Status Manager and select the Activity Log tab.
2. Expand the Log Query Bar. By default the Log Query Bar is collapsed.
The Log Query Bar opens.

3. Specify the desired options.

View

Specify how you want to group the activity log messages. You can group by week, type and job.

- The Group by Week lets you group the activity log messages by the week (default).
- The Group by Jobs option, lets you group the Activity Log with the parent job together with all of its child jobs. For each parent job and its corresponding child jobs, the Activity Log presents you with a description for the job (default).
- The Group by Type option lets you group error messages, warning messages, and information messages.

Job status

Specify the types of jobs that you want to view in the Activity Log. You can view All, Finished, All unsuccessful, Canceled, Failed, Incomplete, Crashed and Unknown.

Message type

Specify the types of messages that you want to view in the Activity Log.

You can view All, Error, Warnings, Errors and Warnings, Informations, Errors and Informations, and Warnings and Informations.

Date

Specify a date or range of dates of messages that you want to view in the Activity Log.

You can show all messages, filter messages such that only messages before or after a specified date display, or display a specific range of dates.

Job ID

Specify a know job ID.

Session

Specify a know session.

Keywords

Sort the activity log by keywords. You can specify Job Name or Message.

4. Click Update.

The Activity Log displays the results according to the specified query.

Note: To get the latest jobs, with the existing filters, click Refresh on the toolbar or F5.

Tape Log Tab

The Tape Log tab in the Job Status Manager displays if you enabled the option Show Tape Log on Job Status Manager while configuring the Tape Engine. For more information, see the section Tape Engine Configuration.

Note: After you enable the option "Show Tape Log on Job Status Manager," you must click Refresh in the Job Status Manager for the changes to take effect.

More information:

[Tape Engine Configuration](#) (see page 462)

Job Detail Tab

The Job Detail tab in the bottom panel displays details about any job in the queue, including the source and destination targets and the job's schedule. If you have selected customization options such as Pre/Post backup requirements, they will be displayed here. After a job has started, you can view its sequence and session number.

Job Log Tab

The Job Log tab in the bottom panel displays information about specific jobs that have been executed. It is generated for each job that CA ARCserve Backup runs. You can specify the level of detail in the log by choosing the Log options before you submit the job. For information on how to configure and view the log report for a job, see the online help.

CA ARCserve Backup provides the following log options:

- **Log All Activity**--Record all of the activity that occurs while the job is running.
- **Log Summary Only (default)**--Record summary information on the job (including source, destination, session number, and totals) and errors.
- **Log Disabled**--Do not record any information about this job.

How Save Node Information Works

Saving a node to the CA ARCserve Backup database makes it accessible to all users on the same domain. CA ARCserve Backup views the Primary Server, Member Servers, and all agents in a domain as nodes.

The Save Node Information feature lets you perform the following tasks:

- Save new nodes to the CA ARCserve Backup database
- Save the user account information to the CA ARCserve Backup database
- Filter nodes by agent type

How to Add, Import, and Export Nodes

Setting up a job in an environment with a lot of nodes and agents can be a time-consuming and tedious task. If you have multiple nodes and agents to be backed up, it may take time to add the nodes to the Backup Manager one at a time. The Add, Import, and Export Nodes feature lets you quickly and easily add multiple nodes and agents using the CA ARCserve Backup user interface, whether or not the nodes and agents will be backed up. You can use the Add, Import, and Export Nodes feature to add multiple nodes and agents into the system in either of the following ways:

Add multiple nodes and agents using the user interface

1. From the Backup Manager Source Tab or the Restore Manager Destination Tab select a node.
2. Use the Add/Import/Export Nodes dialog to manually enter the names of all the nodes and agents or select the nodes from the left-pane list of nodes and agents detected by auto-discovery.
3. Specify a user name and password for the nodes.
4. Save the information in the CA ARCserve Backup database.
5. View the nodes and agents in the Backup Manager Source tree.
6. (Optional) Export the current nodes and agents to a .csv file.

Note: A .csv file is a comma separated value file format.

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

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

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

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

More information:

[Add, Import, and Export Nodes Using the User Interface](#) (see page 316)

[Add Multiple Nodes and Agents Using a .csv and .txt File](#) (see page 319)

[Export Multiple Machines to a Text File](#) (see page 320)

Add, Import, and Export Nodes Using the User Interface

The Add, Import, and Export Nodes feature lets you quickly and easily add multiple nodes and agents using the CA ARCserve Backup user interface, whether or not the nodes and agents will be backed up.

To add, import, and export nodes using the user interface

1. Open the Backup Manager and select the Source tab.
2. Right-click the Windows Systems object in the browser and select Add/Import/Export Nodes from the pop-up menu.

(Optional) From the Properties frame, click Add/Import/Export Nodes.



The Add/Import/Export Nodes dialog opens and any existing nodes and agents are added to the list of agents which will be added to the Source tree as viewed in the right-pane.

3. Add the nodes and agents to the list in the right-pane, which will be added to the Source tree on the user interface. This can be done in the following ways:

- Specify the host name or host name (IP address) of the nodes and agents that you want to add in the text box and click Add.

The best practice is to specify the host name and the IP address of the target system. This approach ensures that CA ARCserve Backup can accurately detect the target system, based on its IP address, and display the system under the Windows Systems object.

Note: If you specify only the host name, CA ARCserve Backup sets the IP address value to 0.0.0.0.

- Select those nodes and agents from the list of nodes and agents detected by auto-discovery in the left-pane and click Add or Add All.

You can select multiple nodes and agents using the CTRL or Shift key. The nodes and agents are removed from the left-pane list after they have been added to the right-pane list.

- Click Import to add a list of nodes and agents using a .csv or .txt file.

Example: .txt file:

```
Hoatname1(IP)
Hostname2(IP)
Hostname3(IP)
Hostname4(IP)
```

Example: .csv file:

```
Hostname1(IP), Hostname2(IP), Hostname3(IP), Hostname4(IP), ...
```

Note: For more information, see [Add Multiple Nodes and Agents Using a .csv or .txt File](#) (see page 319).

The nodes and agents that will be added to the Backup Manager Source tree are displayed in the right-pane list.

4. (Optional) Click Delete or Delete All if necessary to remove items from the right-pane list.

The Delete and Delete All buttons are only enabled if you select a node or multiple nodes in the right-pane list. If the node was originally entered in the text box or imported from a .csv or .txt file, and you click Delete, the nodes will be removed from the right-pane list. If the node or agent was detected by auto-discovery, and you click Delete, the nodes or agents display in the left-pane list of nodes and agents detected by auto-discovery.

5. Select the nodes and agents in the right-pane list you want to enter a user name and password for and then click Security.

(Optional) From the list of nodes and agents that will be added to the Source directory tree, double-click the Host name or Address value of the target system.

The Security dialog opens where you can add the user name and password for multiple nodes and agents at one time. The nodes and agents displayed on the Security dialog are provided from the right-pane list on the Add/Import/Export Nodes dialog.

6. Enter the user name and password and click OK.

You are returned to the Add/Import/Export Nodes dialog and the user name and password are added to the right-pane list.

7. (Optional) Select a node or agent in the left-pane list and click Properties.

The Server Properties dialog opens and displays the Domain name, Server name, IP address, Last response time, and Products installed. These properties are detected by the auto-discovery service, so the Properties button will only be enabled when you select a node or agent in the left-pane list and click Properties.

8. Click OK.

The nodes and agents are added to the Backup Manager Source tree or if an existing node or agent was deleted, it will be removed from the Backup Manager Source tree. If a node or agent name is duplicated, you will see a warning message indicating that this is a duplicate name and the node or agent will not be added to the Backup Manager Source tree. You can however, add multiple host names with the same IP address.

More information:

[How to Add, Import, and Export Nodes](#) (see page 315)

[Add Multiple Nodes and Agents Using a .csv and .txt File](#) (see page 319)

[Export Multiple Machines to a Text File](#) (see page 320)

Add Multiple Nodes and Agents Using a .csv and .txt File

The Import function allows you to quickly and easily add multiple nodes and agents using the CA ARCserve Backup user interface by importing them from a .csv or a .txt file.

Note: A .csv files is a file that uses a comma separated value format.

To add multiple nodes and agents using a .csv and .txt file

1. Open the Backup Manager and select the Source tab.
2. Right-click Windows Systems in the browser.
A pop-up menu opens.
3. Choose Add/Import/Export Nodes from the pop-up menu.
The Add/Import/Export Nodes dialog opens.
4. Click the Import button.
The Windows Open dialog opens.
5. Browse to the file containing the nodes that you want to import click Open.
The nodes and agents are added to the right-pane list on the Add/Import/Export Nodes dialog.
6. Select the nodes and agents in the right-pane list that you want to enter a user name and password for and then click Security.
The Security dialog opens where you can add the user name and password for nodes and agents at one time. The nodes and agents displayed on the Security dialog are provided from the right-pane list on the Add/Import/Export Nodes dialog.
7. Click OK.
The nodes and agents are added to the Backup Manager Source tree.

More information:

[How to Add, Import, and Export Nodes](#) (see page 315)

[Add, Import, and Export Nodes Using the User Interface](#) (see page 316)

[Export Multiple Machines to a Text File](#) (see page 320)

Export Multiple Machines to a Text File

Nodes and agents that are already entered Backup Manager Source tab can be exported to a .txt file to make it easy to import the list of nodes and agents to another CA ARCserve Backup server.

To export multiple machines to a text file

1. Open the Backup Manager and select the Source tab.
2. Right-click Windows Systems in the browser and select Add/Import/Export Nodes from the pop-up menu.

The Add/Import/Export Nodes dialog opens.

3. Click Export

The Export dialog opens.

4. Select the nodes and agents you want to export.

Note: By default, all nodes and agents are selected for you.

5. (Optional) Click Select All or Clear All to select or clear the nodes and agents in the list that you want to export.

6. Click OK.

The Windows Save As dialog opens.

7. Select a path where the file should be created and saved.

The selected nodes and agents are exported to a .txt file.

Note: The user name and password are not exported.

You can now use the newly-created .txt file to import the list of nodes and agents to another CA ARCserve Backup server.

More information:

[How to Add, Import, and Export Nodes](#) (see page 315)

[Add, Import, and Export Nodes Using the User Interface](#) (see page 316)

[Add Multiple Nodes and Agents Using a .csv and .txt File](#) (see page 319)

Filter Nodes

You can determine which machines in the domain have the same agents installed. CA ARCserve Backup lets you filter nodes from the Backup Manager Source tree and the Restore Manager Source tree and Destination tree.

Note: Only the Windows System and UNIX/Linux Systems catalogs can be filtered.

To filter nodes

1. From the Backup Manager, select the Source tab.
2. Select either the Windows System or UNIX/Linux System catalog and right-click.
3. From the right-click menu, select Filter by Application Type.
The Filter by Application Type dialog opens.
4. Click the Filter by Application Type.
Note: The default is Show all nodes.
5. Select one or more agent types from the agent list.
6. Click OK.

The nodes are filtered and a list of agents is displayed

Modify a Node

You can change the IP address or host name for an agent.

To modify a node

1. From the Backup Manager, select the Source tab.
2. Select a node and right-click.
3. From the right-click menu, select Modify Agent.
The Agent Option dialog opens.
4. Clear the Use computer name resolution checkbox.
5. Enter a Host name and an IP address.
6. Click OK.
7. Update related account information. For more information on updating account information, see Security Dialog.

Delete a Node

You can delete a node from the Backup Manager source tree. The node information, all accounts associated with the node, and its agents will be deleted from the CA ARCserve Backup database.

To delete a node

1. Select a node.
2. From the right-click menu, select Delete Node.

The delete confirmation dialog opens.

3. Click Yes.

The node is deleted.

How to Use the Job Scheduler Wizard to Schedule Jobs

The CA ARCserve Backup command line enables direct control over all operations that can be performed by a CA ARCserve Backup server. The Job Scheduler Wizard provides an alternative to entering job scheduling commands in the Command Prompt window.

The benefits of using this wizard rather than the command line include:

- Jobs can be scheduled and repeated.
- Jobs appear in the Job Queue and Activity log.
- Jobs can be stopped in the Job Queue.
- The commands you can enter are not limited to CA ARCserve Backup. You can use this wizard for virtually any executable, such as Notepad.exe.
- It provides an easy way to quickly package and submit jobs.

Important! All scheduled times for CA ARCserve Backup jobs are based upon the time zone where the CA ARCserve Backup server is located. If your agent machine is located in a different time zone than the CA ARCserve Backup server, you will need to calculate the equivalent local time that you want the job to be run.

When you submit a job using the Job Scheduler Wizard, it is labeled as a generic job in the Job Queue and Activity log. Although you can modify a generic job using the Job Queue; you can only reschedule and stop it.

Note: You must have Administrator rights on the local Windows machine to submit jobs using the Job Scheduler Wizard.

Job Scripts

A script is a job that you saved to a file. It contains the original source, destination, options, and schedule information for the job. It will also contain any filters you created to include and exclude files and directories.

Creating a script has the following advantages:

- You can re-use the same settings later.
- You can copy your settings to a different Windows machine running CA ARCserve Backup.
- You can quickly resubmit regularly executed jobs after a job has been accidentally deleted.

Create a Job Script

You can save almost any type of job as a script. A script is a set of CA ARCserve Backup instructions that let you execute jobs.

To create a job script

1. After you create the job, click **Start** toolbar button.
The Submit Job dialog opens.
2. Click **Save Job** button to save the job criteria in a script.
The **Save Job Script** dialog opens.
3. Enter a name for the script and click **Save**.
The job script is saved.
4. Click **OK** to submit the job to the queue.
The job is submitted and a job script is created.

Execute a Job Using a Script

You can execute almost any type of job using a script. A script is a set of (CA ARCserve Backup) instructions that let you execute jobs.

To execute a job using a script

1. Open the **Job Status Manager** and select the **Job Queue** tab.
Click the **Add** toolbar button.
The **Add Job** dialog opens.
2. Browse to and select the script for the job that you want to execute.
Click **Open**.
The **Specify a Server** dialog opens.
3. From the drop-down list, select the server from which you want the the job to execute and click **OK**.
The job information for the previously saved script will be displayed in the Job Queue as a new job.

For more information on how to create and use scripts, see the online help.

Job Templates

A job template contains a series of settings such as the destination, options, and schedule information for the job. Similar to job scripts, a template can also contain any filters you created to include and exclude files and directories.

Job templates are different, however, from job scripts because they provide the flexibility to repeat custom backup schedule settings on other CA ARCserve Backup machines. Because the job template does not retain the backup source information as the job script does, the template files can be copied and applied to any new server source running CA ARCserve Backup. Contrarily, job scripts can not be modified to accommodate new server sources.

You can choose from seven default job templates or you can create a custom template to meet your individual backup needs. The default job templates are designed to meet specific backup tasks such as rotation scheme, backup method, and GFS options. The default job templates can be accessed from the File menu when you choose the Open Job Template option.

Create Custom Job Templates

You can create a custom job template that you can save for future jobs on any CA ARCserve Backup system.

To create a job template

1. From the CA ARCserve Backup Manager window, select Backup from the Quick Start menu.

The Backup Manager Window opens.

2. Make selections for your backup job by accessing the Source, Staging, Destination, and Schedule tabs.

Click the Start toolbar button to submit the job.

The Submit Job dialog opens.

3. Click Save Template.

The Save Job Template dialog opens.

4. In the File Name field, specify a name for the job template and click Save.

The job is saved as a job template with an .ast file name extension.

Note: While default job templates are stored in the Templates/Jobs folder in the CA ARCserve Backup directory, you can save your template in any directory you want. To open your custom job template on a local machine or from a remote server, access the File menu and choose the Open Job Template option. After the job template is open, you can submit your job.

Windows-Powered NAS and Storage Server 2003 Device Configuration

CA ARCserve Backup provides support for backup and restore of Windows-powered NAS and Storage Server 2003 devices (referred to as Windows-powered NAS).

When you install CA ARCserve Backup on Windows-powered NAS, a new CA ARCserve Backup tab is available on the Web administration user interface for the device. By accessing the tab, you can connect directly with the CA ARCserve Backup components.

Access CA ARCserve Backup Through the Windows-powered NAS Device

You can administer backup and restore jobs as well as perform agent maintenance for Windows-powered NAS devices through the Web interface. A seamless integration of the CA ARCserve Backup Home Page is easily accessible from the Windows-powered NAS Web administration interface.

Links to CA ARCserve Backup Manager, Device Configuration, or Client Agent Admin are displayed from the Windows-powered NAS menu option. The options available are dependent upon the options installed on the Windows-powered NAS Device.

Use the following table to determine what options are available in the Windows-powered NAS Web administration interface based on a specific CA ARCserve Backup component install.

Installed CA ARCserve Backup Component	Options Available in Windows-powered NAS Interface
CA ARCserve Backup Manager	CA ARCserve Backup Manager
CA ARCserve Backup Server	Device Configuration
CA ARCserve Backup Windows Client Agent	Agent Admin

CA ARCserve Backup and Windows-powered NAS Device Configuration

The following describes basic Windows-powered NAS configurations supported by CA ARCserve Backup.

Backup Devices Connected Directly to Windows-powered NAS Devices

You can configure and deploy CA ARCserve Backup directly on a Windows-powered NAS as displayed in the following illustration:



You can use the Web interface integration provided by CA ARCserve Backup on a remote server and perform backup and restore tasks as well as monitor scheduled jobs configured for the installation.

How You Can Back Up Devices Connected to CA ARCserve Backup Server

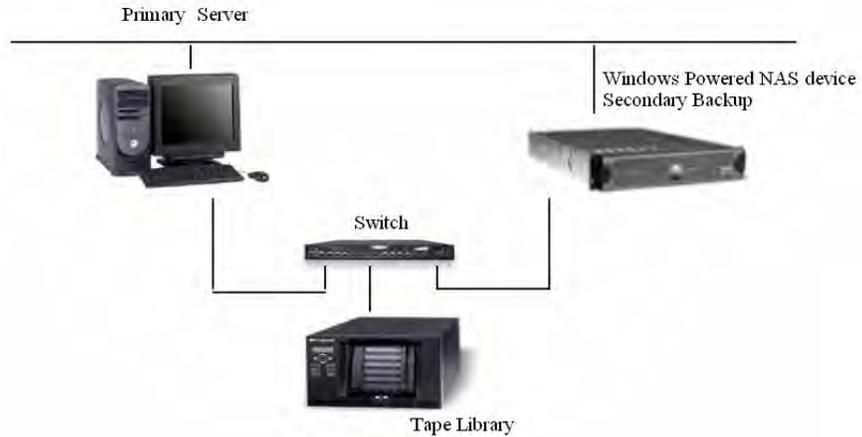
You can configure CA ARCserve Backup Windows Client Agents on the Windows-powered NAS device. Agents can be administered using the integrated Web administration interface provided by CA ARCserve Backup.

The Agents can be backed up from the remote CA ARCserve Backup Server which may be running on another Windows-powered NAS device as shown in the following illustration.



How You Can Back Up Devices Shared Between CA ARCserve Backup and Windows-powered NAS

You can configure CA ARCserve Backup Server, Manager, and the SAN Option on a Windows-powered NAS device and create a secondary remote CA ARCserve Backup server with a SAN Option. Both machines can connect to a shared backup device such as a tape library through a fiber switch as displayed in the following illustration.



Chapter 6: Managing Devices and Media

This section contains the following topics:

[Device Management Tools](#) (see page 329)

[Device Manager](#) (see page 355)

[How to Optimize Tape Usage](#) (see page 396)

[How Media Pools Work](#) (see page 401)

[Media Management Administrator \(MM Admin\)](#) (see page 413)

[MM Admin Interface](#) (see page 414)

[How the Media Management Process Works](#) (see page 421)

Device Management Tools

CA ARCserve Backup provides a number of ways to help you manage, monitor, and maintain your devices and media:

- The Device Manager gives you information about storage devices connected to your system, the media in these devices, and the status of these devices. It is the starting point for all media and device monitoring and maintenance operations.
- The Media Pool Manager lets you create, modify, delete, and manage media pools, collections of media managed as a unit to help you organize and protect your media.
- The Media Management Administrator (MMO) provides the tools you need to control, manage, and protect media resources.

Tape Library Configuration

The Tape/Optical Library configuration option lets you configure a single-drive tape or optical library in a Windows environment.

The following sections describe the tasks that you can perform to fully configure your library.

Note: For information about working with and configuring multiple-drive tape and optical libraries and Tape RAID libraries, see the *Tape Library Option Guide*.

More information:

[Configure Devices Using the Device Wizard](#) (see page 108)

Device Assignment

Assigning a drive to a library allows CA ARCserve Backup to recognize the drive's existence within the library.

Usually the manufacturer configures a library in such a way that the first library drive has the lowest SCSI ID number and the last library drive has the highest SCSI ID number.

Note: This is not always the case. See the documentation that came with your library for information on how its drives are configured.

To manually assign a drive to a library, highlight the drive you want to assign from the Available Devices list and the library in which the drive should reside from the Library Devices list then use the Assign button to move the drive to the library. To un-assign a drive from a library, highlight the drive in the Library Devices list and click Remove.

Note: All drives must be empty for CA ARCserve Backup to complete the drive configuration. The process may take a few minutes, depending on the number of drives in your library.

Configure a Library

CA ARCserve Backup automatically detects and configures your libraries as the Tape Engine starts. You do not need to run a wizard or other external application to enable CA ARCserve Backup to detect your libraries.

Note: If CA ARCserve Backup does not automatically configure your libraries, use Device Configuration to manually configure your libraries.

To configure a library, you must first ensure that the following prerequisite tasks are complete:

1. Install the CA ARCserve Backup base product.
2. Install the license for the CA ARCserve Backup Tape Library Option as required for your environment.
3. Start the Tape Engine.

CA ARCserve Backup automatically detects and configures your libraries.

4. If you want CA ARCserve Backup to read the tapes, open the Device Manager window, browse to and select the library. Click the Inventory toolbar button.

CA ARCserve Backup reads the tapes.

5. If the library is shared on a SAN, log in to the CA ARCserve Backup Primary server.

You are now ready to configure a library.

To configure a library

1. Open the Device Manager window and browse to the library.
Right-click the library and select Library Properties from the pop-up menu.
The Library Properties dialog opens.

2. Click the General tab.

Modify the following General options as required for your library:

Bar code reader installed

If your library contains a bar code reader, this option lets you use the bar code reader in the device to inventory the tapes in the library.

Set unknown bar code media to not inventoried during initialization

To enable this option, you must first select the **Bar code reader installed** option.

This option lets CA ARCserve Backup initialize faster by designating media with a bar code that is not recorded in the CA ARCserve Backup database as "Not Inventoried." This option prevents CA ARCserve Backup from inventorying all the slots as the Tape Engine starts. Media that is designated as not inventoried can remain in its slot until you need it. To use media that is designated as "Not Inventoried," you must inventory the media using the Manual Inventory option from the Device Manager window.

Library Quick Initialization

To enable this option, you must first select the **Bar code reader NOT installed** option.

Note: If the library does not support bar codes and this option is disabled, CA ARCserve Backup inventories the entire library when CA ARCserve Backup starts.

This option lets CA ARCserve Backup initialize faster by bypassing the inventory slots process when the Tape Engine starts. When you use this option, CA ARCserve Backup assumes that the media in the slot have not been added, removed, moved, or swapped since the last shutdown. If you added, removed, moved, or swapped media, you should manually inventory the entire library or inventory the slots that changed.

Note: CA ARCserve Backup must inventory the library after you configure the library. The quick initialization option takes affect after you complete the first full inventory of the library.

Eject media upon backup job completion

This option lets you direct CA ARCserve Backup to move the tapes back to their original slots after the backup job is complete rather than allow them to remain in the drives.

Note: You can override this option on a job-by-job basis by enabling the global option for jobs called Do not Eject Media. In addition, if you do not enable the ejection of media after a backup job completes and later decide that you want to eject media after a particular job, you can enable the global option for jobs called Eject Media.

Library is a VTL

This option lets you set up a library to function as a virtual tape library (VTL).

When you identify a library as a VTL, read performance improves. This capability lets CA ARCserve Backup maximize drive efficiency and overall VTL backup and data migration performance.

Important! You should not identify a physical library as a VTL. When you identify a physical library as a VTL, the library's backup and data migration performance can be adversely affected.

3. Click the Cleaning tab.

Modify the following Cleaning options as required for your library:

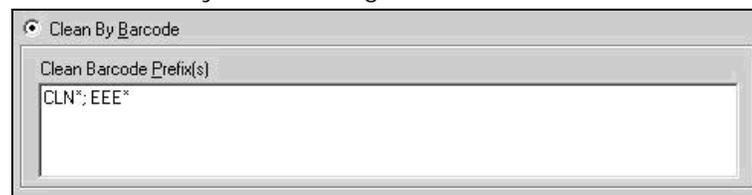
Clean by slot

This option lets you designate specific slots as cleaning slots. You can specify one or more cleaning slots and they do not need to be in a successive order.

Clean by Barcode

This option lets you specify cleaning slots for your library based on a specific bar code or a range of bar codes using a prefix and a wildcard character. In the Clean Bar Code Prefixes field, enter the prefixes of your bar coded cleaning tapes.

Specify the bar code prefixes into the Clean Barcode Prefix(s) field as illustrated by the following:



Note: The asterisk is a wildcard character.

Click OK.

The cleaning slots are set based on their bar code prefix.

Examples:

- The bar code on your cleaning tape is CLN123. In the Clean Barcode Prefix(s) field, specify CLN123.
- There are several cleaning tapes in your library. The bar code prefix for the cleaning tapes is ABC. In the Clean Barcode Prefix(s) field, specify ABC*.
- There are several cleaning tapes in your library. The cleaning tapes' bar code prefixes are ABC, CLN1, and MX. In the Clean Barcode Prefix(s) field, specify ABC*; CLN1*; MX*.

Automatic tape cleaning

This option lets you direct CA ARCserve Backup to manage your tape cleaning tasks automatically. When you enable this option you must specify the number of hours that must elapse between cleaning tasks.

4. Click OK.

Your library is successfully configured.

RAID Device Configuration Option

The RAID Device configuration option lets configure a RAID device in the Windows environment.

To configure a RAID Device, the Tape Engine must be stopped. If your Tape Engine is running, a pop-up window is displayed to allow you to stop the engine.

The following sections describe the steps required to fully configure your RAID device.

Note: For information about configuring Tape RAID device, see the *Tape Library Option Guide*.

More information:

[Configure Devices Using the Device Wizard](#) (see page 108)

RAID Level Configuration

Choose the RAID device from the Device Configuration dialog.

When you click Next, the RAID Option Setup dialog appears, enabling you to:

- Create a new RAID device
- Assign a RAID level
- Delete an existing RAID
- Change the RAID level

To review the attributes of each RAID level, instructions on selecting a RAID level, and instructions on assigning drives to the RAID device, see the online help.

RAID Group Configuration

The RAID device must be added to a group in the Device Manager to perform backup, restore, and copy operations using that RAID device. When running the job, CA ARCserve Backup automatically assigns a RAID device to a group, if it is not already assigned.

For information on how to manually assign a RAID device to a RAID group, see the online help.

Virtual Library Configuration Option

The Virtual Library configuration option lets you configure or modify the configuration of a virtual library in the Windows environment.

To configure a virtual library, the Tape Engine must be stopped. If your Tape Engine is running, a pop-up window is displayed to allow you to stop the engine.

The Virtual Library option is used to set up all virtual libraries. It enables you to define virtual libraries and their parameters, including the number of slots and drives required for the library. At minimum, a virtual library must have at least one slot and one drive associated with it.

Because the Virtual Library feature works on existing configured libraries, you must install the CA ARCserve Backup Tape Library Option and configure your physical libraries prior to configuring virtual libraries.

Note: You must separate WORM (Write Once Read Many) and non-WORM media in the same library using the Virtual Library configuration option. If WORM and regular media are not separated, the Job Manager treats all media as WORM media. However, the Device Manager can manage these media correctly.

For more information about configuring a virtual library, see online help or the *Tape Library Option Guide*.

More information:

[Configure Devices Using the Device Wizard](#) (see page 108)

Control Devices Using Removable Storage Management

The Enable/Disable Devices (for RSM) configuration option lets you enable or disable devices for Removable Storage Management (RSM) in the Windows 2000 and Windows Server 2003 environment.

To enable or disable devices for RSM, the Tape Engine must be stopped. If your Tape Engine is running, a pop-up window is displayed to allow you to stop the engine.

Servers running Windows 2000 and Windows Server 2003 take control of all the devices attached to the server when the Removable Storage service is enabled. This service manages removable media, drives and libraries. To control these devices CA ARCserve Backup must have exclusive access to them.

When RSM has exclusive control of device, CA ARCserve Backup cannot send SCSI commands directly to the device. However, when CA ARCserve Backup has exclusive control of a device, it can communicate (input and output commands) directly to the device.

When you choose the Enable/Disable Devices (for RSM) option, you are provided with a list of all the devices that are currently available in the system. CA ARCserve Backup manages the devices currently selected. If you want another application to manage any device, clear the selected device.

Note: You do not need to disable a device in the RSM if the device driver is not installed on the CA ARCserve Backup server. RSM functions in this manner because the lack of a device driver prevents RSM from detecting the device. CA ARCserve Backup does not require the presence of a device driver to be able to detect a device.

More information:

[Configure Devices Using the Device Wizard](#) (see page 108)

How to Create File System Devices

Device Configuration is a wizard-like application that lets you create file system devices, or modify the configuration of a file system device (FSD) within the Windows environment.

You configure an FSD to a folder on a specific drive. When you can specify the FSD as your backup destination, each session is stored as an individual file within that folder.

CA ARCserve Backup lets you configure an FSD without stopping the Tape Engine. When you configure an FSD, you can change the credentials of an FSD used for remote access by clicking Security.

From Device Configuration, you can add one or many devices. When you click Next, CA ARCserve Backup verifies the validity of information specified for all devices and alerts you if a particular device failed verification. Click the corresponding Verify button located in the Verify and Status column, or do so for each device as you configure it, to ensure successful verification before continuing. There are three possible outcomes displayed in this column:

- Pending--Displayed while a device is being configured.
- Pass--Displayed when verification of the information you specified succeeds.
- Failed--Displayed when CA ARCserve Backup finds problems with the information you specified. Click Failed in the Verify and Status column to obtain the cause of failure for each device that did not pass verification.

The status displayed in the Verify and Status column reads Pending while devices are being configured. Click the Verify button next to the status to check the accuracy of the information you provided. CA ARCserve Backup displays the Volume Size of the drive specified and a status of Pass if the information is valid.

If the status displayed is Failed:

- Make sure the paths you specified for the Location are unique for each device.
- Ensure the security credentials are accurate.
- Check that the volume is shared.

Staging backup operations can quickly consume a large amount of free disk space on file system devices. Due to the maximum file size limitations of FAT 16 and FAT 32 file systems, you should not use these file systems on file system devices designated for staging operations.

When you are creating an FSD, you can specify the Location of the FSD using any of the following formats:

- The path to the local folder, for example, c:\fs_drive.
- The path to the folder on the mapped drive, for example, k:\fs_drive.
- The UNC path, for example, \\server01\fs_drive.

When you use a mapped drive as an FSD:

- CA ARCserve Backup can use the mapped drive, but you must have logged in to the mapped drive previously.
- If you use a mapped drive for an FSD, CA ARCserve Backup converts the mapped drive to a universal naming convention (UNC) path and prompts you to provide log in credentials when you click Finish.
 - The log in credentials provided must enable full access to the mapped drive.
 - By default, CA ARCserve Backup uses the CA ARCserve Backup System Account to gain access to each remote FSD. You can change the credentials that you use with the selected file system device by using Security.
 - You do not need to provide credentials when you create an FSD using a local disk.

Important! CA ARCserve Backup does not support sharing an FSD with multiple CA ARCserve Backup servers. When an FSD is shared, the ARCserve servers using the FSD can overwrite the other server's backup data.

Note: CA ARCserve Backup supports configuring an aggregate total of 255 FSDs and DDDs (only if the number of physical devices configured is 0).

To create file system devices

1. Open the CA ARCserve Backup Manager Console.
From the Navigation Bar, expand Administration and click Device Configuration.
Device Configuration opens.
2. On the Welcome to Device Configuration dialog, select the File System Devices option and click Next.
3. Follow the prompts on the subsequent dialogs and complete all required information.

Add More than One File System Device to a Group

To add multiple file system devices to the same device group, the file device name you specify in Device Configuration should be the same for each device you want to include in the group. You can also use Configure Groups to place multiple file system devices in the same group after the file system devices have been created.

Device Commands for File System Devices

The device commands that are available for file system devices are:

- **Format**--Deletes the sessions from that folder.
- **Erase**--Deletes the sessions and writes a blank header file on that folder.

The device commands that are not available for file system devices are:

- Retension
- Compression
- Eject
- Long erase

Configure Devices Using Enterprise Module Configuration

Enterprise Module Configuration is a wizard-like application that lets you configure the following devices:

- **StorageTek ACSLS**--The StorageTek ACSLS configuration option lets you configure or modify the configuration of a StorageTek ACSLS Library. With this option, the CA ARCserve Backup server can interface with the StorageTek ACSLS libraries to manage backup and restore operations, tape volume movement, and tape volume organization.

To configure StorageTek ACSLS library, ensure that it is properly installed and running before you start Enterprise Module Configuration.

For information about using StorageTek ACSLS libraries with CA ARCserve Backup, see the *Enterprise Module Guide*.

- **IBM 3494**--The IBM 3494 configuration option lets you configure or modify the configuration of an IBM 3494 library. With this option, you can use the full capabilities of CA ARCserve Backup with the large tape volume capacities of the IBM® TotalStorage® Enterprise Automated Tape Library 3494.

To configure IBM 3494 Libraries, ensure that the following configurations are complete before you start Enterprise Module Configuration:

- All libraries are properly attached to your network.
- IBM 3494 Automated Tape Library software is installed on the primary server.

For information about using IBM 3494 libraries with CA ARCserve Backup, see the *Enterprise Module Guide*.

- **Image Option**--The Image Option configuration option lets you install a driver on target systems to enable Image Option capabilities. With this option, you can perform high-speed backups by bypassing the file system, creating a snapshot image of the drive, and reading data blocks from the disk.

For information about backing up and restoring data using the Image Option, see the *Enterprise Module Guide*.

- **Serverless Backup Option**--The Serverless Backup Option configuration option lets you install a driver on target systems to enable Serverless Backup Option capabilities. With this option, you can perform backups with near-zero impact to the system CPU by allowing applications on servers to continue to run while backups are in progress.

For information about backing up and restoring data using the Serverless Backup Option, see the *Enterprise Module Guide*.

To configure devices using Enterprise Module Configuration

1. From the Windows Start menu, click Start, point to Programs (or All Programs), CA, ARCserve Backup, and click Enterprise Module Configuration.

The Enterprise Module Configuration, Options dialog opens.

2. Click the button for the device that you want to configure, follow the prompts on the subsequent dialogs, and complete all required information.

Deduplication Device Management

Use Device Configuration to create data deduplication devices, to remove existing deduplication devices, or to change the properties on an existing device. You must have the proper security access in order to create a data deduplication device on a remote server.

Note: You may also create deduplication devices using the Device Wizard or the Create Deduplication Device option from the Device Manager.

More information:

[Create Deduplication Devices](#) (see page 341)

[Remove a Deduplication Device](#) (see page 346)

[Modify Deduplication Device Settings](#) (see page 347)

[Protect Deduplication Devices with CA XOssoft](#) (see page 348)

[Configure Groups for Data Deduplication](#) (see page 348)

[Configure Deduplication Groups](#) (see page 353)

Create Deduplication Devices

To deduplicate data, create and choose a deduplication device group as the backup destination. When you create new deduplication devices, CA ARCserve Backup automatically assigns each device to a new deduplication device group.

You can create deduplication devices locally or remotely. When creating remote deduplication devices, you must manually specify security credentials by clicking the Security button on the Device Configuration dialog, as instructed in the following procedure, otherwise CA ARCserve Backup attempts to use the system account.

From Device Configuration, you can add one or many devices. When you click Next, CA ARCserve Backup verifies the validity of information specified for all devices and alerts you if a particular device failed verification. Click the corresponding Verify button located in the Verify and Status column, or do so for each device as you configure it, to ensure successful verification before continuing. There are three possible outcomes displayed in this column:

- Pending--Displayed while a device is being configured.
- Pass--Displayed when verification of the information you specified succeeds.
- Failed--Displayed when CA ARCserve Backup finds problems with the information you specified. Click Failed in the Verify and Status column to obtain the cause of failure for each device that did not pass verification.

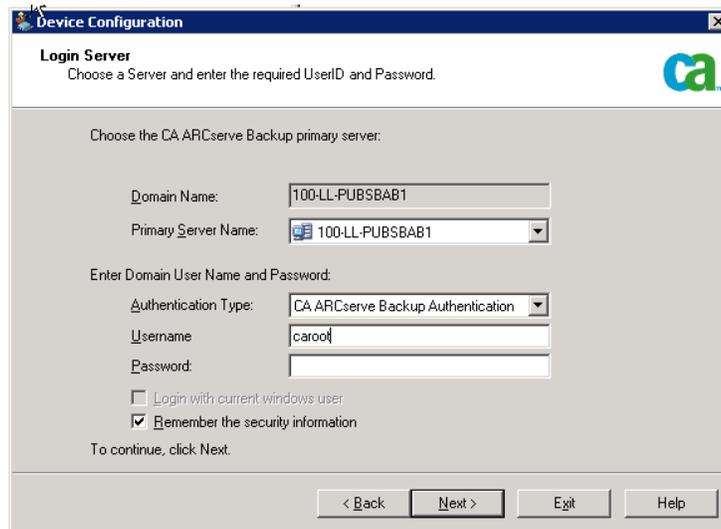
To create deduplication devices

1. From the CA ARCserve Backup Manager Console, expand Administration and click Device Configuration.

The Device Configuration screen opens.

2. Select Deduplication Device and click Next.

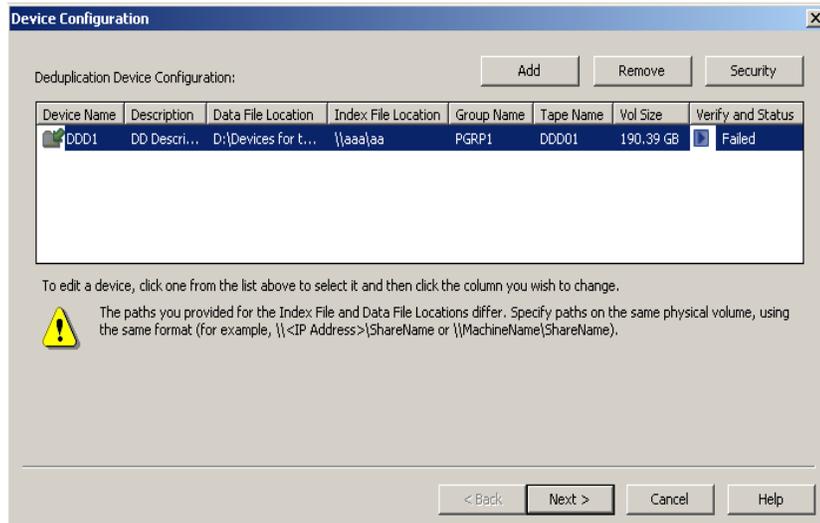
The Login Server screen opens.



3. Specify the primary server name, authentication type, user name and password and then click Next.

- Specify the server on which the deduplication device is to be created and click Next. For local servers (default), you may browse and select a path. If you wish to specify a remote server, you must have administrator rights to that server and must manually type the path.

The Deduplication Device Configuration screen opens.



5. Click Add to access the Deduplication Devices list.
 - a. Click the entry in the Deduplication Device Name column to edit it or accept the default.
 - b. Click the entry in the Description column to edit it or accept the default.
 - c. Click the entry in the Data File Location column to specify a path. You can type one manually or browse for an existing one.

To enter a location for a remote Data File, you must specify the Machine Name or IP Address, followed by the Share Name. Use the following format:

`\\MachineName\ShareName` or `\\IPAddress\ShareName`

Notes:

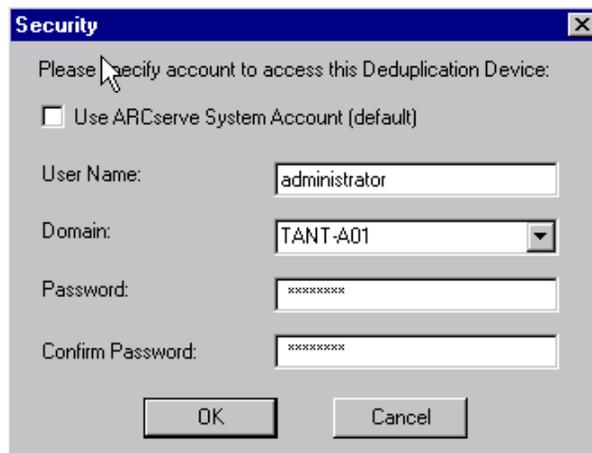
- The Data and Index File Location fields are empty, by default. When you create the deduplication device, CA ARCserve Backup can create the path you specify if it does not exist, or you can browse for one that does exist.
 - To reduce fragmentation for the first full backup job:
 - At the beginning of the backup, the Tape Engine pre-allocates 1 GB (configurable in the registry) to the data file.
 - Before the backup is done and you reach the end of the data file, increase the size of the data file by allocating another 1 GB.
 - At the end of the backup, if the empty space in the data file is more than 512 MB, reduce the data file size by 512MB. Otherwise, waste the space in the last 512 MB. In this situation, you will end up where the bytes at the end of the data file on the disk will not have valid data.
- So, the minimum size is 512 MB, even if only a byte file is backed up.
- d. Click the entry in the Index File Location column to specify a path. To avoid errors, use the same format used in the previous step to enter a remote location, or click the arrow to browse your directory structure.

Important! You should specify different paths for the Index File Location and Data File Location that are on NTFS volumes, and the locations should not contain data from other applications. To help you ensure the best performance, the Index File Location should reside on a disk with a fast seek time, such as a solid state disk.
 - e. Click the Group Name column and provide a name. If you leave this blank, a name is automatically provided that you can change in Group Configuration. This is the name you will select when submitting backup jobs that use deduplication devices.

Repeat this step as necessary to add more devices.

Note: CA ARCserve Backup supports configuring an aggregate total of 255 FSDs and DDDs (only if the number of physical devices configured is 0).

6. If you specified remote path locations, click Security to provide login information.



- a. Clear the Use ARCserve System Account (default) option to enable the security fields.
 - b. Enter the User Name, Domain, and password. Confirm the password in the last field.
 - c. Click OK to return to Device Configuration.
7. The status displayed in the Verify and Status column reads Pending while devices are being configured. Click the Verify button next to the status to check the accuracy of the information you provided. CA ARCserve Backup displays the Volume Size of the drive specified and a status of Pass if the information is valid.

If the status displayed is Failed:

- Make sure the paths you specified for the Index and Data File Locations are in the same format.
- Ensure the security credentials are accurate.
- Confirm the drive you specified is NTFS. Deduplication devices can be created only on NTFS volumes.
- Check that the volume is shared.

8. Click Next.

CA ARCserve Backup verifies the information specified for all devices in the list. If information is valid, the deduplication devices are added to the list. If any information is not valid, failed devices in the list are marked with a red Failed status. Click the corresponding Failed status to determine the cause of an individual error and resolve it. When all devices pass verification, a summary screen is displayed.

9. Click Next to return to the Welcome to Device Configuration screen or click Exit to leave Device Configuration.

Important! When you create a deduplication device, the purge policy is automatically set to four weeks. That default purge policy is inherited by every job you set up for the device. If you wish to retain backups longer than four weeks, you must adjust the purge time when you submit the backup job.

More information:

[Specify Copy and Purge Policies for Disk Staging Backups](#) (see page 205)

Remove a Deduplication Device

When devices break down, or when you no longer wish to use a device for deduplication, you can remove the device from CA ARCserve Backup.

To remove an existing deduplication device

1. Open Device Configuration and choose Deduplication Device.
2. Click Next.
The Login Server screen opens.
3. Specify the domain name, primary server name, and authentication type.
4. Enter your user name and password and click Next.
5. Specify the server on which the deduplication device is to be removed and click Next.
The Deduplication Device Configuration screen opens.
6. Click the device you wish to remove to select it.
7. Click Remove.
The selected device is flagged for removal. If you wish to keep the device, click Cancel Removal.
8. Click Next.
9. Click Exit.

Modify Deduplication Device Settings

You may change the device name, description, and data or index file locations. However, you may not modify the device's group or tape names.

To modify deduplication device settings

1. From the CA ARCserve Backup Manager Console, expand Administration and click Device Configuration.

The Device Configuration screen opens.

2. Select Deduplication Device and click Next.

The Login Server screen opens.

3. Specify the domain name, primary server name, and authentication type.

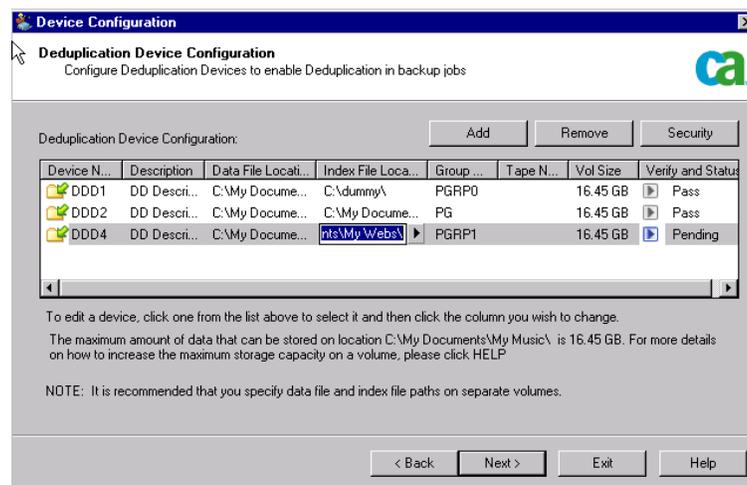
4. Enter your user name and password and click Next.

5. Specify the server on which the deduplication device is to be created and click Next.

The Deduplication Device Configuration screen opens.

6. Click a device from the Deduplication Devices list to modify settings.

7. Click a value under the Deduplication Device name, Description columns. You cannot change the Group and Tape Names from this screen. Use Group Configuration to change the Group Name. You can also add a Data File or Index File path if these fields are blank, but you cannot change these values once the device is formatted.



8. Specify new settings. If you specify remote locations for Data File or Index File Locations, click Security and provide the required User Name, Domain and Password. Retype the password to confirm.

9. Click Next.

10. Click Exit to leave Device Configuration if you are done modifying settings.

Protect Deduplication Devices with CA XOSoft

When deduplication devices are installed locally, the deduplication data files are excluded from CA ARCserve Backup jobs. If you wish to protect the deduplication device itself, you can do so using CA XOSoft.

With CA XOSoft, you can create a scenario that replicates the index and data file paths for a deduplication device. For more information, see the topic, [Create CA XOSoft Scenarios for Deduplication Devices](#). (see page 691)

Configure Groups for Data Deduplication

When you create a deduplication device, CA ARCserve Backup automatically adds it to a deduplication device group. However, for times when you need to reassign devices, rename or delete existing groups, use Device Group Configuration. You can even add a new (empty) group and assign a device to it later.

Once groups are created, use Configure Deduplication Groups on the Device Manager properties screen to set deduplication group properties, such as the maximum number of streams, or optimization. Properties set here apply to device groups used in both the staging or destination phases of a backup job.

Add a New (empty) Deduplication Group

You can create a new regular group and then assign a deduplication device to it, making the regular group a deduplication device group. For example, if an existing device is busy or damaged, but the group has been specified in various backup jobs, you can remove the existing device from a particular group and then assign a new device to it.

Note: You can assign only one deduplication device to a group.

To add a new empty deduplication group

1. From the Administration menu in the Navigation Bar on the CA ARCserve Backup Manager Console, select Device Group Configuration.

Device Group Configuration appears.

2. Click Next.
3. On the Login Page, provide credentials and click Next.
4. On the Options dialog:
 - a. select the server you would like to configure,
 - b. choose Configure Groups,
 - c. click Next.
5. From the Device Group Configuration dialog, click New.

The New Group dialog opens.
6. On the New Group dialog,
 - a. Choose Regular Group,
 - b. enter a Name for the new group,
 - c. click OK.

The new regular group appears in the Groups list, but contains no device. You may now assign an available deduplication device to this group.

Assign a Deduplication Device to a Group

You can reassign devices to groups using Device Group Configuration. Make sure the desired group is empty before you begin. If it is not empty, remove any devices and then proceed.

To assign a deduplication device to an empty group

1. From Device Group Configuration, click a Group from the list of available groups on the left.
2. From the list of Available Devices on the right, click a device to select it.

Note: If there are no Available Devices to choose from, remove a device from another group or delete an existing device groups. Devices in deleted groups are moved to the Available Devices list.

3. Click Assign.

The device is added to the group you selected.

4. Click Finish when you are done assigning devices.
5. Click Exit to leave Device Group Configuration.
6. Click OK to clear the confirmation message.

You can convert an existing FSD group to a deduplication group by removing the FSD devices from it and adding a deduplication device to it. Similarly, you can convert a deduplication group to a normal FSD group in the same manner.

Remove a Deduplication Device from a Group

You can remove a deduplication device from a group and reassign it elsewhere.

To remove a deduplication device from a group

1. From Device Group Configuration, click a Group from the list of available groups on the left.
2. Select the device inside this group to select it.
3. Click Remove.

The device is removed from the Group and added to the list of Available Devices.

4. Click OK when you are done removing devices.

You may reassign devices you have removed to other device groups.

Delete a Deduplication Device Group

You may delete a deduplication group. The device assigned to a deleted group is moved to the list of available devices for reassignment.

To delete a deduplication group

1. From the Administration menu in the Navigation Bar on the CA ARCserve Backup Manager Console, select Device Group Configuration.
Device Group Configuration appears.
2. Click Next.
3. On the Login Page, complete the required fields and click Next.
4. On the Options dialog, select the server you would like to configure, choose Configure Groups and then click Next.
5. From the Device Group Configuration dialog, click a Group from the Groups list to select it.
6. Click Delete.
A confirmation message appears.
7. Click OK to continue.
The selected group is deleted. The device assigned to the deleted group is moved to the Available Devices List.
8. Click Finish if you are done deleting groups.
9. Click Exit to leave Device Group Configuration.
10. Click Yes to clear the confirmation message.

Rename a Deduplication Device Group

If you wish to rename an existing deduplication device group, you may do so from Device Group Configuration.

1. From the Administration menu in the Navigation Bar on the CA ARCserve Backup Manager Console, select Device Group Configuration.
Device Group Configuration appears.
2. Click Next.
3. On the Login Page, complete the required fields and click Next.
4. On the Options dialog, select the server you would like to configure, choose Configure Groups and then click Next.
5. From the Device Group Configuration dialog, click a Group from the Groups list to select it.
6. Click Rename.

The Rename Group dialog opens.

7. From the Rename Group screen,
 - a. Type a new name for the device group,
 - b. Click OK

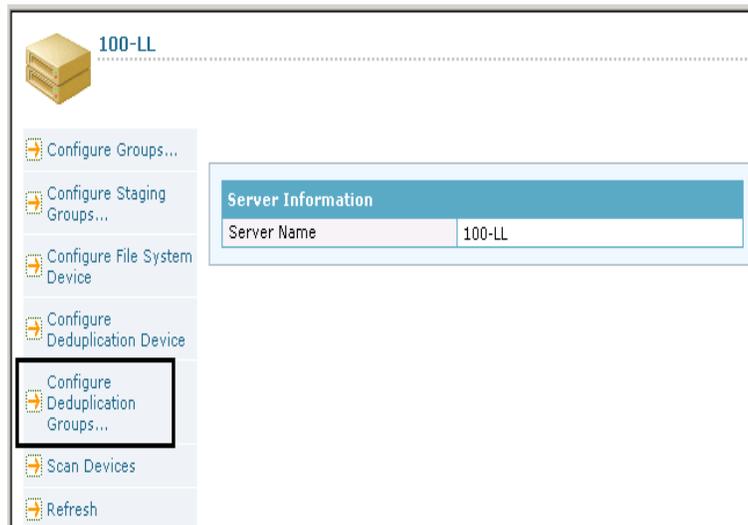
The name is changed and the device previously assigned to the group remains unchanged.

Configure Deduplication Groups

Use the Configure Deduplication Groups option from Device Manager properties to set the properties for a deduplication device group. You must have deduplication devices created first.

To configure deduplication groups

1. From the CA ARCserve Backup Manager Console, select Administration, and click Device to show Device properties.
2. Click Configure Deduplication Groups. The Deduplication Device Group Configuration dialog opens.



3. From the list of Groups displayed, choose the group you wish to configure and then complete the following fields, as needed.

Max Threshold

Specifies the maximum amount of space that can be used on a disk before a job fails. When the maximum threshold is reached, CA ARCserve Backup fails the jobs.

Default Value: 80%

The Max Threshold is represented as either a percentage of the total capacity used on the disk, or as the total number of GB or MB used.

Max # Streams

Specifies the maximum number of simultaneous streams to the device.

Default Value: 4

Pause Data Migration

Instructs CA ARCserve Backup to halt the data migration process. This option applies only to deduplication groups used in staging operations.

Default Setting: Disabled

Allow optimization in Data Deduplication backups

Directs CA ARCserve Backup to examine file header parameters first. The process of identifying natural boundaries and performing hash calculations is performed only on files whose header details have changed since the last backup, greatly enhancing backup throughput.

Default Setting: Enabled

Note: You cannot optimize stream-based data (for example, MS SQL or Oracle). If you use Optimization, please also ensure the Reset archive bit after backup with optimization option on the Operation tab in Global Options is enabled. Failure to reset the archive bits after a backup job means Optimization considers **all** files to be changed, even if no changes actually took place. We recommend disabling optimization in rare situations where applications running on the machine being backed up reset the file archive bit and file attributes like modified time.

Enable Global Deduplication

Lets you to perform deduplication on the C:\ drives of different machines.

Delayed Disk Reclamation

Lets you reclaim disk space created by the deduplication process. Delayed disk reclamation reduces the risk of disk fragmentation.

Expedited Disk Reclamation

Lets you immediately reclaim disk space created by the deduplication process. Although expedited disk reclamation improves the performance of disk reclamation, it can introduce disk fragmentation to the device. This option is enabled by default to improve the performance of disk reclamation.

4. Click OK when you are done configuring deduplication groups.

Note: You can also access the deduplication device group configuration dialog from the Device Group Configuration wizard or from the Device Manager toolbar.

More information:

[Global Deduplication](#) (see page 694)

Device Manager

The Device Manager provides information about storage devices that are connected to your system, the media in these devices, and the status of these devices. When you highlight a storage device or the adapter card it is configured to, summary information is displayed about the adapter card or the storage device, such as the vendor, model name, and board configuration.

If you have more than one storage device connected to your machine, CA ARCserve Backup lets you separate them into groups. Establishing device groups is the key to the flexibility and efficiency of CA ARCserve Backup.

By default, CA ARCserve Backup is installed with each storage device assigned to its own group. If identical storage devices (same make and model) are detected, it automatically places them in the same group. You can use Device Group Configuration to:

- Create a new device group
- Assign a device to a device group (including a RAID group)
- Remove a storage device from a device group
- Rename or delete a device group
- Use a RAID tape set as one unit

Maintenance Tasks

Using the Device Manager, you can perform the following maintenance tasks on your media:

- [Format media](#) (see page 356).
- [Erase data](#) (see page 357).
- [Retention tapes](#) (see page 359).
- [Compress data](#) (see page 360).
- [Eject media](#) (see page 360).
- [Online and Offline drives](#) (see page 361).
- [Rebuild media - RAID devices only](#) (see page 362).
- [Scan device - USB storage devices only](#) (see page 362).

Important! Before you use these options, especially formatting and erasing, make sure you have the right media selected.

Format Media

Although CA ARCserve Backup automatically formats blank media during a backup job, you can use this option to manually format your media. Formatting writes a new label at the beginning of the media, effectively destroying all existing data on the media.

Note: Use this option with care. After the media is formatted media, CA ARCserve Backup can no longer restore the data and any job sessions associated with the media.

Low level formatting, which is required on most hard drives and some mini cartridge device drives, is not required for drives that CA ARCserve Backup supports.

To format media

1. Click the Format toolbar button on the Device Manager window.

The Format dialog opens. It displays specific details about the media in your library slots. For example, unformatted media appears as <Blank Media>, and slots reserved for cleaning media do not appear.

Important! File System Devices (FSD) that are part of a staging group cannot be formatted using the Format toolbar button. To prevent accidental formatting of an FSD before the data is migrated to a final destination media, CA ARCserve Backup disables the Format toolbar button on the Device Manager window. If you want to format the FSD, you can either use the command line (`ca_devmgr`) or disable the staging option for the selected FSD.

2. Select the slot containing the media that you want to format. Assign a New Media Name and an Expiration date to the media that you want to format.

Note: When you assign a New Media Name to a slot, the light icon next to the selected slot turns green. Slots with write-protected media appear in red. These media cannot be formatted. You must specify a New Media Name before formatting the media.

Repeat this step if you want to specify more media.

3. If you want to use the media in a media pool, select a slot with the green light icon and check the Use Rotation option. Then, from the Media Pool drop-down list, select the media pool that you want to use the newly formatted media in. In the Serial No. field, you can accept the default serial number or specify a user-defined serial number. (If no media pool name is defined and the media has an assigned bar-coded serial number, then CA ARCserve Backup does not overwrite that serial number during the format procedure.)

Note: Click the Apply to all button if you want to use all of the formatted media in a media pool and assign all the media to the same media pool.

4. Assign a name and an expiration date to the media you want to format. You must specify a New Media Name before formatting the media. For more information about expiration dates, see Expiration Dates.
5. Click OK.

The Format dialog closes and the following message appears:

"Formatting will erase ALL of your data from the media. Do you want to format the media?"

6. Do one of the following:
 - To start the formatting process, click OK.
CA ARCserve Backup formats the media.
 - To cancel the formatting process, click Cancel.
CA ARCserve Backup does not format the media.

Erase Media

Use this option to erase all data from a single media or from multiple media. CA ARCserve Backup also erases all references to the contents of this media (if any) from the database. When you reformat this media, its physical history (read and write passes) is retained.

You should verify that you have selected the correct media before using the Erase option. Erased data cannot be retrieved. When erasing media, you can choose from the following options:

- **Quick Erase**--Quick Erase effectively erases media. It avoids the time a Long Erase would take (minutes to hours) by overwriting the media label. The media history remains available to CA ARCserve Backup for tracking purposes.
- **Quick Erase Plus**--This option performs the same operation as Quick Erase, and also erases bar codes and serial numbers. For more information about bar code and serial number cataloging, see Mount and Dismount Option.

Note: If the media you are erasing does not have a serial number or bar code, this option functions in the same manner as the Quick Erase option.

Media erased using the Quick Erase Plus option can no longer be tracked by CA ARCserve Backup, and information such as the expiration date is no longer carried forward.

- **Long Erase**--Long Erase completely removes all data from media. It takes much longer than a Quick Erase, but the media is literally blank. For security reasons, use the Long Erase option to ensure that all data on your media is erased completely.

The Long Erase option is the equivalent of formatting the optical platter when erasing optical media.

Note: The long erase process consumes more time than the quick erase process. This will be apparent when you erase large capacity libraries. Exercise caution when using this option on large capacity libraries.

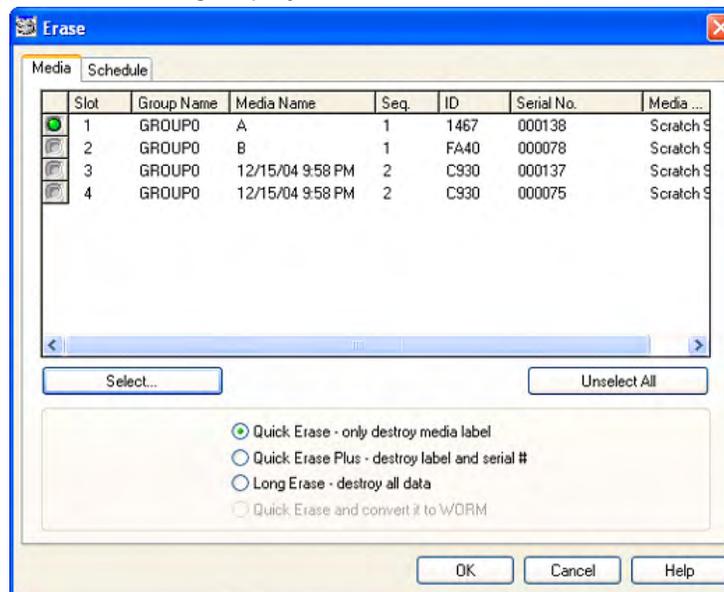
- **Quick Erase and convert to WORM**--This option quickly erases all data from the media. In addition, CA ARCserve Backup converts the media to Write Once - Read Many (WORM) media.

To use this option, CA ARCserve Backup must detect DLTWORM capable media in the library or in a stand-alone drive.

To erase media

1. Click the Erase toolbar button.

The Erase dialog displays.



In this dialog, slots reserved for cleaning media do not display.

2. Select the slot you want to erase. When you select media, the light icon next to the media turns green.

You can press the Shift key to select multiple contiguous media. Press the Ctrl key to select multiple noncontiguous media. You can also click and drag the light icon to select multiple contiguous media.

3. Select an erase method, click OK, and then click OK to confirm.

CA ARCserve Backup erases the media.

Retension Tapes

Use the Retension option to make sure a tape is evenly wound and properly tensioned to avoid errors, jamming, or breaking. You should retension a tape if you are having trouble writing to it or reading from it.

Note: This feature applies only to quarter inch cartridge tapes.

To retension a tape

1. Insert the tape into a storage device.
2. Select that tape.

In the left pane of the Device Manager, expand the tree under the storage device that the tape is in.

Then highlight the tape.

Click the Retension toolbar button.

Click OK.

CA ARCserve Backup retensions the tape.

Compress Media

Use the Compression option only if your storage device supports tape compression. If it does not, the Compression toolbar button will be disabled.

Note: Set the Compression option off only if you plan to use a media in another drive that does not support compression. In this case, the drive that does not support compression will not be able to read the compressed data on the media.

To turn compression on or off

1. Open the Device Manager and browse to the library that you want to configure.

2. Select the device drive in the Device Management tree.

If the device drive supports compression, then CA ARCserve Backup enables the Compression toolbar button. To verify if the device supports compression, select the Detail tab when the device is highlighted.

3. Click the Compression toolbar button.
4. Click OK to set the Compression Mode to Off (if it is On) or On (if compression is Off).

Eject Media

Use this option to eject media from library storage drives and return the media to their home slots (the slot with which the media was associated during the inventory process).

To eject the media from all drives in a library or a single drive

1. Open the Device Manager window.
2. From the Device Manager's devices directory tree, do one of the following:
 - To eject the media from all drives in a library, select the library.
 - To eject the media from a single drive, select the individual drive.
3. To eject the media, do one of the following:
 - Right-click the library or drive and select eject from the pop-up menu.
 - Click the Eject toolbar button.
4. Click OK to confirm.

CA ARCserve Backup ejects the media.

Online and Offline Drives

You can status library drives as offline or online from the Device Manager by right-clicking on the drive and selecting offline or online, depending on the current state of the drive.

This can be useful for marking defective drives in a library as offline, and prevents CA ARCserve Backup from using the drive until it is repaired and in an online status.

Note: If there is media inside the drive you want to mark as online or offline, eject the media prior to marking the drive offline. CA ARCserve Backup cannot access the media inside an offline drive.

To online and offline drives

1. Open the Device Manager and browse to the server connected to the library containing the drive that you want to status as online or offline.
2. Expand the library, right-click the drive, and select Online or Offline from the pop-up menu.

The drive status changes to offline or online.

Note: Drives display in a disabled mode when it is in an offline state.

Rebuild Media

Note: This option applies to RAID devices only.

Using the Rebuild option you can rebuild one missing or unusable tape containing backup data in a RAID level 5 environment.

Due to the architecture of RAID Level 5 (striping with parity), you cannot rebuild more than one missing or defective tape.

The following procedures describe how to rebuild the tape.

To rebuild a tape drive RAID

1. Eject the incomplete RAID set, using the eject option from CA ARCserve Backup Device Manager (choosing 'Eject' while highlighting the RAID ejects all tapes in RAID).
2. Insert a tape that the user wants to use as the replacement for the missing tape in one of the tape drives.
3. Chose Erase from the Device Manager.
CA ARCserve Backup erases the tape.
4. Insert the incomplete RAID set in the other tape drives and click the Rebuild toolbar button.
CA ARCserve Backup rebuilds the media.

To rebuild tape library RAID

1. If there are no blank tapes in the library, import one tape, or erase an unused tape in the library.
2. Choose the RAID set that you want to rebuild and click the Rebuild toolbar button.
CA ARCserve Backup rebuilds the media.

Scan Devices

Use the Scan Device option to enumerate USB storage devices that are connected directly to the CA ARCserve Backup server.

Note: This option applies to USB storage devices only.

To scan a USB storage device using the Scan Device option

1. Open the Device Manager.
2. Connect the USB storage device to the CA ARCserve Backup server.
3. Select the USB controller icon in the device directory tree and click the Scan Device toolbar button.

CA ARCserve Backup detects and enumerates the device in the Device Manager, device directory tree.

Important! If the drivers for the USB storage device are not Plug and Play (PnP) compatible, CA ARCserve Backup may not be able to detect and enumerate the storage device. To resolve this, you must configure the USB storage device by stopping and restarting the Tape Engine.

To scan a USB storage device by stopping and starting the Tape Engine

1. Stop the Tape Engine by doing the following:

- a. From the Quick Start menu, select Server Admin.

The Server Admin Manager opens.

- b. From the server tree, locate and select the primary server.

The CA ARCserve Backup services appear in the right side of the window as illustrated by the following screen:

Name	Status	Up Time (days:hours:mini...	Description
CA ARCserve Communication Foundation	Started	2 : 23 : 35	Provides data used by CA ARCserve Backup Dashboard.
CA ARCserve Database Engine (ODBC)	Started	2 : 23 : 35	Provides database services for ARCserve Backup products. If thi...
CA ARCserve Discovery Service	Started	2 : 23 : 35	Enables the discovery of all ARCserve Backup products on the ne...
CA ARCserve Domain Server	Started	2 : 23 : 34	Provides the management of domains and authentication service...
CA ARCserve Job Engine	Started	2 : 23 : 35	Maintains and executes jobs from the ARCserve Job Queue. If t...
CA ARCserve Management Service	Started	2 : 23 : 35	Provides remote services for command line utilities.
CA ARCserve Message Engine	Started	2 : 23 : 35	Allows remote management of other ARCserve Servers.
CA ARCserve Service Controller	Started	2 : 23 : 35	Enables remote start/stop of ARCserve Backup services.
CA ARCserve Tape Engine	Started	2 : 23 : 34	Manages the configuration and operation of backup devices for ...

- c. Right-click CA ARCserve Tape Engine and select Stop on the pop-up menu.

The Tape Engine stops.

Note: Do not close the Server Admin Manager.

2. Attach the USB storage device directly to the CA ARCserve Backup server.

3. Restart the Tape Engine by doing the following:

- a. From the server tree, locate and select the primary server.

The CA ARCserve Backup services appear in the right side of the window.

- b. Right-click CA ARCserve Tape Engine and select Start on the pop-up menu.

The Tape Engine starts.

After the Tape Engine starts, CA ARCserve Backup detects and enumerates the device in the Device Manager device directory tree.

More information:

[Configure USB Storage Devices](#) (see page 386)

Schedule Device Management Jobs

Under Device Management, you can submit a scheduled Format or Erase job. In the Format or Erase dialog, choose Run Now to run and submit the device command now or choose Schedule to submit a device command job to the CA ARCserve Backup queue and run later. Specify the date and time you want to run the device command.

For more information about the Run Now option, refer to the section Job Queue Tab.

More information:

[How to Manage Jobs Using the Job Queue Tab](#) (see page 302)

Device Management Functions for Libraries

Using the Device Manager, you can perform the following management tasks for your libraries.

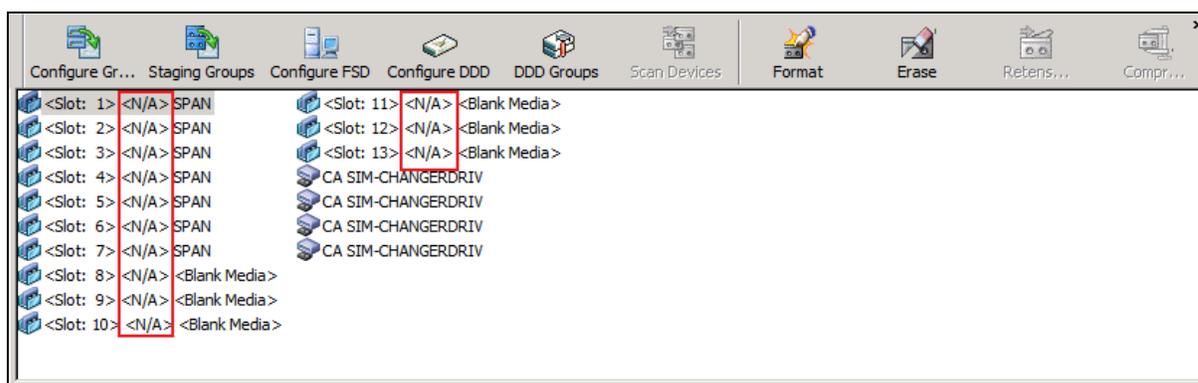
- [Inventory the slot range](#) (see page 367).
- [Mount and Dismount a magazine](#) (see page 369).
- [Import and export media](#) (see page 370).
- [Clean media - for tape libraries only](#) (see page 373).
- [Offline and online removable drives](#) (see page 376).
- [Configure library device groups](#) (see page 381).

How CA ARCserve Backup Labels Media with Bar Codes or Serial Numbers

Labeling media allows the library to quickly recognize and differentiate one media from the others. Bar code recognition is a library-specific feature. Each media comes from its manufacturer with a bar code label affixed to the outer edge of the media cartridge. This label has a predefined serial number in letters and numerals, which is used as the media serial number when the media is formatted.

If you select a media pool name and the media has an assigned bar coded serial number, that serial number is preserved and the media pool range is ignored.

Note: When the serial number or bar code does not exist on the media, CA ARCserve Backup displays N/A (not available) on the media description in the Device Manager as illustrated by the following screen.



How to Choose Expiration Dates

The expiration date tracks how long media should be in service. The life of media is generally based on passes. A pass is defined as the storage drive head passing over a given point on the media. For example, a backup without verification constitutes one pass, whereas a backup with verification constitutes two passes.

Tape manufacturers rate their tapes' useful lives from about 500 to 1500 passes. This does not mean that the tape is unusable after it reaches the maximum number of passes, only that it is more susceptible to errors at this point.

You should choose expiration dates based on how you plan to use the tape. If you plan to use the tape often, (for example, a few times a week), you should set the expiration date to one year, or less, from the date of formatting. By contrast, if you plan to use the tape only once or twice a month, you can set the expiration date to two or three years from the current date.

When media reaches its expiration date, CA ARCserve Backup notifies you that you cannot overwrite to expired media. To remedy this condition, you can specify to append the backup data to the expired media by doing the following:

1. Open the Backup Manager and click the Options toolbar button.
The Global Options dialog opens.
2. Select the Backup Media tab.
In the First Backup Media section, click the Append option.
Click OK.
Resubmit the job.

Expiration Dates for New Media

CA ARCserve Backup formats media using the following guidelines:

- If you are formatting new, blank media, the default expiration date is three years from the current date.
- If you are reformatting media, the expiration date that appears is the date you specified the first time the media was formatted.

How CA ARCserve Backup Logs Expired Media

CA ARCserve Backup logs messages in the Activity Log that relate to media that is expired or will expire in certain number of days.

- When the backup job appends the backup data to an expired media, a warning message is displayed as shown below:

```
This job is appending to an expired media.  
(MEDIA=media_name[S/N:serial_number], ID=media_id, SEQ=sequence_number)
```

- When a backup job chooses a media to overwrite or append the backup data, it checks the alert period of the media expiration and displays the following message:

```
This job is using media that will expire after <# of days>  
(MEDIA=media_name[S/N:serial_number], ID=media_id, SEQ=sequence_number).
```

Where <# of days> represents a specific number days (for example, 3, 5), Media_name represents the name of the media (for example, tape1, Media_id represents the media ID (for example, 3d3c), and Sequence_number represents the sequence number.

Note: This operation applies to both first tape and spanning tape.

- The alert period of the media expiration is 30 days by default. You can change this by adding the DWORD AlertPeriodForTapeExpiration to the following registry key to set the alert period (number of days):

```
\\HKEY_LOCAL_MACHINE\ComputerAssociates\CA ARCserve  
Backup\Base\Task\Backup\AlertPeriodForTapeExpiration
```

Note: This approach only applies to tape media, and you cannot overwrite to an expired media.

Inventory Slots

The Inventory Slots option checks the library slots and reads the media header. It then associates the media header with the slot in which it was found (called the home slot). In this way, the Tape Engine can track changes made to media in the library. For example, media added or removed from a magazine or moved to a different slot.

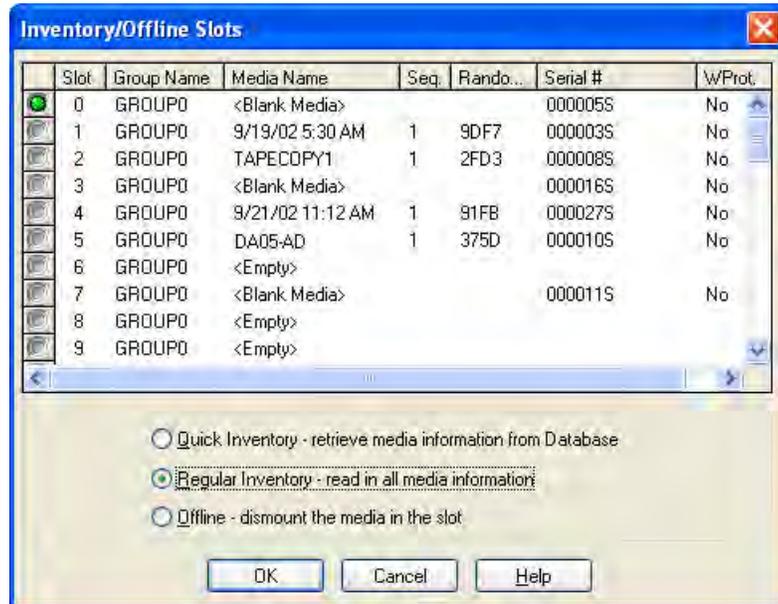
Be aware of the following considerations when using the Inventory Slots option to inventory media:

- Each media that you load into the storage drives in the libraries must have a unique serial bar code number.
- You should only add and remove media when the Tape Engine is running so that you can immediately inventory your slots.
- For media that was created using a previous ARCserve release, this release automatically creates a new media pool with the same name given to media that was inventoried and used in a media pool in the previous ARCserve release.

To inventory slots

1. Right-click a slot and select Inventory/Offline Slots from the pop-up menu.

The Inventory/Offline Slots dialog displays as shown in the following example.



2. Select the slot you want to inventory. Press the Shift key to select multiple contiguous media. Press the Ctrl key to select multiple non-contiguous media. The light icon next to selected media turns green.

Note: You can also click and drag the light icon to select multiple contiguous media.

3. Choose one inventory method:
 - **Quick Inventory**--The Tape Engine matches the bar code number to the media serial number, if the library supports bar codes, and the bar code option is enabled. You can only use this method if you are using the bar code option.
 - **Regular Inventory**--The Tape Engine reads all the media information from the media.
Note: This method is also known as a Manual Inventory.
 - **Offline**--Dismounts the selected slots.
4. Click OK.
CA ARCserve Backup inventories the slots.

Mount and Dismount Magazines

Use this option to mount (load) or dismount (remove) a magazine from the library. Mounting a magazine initiates an inventory of the slots in the magazine. Dismounting a magazine returns all media to their home slots and prepares the magazine for removal. The time this process requires varies based upon the number of media in the magazine you are mounting or dismounting. Additionally, the time required to mount and dismount magazines can vary from vendor to vendor.

This option checks the library slots and reads the media header. It then associates the media header with the slot in which it was found (its home slot). This enables the Tape Engine to keep track of any changes made to media in the library (media added to or removed from a magazine or moved to a different slot).

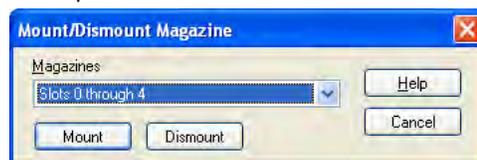
If you are using bar codes, each media that you load into a storage drive in the libraries must have a unique serial bar code number. If you purchased two media having identical serial numbers, you must use one of the media in a different backup session.

You should add and remove media only when the Tape Engine server is running, so that you can immediately inventory your slots.

To mount or dismount a magazine

1. Click the Mount toolbar button.

The Mount/Dismount Magazine dialog displays as shown in the following example:



2. Select the magazine you want to mount or dismount.

Depending on the operation that you want to perform, click one of the following buttons:

- Mount
- Dismount

CA ARCserve Backup mounts or dismounts the magazine.

Import and Export Media

CA ARCserve Backup lets you import media and retrieve media information from the media or the CA ARCserve Backup database. You can also import or export multiple media to or from your library slots.

If the library has mail slots, CA ARCserve Backup lets you move tapes into and out of the library. You can:

- Import one or more media from mail slots to library slots.
- Export one or more media from library slots to mail slots.

When importing media, you can choose one of the following methods:

- **Quick Import**--CA ARCserve Backup imports the media and attempts to use the media's bar code information to retrieve the corresponding information from the CA ARCserve Backup database.

Note: You can only use this method if you are using the bar code option.

- **Regular Import**--Reads all media information from the media itself.

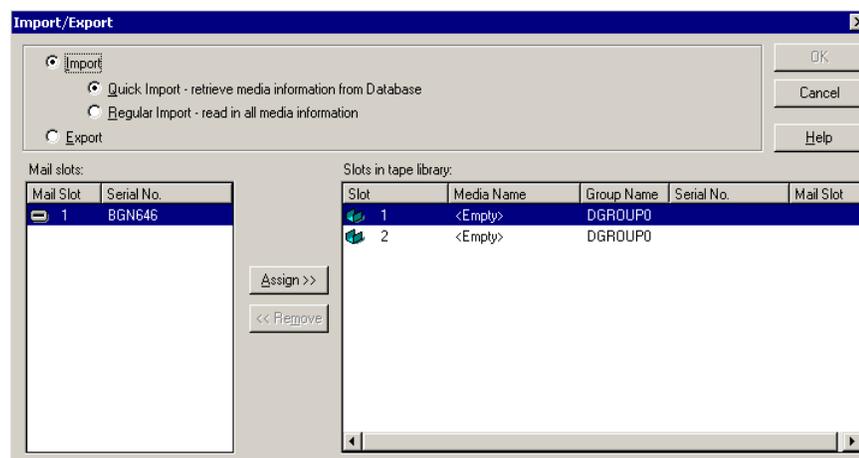
To import media to your library

1. Open the Device Manager and browse to the library that you want to configure.

Select the library in the Device Management tree.

2. Click Import/Export from the tool bar.

The Import/Export dialog opens as illustrated by the following:



3. Choose Import to view all the available empty slots in a media library.

Note: If your library has a bar code reader, the Serial No. field displays the bar code number of your tape. You can use the Serial No. field to identify tapes located in a specific mail slot.

Select the mail slot containing the media you want to assign to your library.

Select the empty slot to which you want to import the media and click Assign.

CA ARCserve Backup imports the media into the library.

Note: It is recommended that you import a cleaning tape to a slot you have already designated as a cleaning slot, or set the barcode as a cleaning tape prefix. You can do this from the Library Properties window of the Device Manager. If you import it to a different slot, you may receive unrecognized media errors.

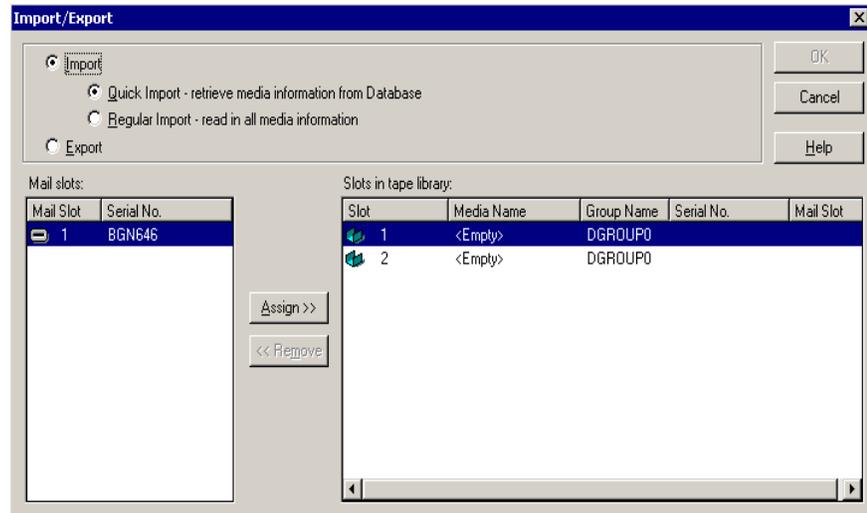
4. Repeat the previous step for each media you want to import.
5. Choose an Import method and click OK.

You have successfully imported media to your library.

To export media from a library

1. Open the Device Manager and browse to the library that you want to configure.
2. Select the library in the Device Management tree.
3. Click Import/Export on the toolbar.

The Import/Export dialog opens as illustrated by the following:



4. Select the Export option to view all the occupied slots in a library.
 Highlight the media you want to export.
 Select the mail slot to export to, and click Assign.
 CA ARCserve Backup exports the media from the library.
5. Repeat the previous step for each media you want to export.
6. Click OK.
 You have successfully exported media from your library.

Clean Media

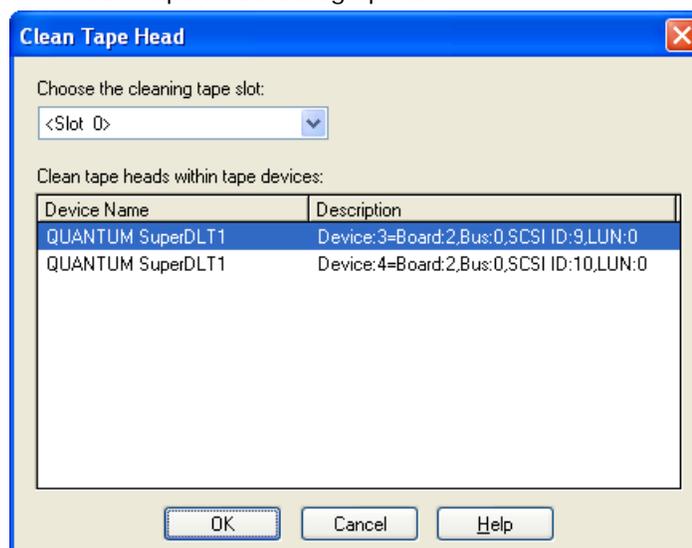
Use this option to clean the tape heads of any media drive in your library.

Note: To use this option, you must have at least one cleaning tape configured in your library.

To clean tape heads

1. Click the Clean toolbar button.

The Clean Tape Head dialog opens.



Note: Offline drives will not be displayed in the list.

2. From the Choose the cleaning tape slot drop-down, select the cleaning slot that you want to use.

From the Clean tape heads within tape device list, select the drive whose head you want to clean.

Click OK.

CA ARCserve Backup cleans the tape heads.

More information:

[Configure a Library](#) (see page 331)

How to Configure Cleaning Slots

This section describes how you can configure more than one cleaning slot.

If supported by your library, you can use CA ARCserve Backup to specify more than one cleaning slot. You can designate a slot based on the following:

- **Slot number**--This option lets you designate specific slots as cleaning slots. You can specify one or more cleaning slots and they do not need to be in a successive order.
- **Bar code prefix**--This option lets you designate slots based on a bar code prefix.

Example 1: If your cleaning tape bar code number is CLN123, specify "CLN*" as the bar code prefix.

Example 2: If you are using more than one cleaning tape, and their bar codes start specify "ABC*" as the bar code prefix.

More information:

[Add Cleaning Slots Based on Slot Number](#) (see page 374)

[Remove Cleaning Slots Based on Slot Number](#) (see page 375)

[Configure Cleaning Slots Based on Bar Code Prefix](#) (see page 375)

Add Cleaning Slots Based on Slot Number

To add cleaning slots based on slot number

1. Open the Device Manager and browse to the library that you want to configure.
2. Right-click the library and select Library Properties from the pop-up menu.
The Library Properties dialog opens.
3. Select the Cleaning tab.
The cleaning options display.
4. Select the Clean by Slot option.
From the Available Slots list, select the slot that you want to designate as a cleaning slot and click the Add button.
The available slot is added to the Clean Slots list.
5. Repeat the previous step to add more cleaning slots.
6. Click OK.
You have successfully added cleaning slots based on their slot number.

Remove Cleaning Slots Based on Slot Number

To remove cleaning slots based on slot number

1. Open the Device Manager and browse to the library that you want to configure.
2. Right-click the library and select Library Properties from the pop-up menu.
The Library Properties dialog opens.
3. Select the Cleaning tab.
The cleaning options display.
4. Select the Clean By Slot option.
From the Available slots list, select the slot that you want to remove.
Click the Remove button to exclude the slot from use as a cleaning slot.
The available slot is removed from the Cleaning Slots list.
5. Repeat the previous step to configure more cleaning slots.
6. Click OK.
You have successfully removed the cleaning slots based on their slot number.

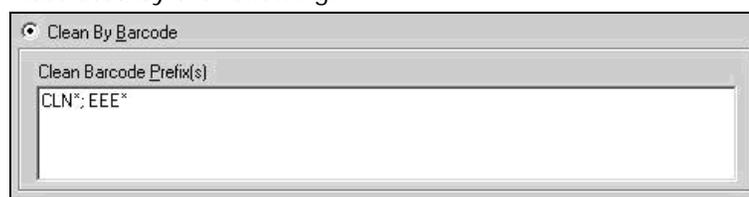
Configure Cleaning Slots Based on Bar Code Prefix

The Clean By Bar Code function lets you specify cleaning slots for your library based on a specific bar code or range of bar codes using a prefix and a wildcard character.

To configure cleaning slots based on bar code prefix

1. Open the Device Manager and browse to the library that you want to configure.
2. Right-click the library and select Library Properties from the pop-up menu.
The Library Properties dialog opens.
3. Select the Cleaning tab.
The cleaning options display.
4. Select the Clean by Barcode option.

Specify the bar code prefixes into the Clean Barcode Prefix(s) field as illustrated by the following:



Note: The asterisk is a wildcard character.

Click OK.

The cleaning slots are set based on their bar code prefix.

Examples: Clean Bar Code Prefixes

The bar code on your cleaning tape is CLN123. In the Clean Barcode Prefix(s) field, specify CLN123.

There are several cleaning tapes in your library. The bar code prefix for the cleaning tapes is ABC. In the Clean Barcode Prefix(s) field, specify ABC*.

There are several cleaning tapes in your library. The cleaning tapes' bar code prefixes are ABC, CLN1, and MX. In the Clean Barcode Prefix(s) field, specify ABC*; CLN1*; MX*.

Offline and Online Removable Drives

CA ARCserve Backup automatically detects removable drives that are connected via Universal Serial Bus (USB) or Serial Advanced Technology Attachment (SATA) to a CA ARCserve Backup primary or member server. Before you can back up data to a removable drive, you must perform a one-time configuration and then bring the removable drive online.

After you perform a one-time configuration, you can specify removable drives as online or offline from Device Manager by right-clicking on the drive and selecting online or offline (depending on the current state of the drive) from the pop-up menu.

Note: If there is media inside the drive that you want to mark as online or offline, eject the media prior to marking the drive offline. CA ARCserve Backup cannot access the media inside a drive that is in an offline state.

CA ARCserve Backup automatically detects and configures removable drives that are connected via USB or SATA to a CA ARCserve Backup primary or member server. Before you can back up data to a removable drive, you must configure the removable drive and then bring the removable drive online.

To specify a removable drive as online

1. Ensure that the removable drive is attached to a CA ARCserve Backup domain primary or member server.
2. Open the Device Manager window and expand the Servers object.
Browse to and select the server to which the removable drive is connected.
CA ARCserve Backup presents you with a list of devices attached to the selected server.
3. From the list of devices attached to the server, select and right-click the removable drive that you want to bring online.
From the pop-menu, select **Online**.
CA ARCserve Backup prompts you to confirm that you want to configure the device.
Note: This message only displays the first time that you bring the removable drive online.
4. Click OK.
CA ARCserve Backup prompts you to confirm that you want to bring the device online.
5. Click OK.
The removable drive is now configured and is in an online state.

Use the **Offline** removable drive option when you want to perform maintenance, repairs, or detach a drive from your CA ARCserve Backup environment. For example:

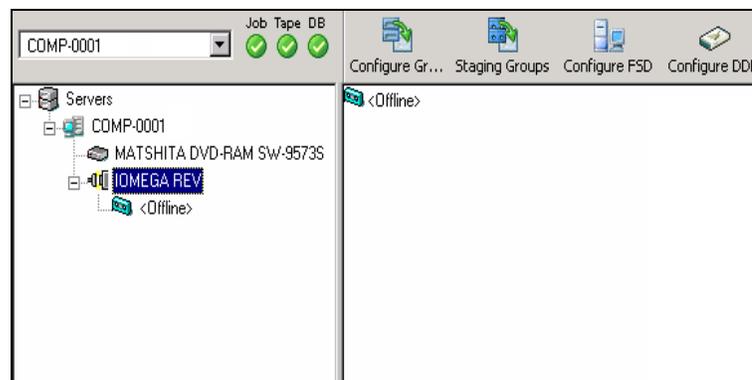
- You do not want to use the removable drive for a period of time and you do not want to overwrite the media in the drive.
- You want to detach the removable drive from the CA ARCserve Backup server so that you can replace it with an identical removable drive, or remove it completely from your CA ARCserve Backup environment.

Important! When the removable drive is offline, jobs associated with the removable drive may fail.

To specify a removable drive as offline

1. Open the Device Manager window, expand the Servers object.
Browse to and select the server to which the removable drive is attached.
CA ARCserve Backup presents you with a list of devices attached to the selected server.
2. From the list of devices attached to the server, select and right-click the removable drive that you want to take offline.
From the pop-up menu, select **Offline**.
CA ARCserve Backup prompts you to confirm that you want to take the removable drive offline.
3. Click OK.
The removable drive is now in an offline state in the Device Manager window.

Note: After you mark the removable drive as offline, *<Offline>* displays in the Device Manager window as illustrated by the following:



How Device Replacement Works

Situations may arise that require you to repair or replace a device that is connected directly to your CA ARCserve Backup server (for example, a single-drive library, tape drive, CDROM, and so on).

When you replace a device, CA ARCserve Backup demonstrates the following behavior:

- After you replace the device with a device that is **different** from the original device and start the Tape Engine, CA ARCserve Backup assumes that the device is a new device and creates a new device group for the device. Since the replacement device is not associated with the original device group, jobs associated with the original device group will fail.

To remedy the failed jobs, you must reconfigure the jobs associated with the original device group and then resubmit the jobs.

- After you replace the device with a device that is the **same** as the original device and start the Tape Engine, CA ARCserve Backup assigns the device to the device group where the original device was assigned.

This behavior ensures that jobs associated with the original device group do not fail.

Limitations:

- The replacement device must be a product from the same manufacturer as the original device.
- The replacement device must be the same type of device as the original device (for example, a single-drive library, a tape drive, and so on).
- The replacement device must be connected to the same adapter and channel as the original device.
- The original device must not be assigned to a RAID device group.
- The CA ARCserve Backup server, where the original device is connected, must not be a member of a SAN domain.

Identify a Library as a VTL

This procedure describes how to set up a library to function as a virtual tape library (VTL).

When you identify a library as a VTL, read performance improves. This capability lets CA ARCserve Backup maximize drive efficiency and overall VTL backup and data migration performance.

Important! You should not identify a physical library as a VTL. When you identify a physical library as a VTL, the library's backup and data migration performance can be adversely affected.

Prerequisite Tasks

Before you can identify a library as a VTL, ensure the following prerequisite tasks are complete:

- Ensure that the Disk to Disk To Tape Option and the Tape Library Option are licensed.
- Ensure that the VTL is properly configured using Device Configuration.
- Ensure that CA ARCserve Backup detects the VTL.

To identify a library as a VTL

1. From the Administration menu in the Navigation Bar on the Home Page, select Device.

The Device Manager window opens.

2. From the Server directory tree, locate the VTL.

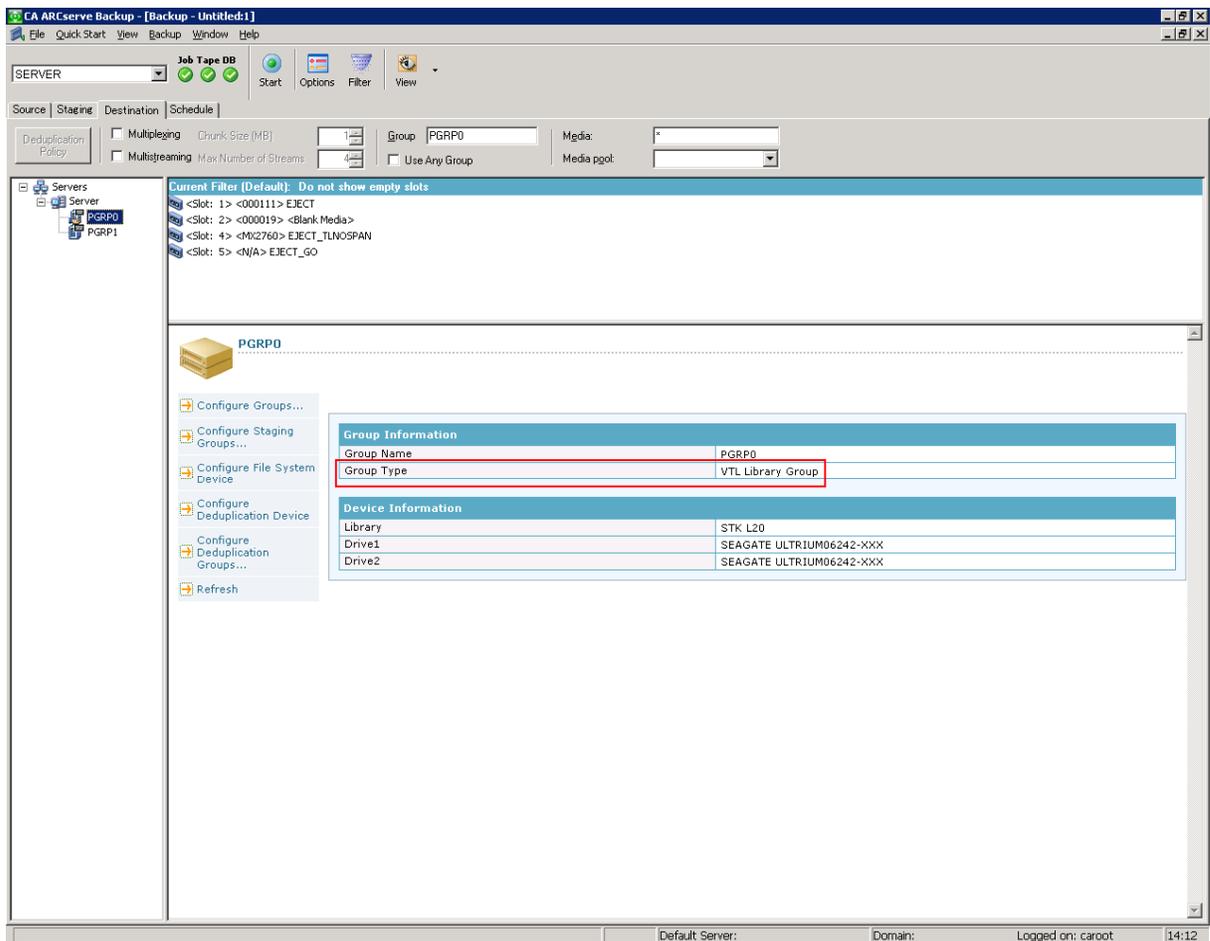
Right-click the VTL and select Library Properties from the pop-up menu.

The Library Properties dialog opens.

3. Select the General tab.

In the VTL (Virtual Tape Library) section, check the Library is a VTL check box and click OK.

The library is identified as a VTL as illustrated by the following screen: .



Note: If you do not want to identify a library as a VTL, repeat the above steps and remove the check mark from the Library is a VTL check box.

Media Movement

When you insert a media into a magazine slot or remove a media from a slot, you must either inventory this slot or remount the magazine.

Important! If you are manually inserting media into a library, always insert media into slots, never into its library drives.

Device Group Configuration Using the Device Manager

CA ARCserve Backup lets you separate the slots in your library into groups. Grouping slots lets you run several types of jobs at the same time. Additionally, if you have several slots in a group, you can let the library span the media in the group for you.

By default, the first time you start the Tape Engine, all the slots in each library you have attached to your machine are automatically assigned to that library group.

After you start CA ARCserve Backup, you can use the Device Manager to:

- [Create new groups](#) (see page 382).
- [Assign slots to groups](#) (see page 383).
- [Remove slots from groups](#) (see page 385).
- [Delete groups](#) (see page 385).
- [Rename groups](#) (see page 385).

Example: Library Configuration Using the Device Manager

For example, if you have two libraries attached to your machine, you will have two library groups—all the slots in the first library are assigned to GROUP0, and all the slots in the second library are assigned to GROUP1. You can retain these library group names, or you can regroup and rename them. Since each slot in a library is viewed as a virtual storage drive, each slot can be assigned its own group.

Create a New Library Group

To create a new library group, you must first open the Device Group Configuration dialog. The following are methods you can use to open the Device Group Configuration dialog.

- From the Device Manager, click the Device menu and select Configure Groups.
- From the Device Manager window or the Staging tab in the Backup Manager window, click the Configure Groups option located in the device properties preview pane, as shown in the following example.



Note: To access the Device Group Configuration dialog using a wizard-like application, from any manager window, click the Configuration menu and select Device Group Configuration.

To create a library group

1. From the Device Manager, click the Device menu and select Configure Groups.

The Device Group Configuration dialog opens. Existing groups, and the slots assigned to each group, are listed here. If you have reserved one of your slots for cleaning media, it cannot be assigned to a group and it does not appear in this dialog.

2. Click New.

The New Group dialog displays.

3. Enter a name for the library group and click OK.

The new library group displays in the Groups field. You can now begin assigning slots to this group.

Assign Slots to a Library Group**To assign slots to a library group**

1. From the Administration menu in the Navigation Bar on the CA ARCserve Backup Manager Console, select Device Group Configuration.

The Device Group Configuration Welcome dialog opens.

2. Click Next.

The Login Page dialog opens.

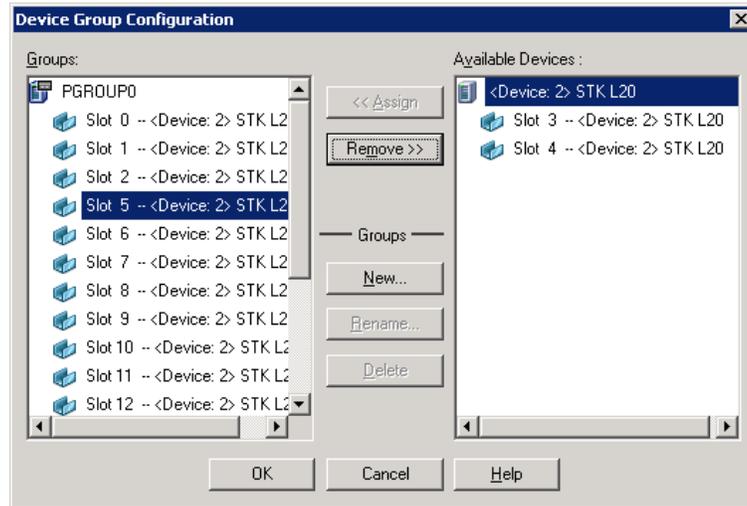
3. Complete the required fields on the Login Page dialog and click Next.

The Options dialog opens.

4. Select the server that you want to configure, click the Configure Groups option, and then click Next.

The Device Group Configuration dialog opens.

Library devices and their corresponding slots available for assignment display in the Available Devices list, as shown in the following example.



5. From the Available Devices list, select the slots that you want to assign to a group. You can select one available slot at a time, or you can select the library to assign all of its available slots to a group.
6. From the Groups list, select the group to which you want to assign the slot.
7. Click Assign.

CA ARCserve Backup removes the slot from the Available Devices list and places it in the Groups list, below the group to which it was assigned.

8. Repeat Steps 5 through 7 to assign more slots to groups.

Note: If there are no slots available, you can remove them from their currently assigned group to make them available to other groups. To do this, from the Groups list, select the slot that you want to make available to other groups and click Remove. The slot is now available to other groups. You can now perform Steps 5 through 7 to assign the slot to a different group.

9. When you are finished, click Finish, and then click Exit to exit Device Group Configuration.

You have successfully assigned slots to a library group.

Remove Slots from a Library Group

To remove slots from a library group

1. From the Device Manager, click the Device menu and select Configure Groups.

The Device Group Configuration dialog displays.

2. Highlight the slot you want to remove. Slots are listed in the Groups list beneath the name of the group to which they were assigned.

3. Click Remove.

The slot is removed from the group to which it was assigned in the Groups list and placed in the Available Devices list.

4. Repeat Steps 2 and 3 to remove more slots from groups.
5. When you are finished, click OK.

You have successfully removed slots from a library group.

Delete a Library Group

To delete a library group

1. From the Device Manager window, click Configure Groups (from the list of functions) or click the Groups toolbar button.

The Device Group Configuration dialog box opens.

2. Select the group you want to delete.
3. Click Delete, and then click OK to confirm.

The group is removed from the Groups list. Any slots that were assigned to the group are placed in the Available Devices list.

Rename a Library Group

To rename a library group

1. From the Device Manager window, click Configure Groups (from the list of functions) or click the Groups toolbar button.

The Device Group Configuration dialog opens.

2. Select the group you want to rename and click Rename.

The Rename Group dialog displays.

3. Enter a new name for the group and click OK.

The new group name is appears in the Groups list.

Universal Serial Bus (USB) Storage Devices

CA ARCserve Backup can detect the following types of Universal Serial Bus (USB) storage devices that are connected to the CA ARCserve Backup server:

- Tape drives
- Media changers
- USB removable drives

After you connect the USB storage devices to your CA ARCserve Backup server, you can use them for all of your backup and restore operations.

Note: If you disconnect USB devices from the CA ARCserve Backup server and do not restart the Tape Engine after disconnection, you can manually assign the disconnected devices to new groups. These assignments are activated after you reconnect your devices to the server and restart the Tape Engine. If you restart the Tape Engine after disconnecting USB devices from the CA ARCserve Backup server, you cannot manually assign the disconnected devices to new groups.

Configure USB Storage Devices

Use the Scan Device option to enable CA ARCserve Backup to detect and enumerate USB storage devices. You can start the Scan Device option by clicking the Scan Device button on the Device Manager toolbar.

Important! The drivers for the USB storage device must be installed on the CA ARCserve Backup server in order for CA ARCserve Backup to detect and communicate with the devices.

Note: For more information about configuring USB storage devices, see Scan Device Option.

More information:

[Scan Devices](#) (see page 362)

Prerequisites for Backing Up to Removable Drives

Before you can back up to removable drives, you must:

- Ensure that the media is formatted to the NTFS or FAT32 filesystem.
Note: If you need to format or reformat the media, consult the manufacturer's documentation for formatting guidelines, or use a Windows-based application to format the media.
- Attach the removable drive to a CA ARCserve Backup domain primary or member server.
- Status the removable drive as online.

Format Removable Media

After CA ARCserve Backup detects your drive, you must format the removable storage media as a CA ARCserve Backup storage media. In the CA ARCserve Backup graphical user interface, removable media is represented as if it is tape media. This is not an error. CA ARCserve Backup treats removable media in the same manner as tape media.

Note: Various manufacturers provide you with pre-formatted media that needs to be manually formatted before you can use it. For more information about how to format the media for the drive you are using, see the manufacturer's documentation.

To format removable media

1. Open the Device Manager window and expand the Servers object.
2. Browse to the server to which the removable drive is connected.
3. Select and right-click the removable drive.
4. From the pop-up menu, select Format media.
CA ARCserve Backup formats the media.

How You Can Configure Removable Device Groups

You configure removable device groups through the Device Management feature. Using this feature, you can perform the following tasks:

- Create or delete new removable device groups.
- Rename removable device groups.
- Assign or remove individual devices from a device group.

Note: You cannot assign a removable drive into a group of media drives. You must create a new group for the removable devices.

Filter Libraries

You can use filters to configure the Device Manager to display only the information you need, thereby increasing data manageability and application performance.

To filter libraries

1. Open the Device Manager window and select Preferences from the View menu.

The Preferences dialog opens.

2. Select the Library Filter tab and specify the filter options that are appropriate to your needs:

Show Empty Slots

Select this option to view the empty slots in the library.

Show Slots Between

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

Select this option to view the blank media in the library.

Show Tapes within Media Pool

Select this option to view the tapes within a particular media pool. Wild cards ("*" and "?") are accepted in the media pool.

Show Tapes Matching Serial

Select this option to view the tapes that match a certain serial number. Wild cards ("*" and "?") are accepted in the serial number.

Show Write Protected Media in Format/Erase dialogs

Select this option to view write-protected media in all Format and Erase dialogs.

If a filter was applied to the current manager, the status bar will indicate it by displaying FILTER in the second panel and it will be detailed in the right panel of the view.

Note: Select the Clear button to clear all the fields of their information and remove all library filter criteria.

3. Optionally, click the Save as Default button after you have entered the criteria for your library filter to apply the filtering criteria to all Device Manager views.

4. Click Apply.

The filtering criteria are applied to the current view.

Note: Click the **Cancel** button to discard the changes to your filtering options.

Removable Drive Support

CA ARCserve Backup supports SCSI and USB removable devices allowing you to back up data, restore data, scan sessions, merge removable sessions, and manage removable media on your removable devices. The Backup Manager identifies and treats the removable media as tape media.

Note: To access the most up-to-date list of certified devices, click the Technical Support link on the CA ARCserve Backup Home Page.

Write Once Read Many (WORM) Support

CA ARCserve Backup allows you to back up your data either to rewriteable media or WORM media. WORM media, with significantly longer shelf life than magnetic media, manifests secure, long-term storage for data you do not want to erase.

CA ARCserve Backup lets you mix WORM and non-WORM media in a library. From the Device Manager, you can identify WORM media by an icon with the letter "W" inside a red circle. In addition, CA ARCserve Backup lets you specify WORM media for custom backup jobs.

The Backup Manager contains three options for Daily, Weekly, and Monthly WORM media rotations for use with GFS rotations. You can locate these options on the Backup Manager, Schedule tab, when you specify the Use Rotation Scheme option.

WORM Media Supported

CA ARCserve Backup supports backing up data to the following WORM media:

- DLT WORM (DLTIce)
- STK Volsafe
- IBM 3592 WORM
- LTO3 WORM
- SAIT WORM

WORM Media Considerations

The following list describes situations that can occur when using a DLT WORM device with DLT WORM media and how CA ARCserve Backup responds to such situations.

- When a backup job spans tapes and the media is WORM media, CA ARCserve Backup needs WORM media to complete the job.
 - If a blank WORM media is not available, and a blank DLT WORM-capable media is available, CA ARCserve Backup automatically converts blank DLT media to DLT WORM media and then completes the backup job.
 - If WORM media is not available for a WORM job to continue, CA ARCserve Backup does not convert non-blank media to WORM media.

- When you are running a backup job that specifies Use WORM Media and there is no WORM media available, CA ARCserve Backup may convert blank WORM-capable media to WORM media for the job.

Note: For these scenarios, the available WORM media must be DLT SDLT-II or higher.

WORM Media Limitations

If you use WORM media, certain CA ARCserve Backup features, specifically those involving media pools, reformatting, and overwriting or reusing media, are disabled because of the nature of the media. These limitations include the following:

- You cannot erase WORM media.
- You cannot submit an Overwrite job to WORM media.
- You cannot format WORM media unless the media is blank.
- You cannot use WORM media for multiplexing jobs.
- CA ARCserve Backup does not automatically assign WORM media to the Scratch Set in a media pool. WORM media cannot be recycled and as such, is always assigned to the Save Set in a media pool.
- CA ARCserve Backup cannot use WORM media with optical devices, file system devices, and the CA ARCserve Backup Tape RAID Option.
- In cross-platform SAN environments, UNIX and NetWare do not support WORM media.

Device Group Configuration

Device Group Configuration is an application that you can use to configure device groups and staging groups.

Using Device Group Configuration you can:

- **Configure groups**--Create, remove, and rename groups, and define device to device group relationships (assign and unassign).
Note: CA ARCserve Backup lets you create a maximum of 128 device groups.
- **Configure device group policies**--Set staging group policies as it relates to disk thresholds and the maximum number of simultaneous streams of data.
- **Pause data migration**--Pause the process of copying data to its final destination in the event the final destination media is not available (for example, you are performing maintenance activities on a library).

To start Device Group Configuration, select Device Group Configuration from the Administration menu in the Navigation Bar on the CA ARCserve Backup Manager console. After the Welcome to Device Group Configuration dialog opens, follow the prompts and complete the required fields to complete the configurations.

DLTSage Error Handling

DLTSage is an error monitoring, reporting, and alerting technology developed by Quantum for use on SuperDLT tape drives. To receive tape drive alerts, you must use SuperDLT tape drives with DLTSage firmware.

CA ARCserve Backup interfaces with the firmware on SuperDLT tape drives to analyze critical tape drive and media performance parameters collected for each track, segment, Magneto Resistive (MR) channel, and optical band. CA ARCserve Backup uses the information collected to:

- Diagnose information such as threshold conditions and tape drive history.
- Identify high-risk tape drives and media that are approaching or have reached their end of life.
- Predict tape drive cleaning needs.
- Analyze tape drive environmental conditions.
- Generate media and hardware error messages.

How DLTSage Error Handling Works

CA ARCserve Backup queries DLTSage using a SCSI Log Sense. If a hardware or media error occurs as a backup job starts, during a backup job, or after a backup job ends, CA ARCserve Backup uses the information captured from the SCSI Log Sense to generate tape drive error messages that display in the Tape Log and the Activity Log.

An error message displays if any of the following conditions exist:

- The tape drive is experiencing difficulties reading from or writing to a tape.
- The tape drive cannot read from or write to a tape, or the media performance is severely degraded.
- The media exceeded its life or maximum number of passes expectancy.
- The tape drive may have a clogged head or needs cleaning.
- The tape drive has a cooling problem.
- There is a potential tape drive hardware failure.

If an error condition is detected, CA ARCserve Backup may attempt to automatically correct the problem and complete the job. However, you must install the CA ARCserve Backup Tape and Optical Library Option to use the capabilities of uninterrupted inline cleaning, drive usage balancing, and error-preventive drive selection features. For more information about automated error resolution, see the *Tape Library Option Guide*.

If the CA ARCserve Backup Tape Library Option is not installed, you must cure the error condition or problem area manually. See the manufacturer's documentation, as necessary.

How CA ARCserve Backup Cures Tape Drive Errors

If an error condition occurs, CA ARCserve Backup makes a second attempt to complete the job. If the error persists, CA ARCserve Backup stops the backup job. The tape drive then relays the information about the error condition to CA ARCserve Backup. You can view the details about the error condition in the Activity Log.

After determining the cause of the error condition and curing the problem, you must restart the job.

How to Ensure that CA ARCserve Backup Spans Media in a Single Drive Autoloader

When CA ARCserve Backup backs up data to a single drive autoloader, and detects there is no blank media at spanning, CA ARCserve Backup pauses the job at spanning to let you insert blank tapes into the drive. This behavior is designed to ensure that backup data spans media properly.

When CA ARCserve Backup spans media and detects no blank media in a single drive library, the events that follow occur:

1. CA ARCserve Backup pauses the job and prompts you to insert blank media into the autoloader.

Note: If there are no empty slots, you can replace older media with blank media. However, you must ensure that you do not remove the media that was recently spanned. If you insert media that is not blank, you may inadvertently erase the data from the media using Device Manager.

2. After you close the door to the autoloader, CA ARCserve Backup inventories all media in the slots.

If the inventory process does not start automatically, you can inventory the media manually using Device Manager.

Note: You must wait for the inventory process to finish, which can take several minutes to complete.

After the inventory process is complete, the backup job resumes using the blank media, after you click OK on the message box that prompted you to replace the media.

To ensure that CA ARCserve Backup spans media in a single drive library

1. Open the Device Manager and browse to the autoloader.
Right-click the device and select Library Properties from the pop-up menu.
The Library Properties dialog opens.
2. Click the General tab.
Clear the Set unknown bar code media to not inventoried during initialization check box.
Click OK.
CA ARCserve Backup inventories the blank media automatically when spanning is required.

Important! If you do not perform the above steps, you must inventory the media manually using Device Manager.

Media Assure

From the Media Assure & Scan Utility, you can select the Media Assure button to display the Media Assure Option dialog. This dialog allows you to enable a media assure operation, which helps you ensure that the sessions on the media are restorable. A Media Assure job scans sessions randomly based on specified criteria.

After a Media Assure & Scan job completes, check the Activity Log in the Job Status Manager for errors. Based on the nature of the errors, you can take corrective actions to remedy the error.

Note: For the Media Assure feature, it depends on the session records in the CA ARCserve Backup database. So, if there are no records for the media in the database or the session records for this media have been destroyed, media assure will not scan any sessions.

Enable Media Assure

Check this option to enable a media assure scan job that will select some sessions to scan randomly. Otherwise, it is a regular scan job.

Scan all data in a session

Select this option to scan all session details.

Scan only session headers for each session

Select this option to scan session headers only and not the session details. This is quicker than scanning all data in a session, however it may be harder to find the problem.

Scan sessions that match the following criteria:

Sessions that were backed up in the last (number) Days

Specifies the number of days that sessions were backed up to include in the Media Assure operation. The default is 7 days. So, all sessions that were backed up in the last 7 days will be scanned.

Choose session no more than

Limits the number of sessions scanned, because there are too many sessions that can fit a scan condition. The default is 20%. A percent or numerical value can be selected.

Specify the Nodes for which the sessions should be scanned (Using "," to separate)

Indicates the sessions to scan in the specified nodes. This can be a wildcard match. For example, if you specify the node name ARC*, sessions will be selected from the node name ARC001 and the node name ARC002. If you don't specify any node name, then any session in all nodes may be selected. By default, all sessions in all nodes may be selected.

How Uninterrupted Drive Cleaning Works

A contaminated tape drive condition is usually discovered when you are running a backup job. A significant number of tape drive and media errors can be remedied by cleaning the tape drive.

For CA ARCserve Backup to perform uninterrupted drive cleaning, you must have a cleaning tape installed in the tape cleaning slot specified during setup, and a specified cleaning schedule. If you did not specify a cleaning schedule, CA ARCserve Backup defaults to a 100 hour period between scheduled tape cleaning operations.

If CA ARCserve Backup detects a contaminated tape drive condition during a backup job, and a cleaning slot is configured, CA ARCserve Backup automatically performs the following analyses and actions:

- If CA ARCserve Backup detects a write error during a backup, and the symptoms relate to a contaminated tape drive or media, CA ARCserve Backup makes a second attempt to write to the tape drive.
- If the second write attempt fails, CA ARCserve Backup cleans the tape drive if one or more of the following conditions exist:
 - The tape drive was never previously cleaned.
 - DLTSage detected the need to clean the tape drive and drive usage exceeds one fourth of the scheduled cleaning.
 - Tape drive usage exceeds one third of the cleaning.
 - The user specified ForceClean the tape drive.

If CA ARCserve Backup determines that a tape drive must be cleaned to continue a job, the following actions take place:

1. CA ARCserve Backup pauses the job.
2. The library returns the tape to its home slot and locks the tape drive.
3. CA ARCserve Backup directs the cleaning operation.
4. The library reloads the tape into the cleaned drive and aligns the tape with the buffer.
5. CA ARCserve Backup resumes the job.

How to Optimize Tape Usage

Suppose you have a scenario where you have multiple disk staging backup jobs or multiple GFS Rotation backup jobs, and each job formats its own tape for incremental or differential backups. If the incremental or differential size of the data is lesser than the capacity of the tapes, the tape usage will not be optimized and space on the tapes will be wasted. In addition, using more tapes will increase the requirement for the number of slots in a tape library and can also result in the need to ship more tapes off-site.

There are two approaches to resolving this problem: [Media Maximization](#) (see page 396) and [Consolidation During Migration](#) (see page 397).

Media Maximization

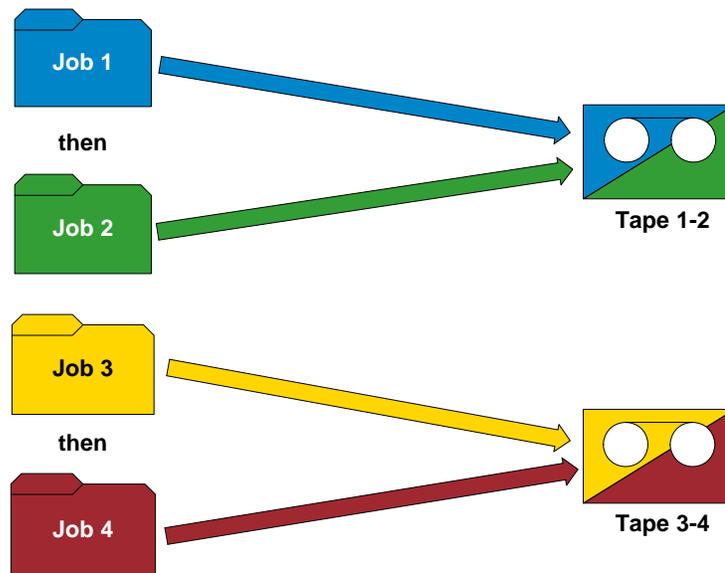
Media maximization is a process that helps optimize disk and tape usage in GFS and rotation jobs. In a GFS or rotation job, when data is backed up on a scheduled basis to the same media pool, CA ARCserve Backup automatically appends the newly backed up data on to a partially filled tape, instead of formatting a new tape each time. Using media maximization, you can optimize disk and tape space and also reduce the number of tapes needed to store your GFS rotation job data.

Media maximization can be used with the types of jobs that follow:

- GFS jobs
- Disk staging GFS jobs
- Disk staging rotation jobs
- Custom disk staging jobs using media pools to append backup data

Note: CA ARCserve Backup applies media maximization to a GFS Rotation job only if the specified media pool prefix is the same for those sets of jobs that are intended to use media maximization. For example, you can consolidate data from Job 1 and Job 2 on to the same tape in media pool A, and you can also consolidate data from Job 3 and Job 4 to another tape in media pool B.

However, in the media maximization process, CA ARCserve Backup does not back up data to a media that is already being used by an active backup job. So, you must ensure that the backup job schedule or migration schedule (in a staging job) is configured so that the backup or migration of data is sequential. If CA ARCserve Backup detects that the media is currently in use, it will revert to formatting a new tape for the second job, rather than wait for the first job to complete.



Consolidation During Migration

Consolidation during migration is a process to help optimize tape usage in staging jobs. Consolidation during migration can be used in a custom job, rotation job, or GFS rotation job.

In a staging job, when data is migrated (or copied) from the staging area to the same media destination (same media pool prefix), the consolidation during migration option allows you to append migrated data onto a partially filled tape, instead of formatting a new tape each time. Through the use of the consolidation during migration option, you can optimize tape space and also reduce the number of tapes needed to store your migrated data.

The consolidation during migration option is similar to the media maximization feature and data will not be migrated to a media that already has an active migration job in process. However, with this option you no longer have the responsibility of scheduling each job so that the next migration job is not started before the previous migration job has been completed. If you select this option, CA ARCserve Backup will automatically detect if the media is currently in use, and if it is, will wait for the current migration job to complete before starting the next migration job. To consolidate data during migration you need to specify the same exact target media prefix and target media pool prefix so that data belonging to different jobs can be consolidated to the same exact tape.

The "Consolidate data across jobs while copying" option (on the Staging Policy Miscellaneous tab dialog), allows you to specify if you want to consolidate the data from different jobs onto a single tape during migration.

Example: Consolidate Data During Migration

You can consolidate data from Job 1 and Job 2 onto the same tape, and you can also consolidate data from Job 3 and Job 4 to another tape. In this scenario you would need to do the following:

- When submitting a backup of Job 1, choose consolidation. Specify the media prefix as AAA and the media pool as MP1.
- When submitting a backup of Job 2, choose consolidation. Specify the media prefix as AAA and the media pool as MP1.
- When submitting a backup of Job 3, choose consolidation. Specify the media prefix as BBB and the media pool as MP2.
- When submitting a backup of Job 4, choose consolidation. Specify the media prefix as BBB and the media pool as MP2.

If you want data to be consolidated from Jobs 1 and 2 and from Jobs 3 and 4, you must specify the exact same media prefix and the exact same media pool in each submitted job. Since the consolidation has to be done to the same tape set you must also choose the same tape library group in the target destination. In addition, the jobs which are supposed to consolidate must run on the same backup server.

Important! If any of these four parameters are different (Media Prefix, Media Pool, target destination, and backup server), the data will NOT be consolidated to the same tape set.

You can also specify the copy method as either to overwrite the data on a tape or to append to the data on an existing tape.

Overwrite

If you have a requirement to consolidate data across multiple jobs and ship the tapes on a daily basis, you should choose the “Overwrite” option. This will ensure that a tape is formatted on a daily basis and all the data backed up on that day would be migrated to a single tape.

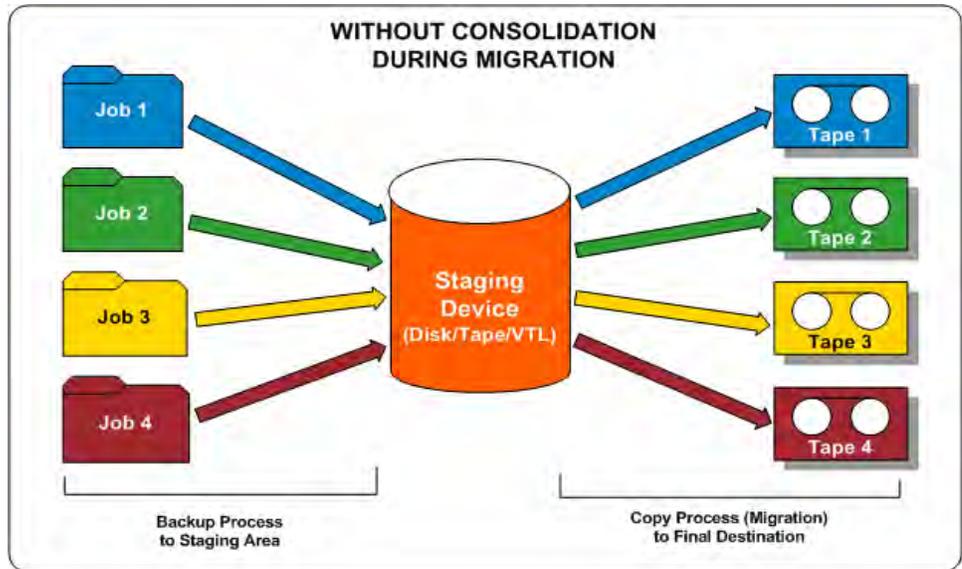
For example, if you have two jobs (Job 1 and Job 2) and you want to ship the tapes offsite on a daily basis. In this scenario you would choose Overwrite. When the backup job finishes on Monday, CA ARCserve Backup would format a final tape for Monday and copy the data from the staging tapes of Jobs 1 and 2 to the final tape. Then, after the backup finishes on Tuesday, CA ARCserve Backup would format a final tape for Tuesday and copy the data from staging tapes of Jobs 1 and 2 to the final tape. This way a tape is formatted every day and helps you to ship the tapes offsite on a daily basis.

Append

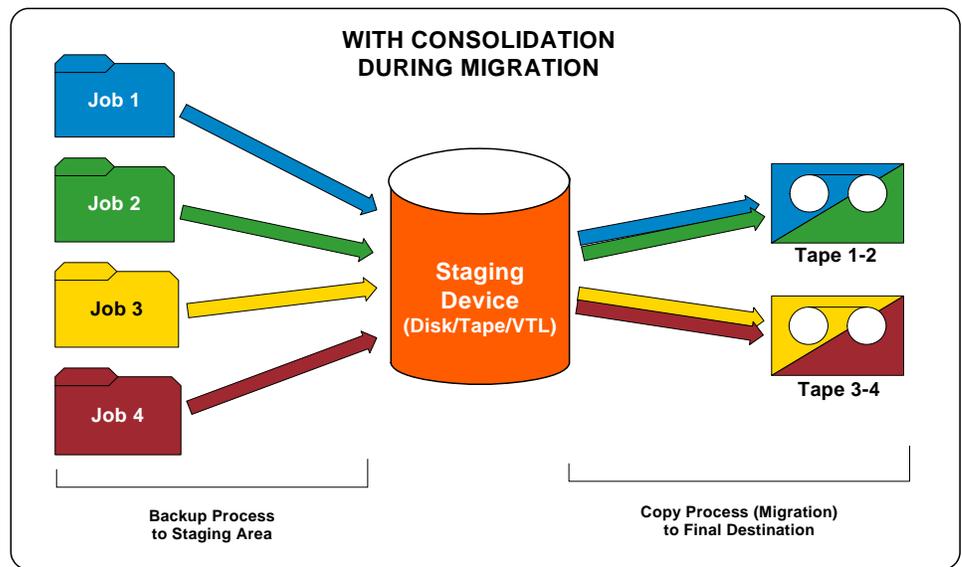
If you have a requirement to consolidate data across multiple jobs (for daily backups) for the whole week to a single tape and ship the tapes on a weekly basis, you should choose the “Append” option. This will ensure that for example, in 5-day GFS rotation jobs, all the incremental or differential data (belonging to different jobs) that are backed up on Monday, Tuesday, Wednesday, and Thursday is consolidated to one tape set. The full backups that happen (for different jobs) on Friday would be consolidated to another tape set.

For example, if you have two jobs (Job 1 and Job 2) and you don't want to ship the tapes offsite on a daily basis. In this scenario you would choose Append. When the backup job finishes on Monday, CA ARCserve Backup would format a final tape for Monday and copy the data from the staging tapes of Jobs 1 and 2 to the final tape. Then, after the backup finishes on Tuesday, CA ARCserve Backup would copy and append the data from staging tapes of Jobs 1 and 2 to the final tape from Monday. A new tape would not be formatted and only one tape would be formatted for the entire week of daily backups. This helps you utilize your tapes more efficiently.

The following diagram shows the tape usage requirements if you do not enable the consolidate during migration option:



The following diagram shows the tape usage requirements if you enable the consolidate during migration option:



How Media Pools Work

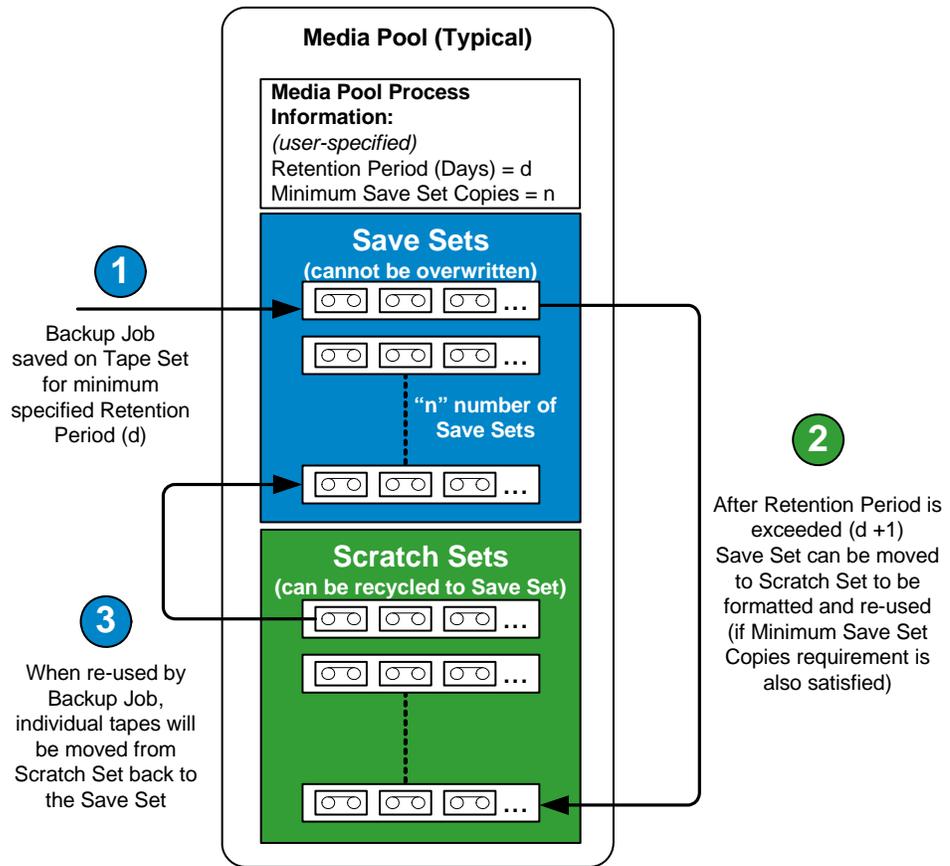
Each media pool is divided into Save Sets and Scratch Sets. These sets are used in conjunction with each other to control the preservation of backup data on tapes until your specified criteria has been met and then allows you to recycle these tapes for reuse. The two user-defined retention criteria are:

- the minimum number of media that must be contained in the Save Set
- the retention period (in days)

Example: Media Pool Used in a Rotation

During a 5-day work week, daily backups are performed on Monday, Tuesday, Wednesday, and Thursday. Each of these daily backups have their own set of backup media (daily Save Sets) that are retained for four days (the user-specified retention period). On the fifth day (Friday), a weekly Save Set is created and the daily Save Set from the previous Monday becomes part of the Scratch Set, so that it can be reused (overwritten). In other words, on the next Monday, and the daily media pool from the previous Monday becomes part of the Scratch Set and can be reused for this Monday's backups. After the new Monday backup is completed, the Scratch Set for that day becomes the Monday Save Set and is retained all week.

The following diagram shows how a typical media pool processes a backup job and the movement of Save Sets and Scratch Sets within a media pool:



Save Sets

The media pool Save Set is a set of media that cannot be overwritten until the media pool's retention requirements that you specify have been met. You can modify Save Set information for all Custom backup jobs, move media from the Save Set to the Scratch Set, or you can move media from one media pool Save Set to another media pool Save Set.

You define the minimum number of media that must be contained in the Save Set and the retention period (in days). These settings determine how long media will be held. After both of these criteria have been satisfied, CA ARCserve Backup releases the oldest media in the Save Set back into the Scratch Set, where it can be recycled and re-used (overwritten).

- The retention period is the number of days in which a media has not been used (written to) before it is moved into the Scratch Set. For example, if you specify a retention period of 14 days, a media remains in the Save Set if it has been used within that specified time. If the media has not been used for 14 days, it is moved to the Scratch Set.
- The minimum number of media contained within the Save Set is the number of media that must be retained in the Save Set before the older media are recycled to the Scratch Set. This is a safeguard for preventing data loss in case backups are not done for extended periods of time.

Note: You will receive a warning if you attempt to format or erase media that is contained in a Save Set.

Scratch Sets

The media pool Scratch Set is a set of media that has been recycled from the Save Set after its specified retention criteria has been satisfied. The media from the Save Set that can be re-used and overwritten are placed in the Scratch Set after they have met the specified criteria (the minimum number of media to save and retention period). The oldest media in the Scratch Set, those that have not been used for the longest period of time, are used first.

Each time a media in the Scratch Set is used, it moves from the Scratch Set to the Save Set. The media moves back to the Scratch Set once the specified retention criteria have been met. If the media meets these retention criteria, CA ARCserve Backup prompts for a blank tape or accepts media from the Scratch Set.

CA ARCserve Backup performs media pool maintenance at the beginning of a job, and will not allow media in the Save Set to be moved to the Scratch Set until the two retention criteria are met. When you select a media pool Scratch Set in the left pane of the Media Pool Manager, the right pane will display the media pool name, the set name, the owner name, and the date the Scratch Set was created.

Save Sets and Scratch Sets

The set of media containing important data that cannot be overwritten is called the Save Set. You can move media from the Save Set in one media pool to the Save Set in another media pool. Media that has not been formatted for the longest period will be used first.

Note: You will receive a warning if you try to format or erase media in a Save Set.

When the media meets certain criteria in a Save Set (minimum number of media in Save Set and retention period) they are recycled to the Scratch Set. Each time a media in the Scratch Set is written to, it moves from the Scratch Set to the Save Set. Additionally, if CA ARCserve Backup detects non-blank media in the Scratch Set, the Media Pool Manager controls the usage of the media such that WORM media containing data is not used.

The retention period is the number of days in which a media has not been used before it is moved into the Scratch Set. For example, if you specify a retention period of 14 days, a media remains in the Save Set if it has been used within that specified time. If the media has not been used for 14 days, it is moved to the Scratch Set.

You define the minimum number of media contained within the Save Set. This is the number of media to be retained in the Save Set before the older media are recycled to the Scratch Set. This is a safeguard for preventing data loss in case backups are not done for extended periods of time.

Media pools apply to every media, regardless of which backup type and method were selected. CA ARCserve Backup performs media pool maintenance at the beginning of a job, and will not allow media in the Save Set to be moved to the Scratch Set until two criteria are met:

- The oldest tape in the Save Set is compared and exceeds the retention time.
- The minimum required number of media is in the Save Set.

If the media meets these criteria, CA ARCserve Backup prompts for a blank tape or accepts media from the Scratch Set.

Serial Numbers

The serial number of a media is one way to categorize media pools. You cannot change the serial number of media, but you can create a serial number for media by:

- **Bar code**--A number is read from a bar code label and this number becomes the serial number. A changer with a bar code reader is required for this method. This will override any previously defined media pool settings.

- **Automatic**--CA ARCserve Backup automatically assigns a serial number for the media based on the base and range of serial numbers set when the pool was created.
 - **Base**--This is the base number, which CA ARCserve Backup will use when automatically assigning serial numbers. The first media formatted will have the same serial number as the base number. Each media's serial number thereafter will be increased by one.
 - **Range**--You can specify the range (up to 31 digits) from which the media pool serial numbers will be categorized.

GFS Media Pools

Grandfather-Father-Son (GFS) Rotation media pools are based on basic media pooling architecture.

GFS Rotation jobs use three media pools: Daily, Weekly, and Monthly, which are based on the information you enter in the Media Pool Name Prefix field when submitting the job.

When a GFS Rotation job runs, CA ARCserve Backup automatically formats and names your media according to the backup type, media pool, and date using the following syntax:

(backup type)-(user-defined media pool prefix)-(day-of-the-week)-(date)

Where..	Is...
backup type	F - full backup I - incremental backup D - differential backup W - weekly backup M - monthly backup A - all daily backups (full, incremental, and differential) when you use the Media Maximization option (enabled by default) and enable the Append Media option. For more information on the Media Maximization option, see the section Media Maximization in GFS Rotation Jobs.
user-defined media pool prefix	The name you assigned to the media pool for your GFS Rotation scheme.
day of the week	An abbreviation for the day of the week on which the job was performed.

Where..	Is...
Date	The date on which the backup was performed in mm/dd/yy format.

This media naming convention allows you to easily identify backup media. For example, the media used for the first full backup in your rotation scheme will have the following name: F TP MON 11/1/05.

Note: CA ARCserve Backup prevents you from using the underscore character (_) and the hyphen character (-) when specifying Media Pool names.

Five-day rotation schemes have the following retention times for each media pool:

- **Daily (_DLY)**--six days (daily media in seven-day Rotation Schemes have a retention time of eight days)
- **Weekly (_WLY)**--five weeks
- **Monthly (_MLY)**--343 days

The following are the formulas used for calculating the number of media in the Save Sets and the retention times for the GFS media pools:

- **Daily pool**--This pool holds the media for daily backup jobs. The default retention period is six days and the number of Save Set media is based on the number of daily media in the GFS Rotation minus one [# of daily media -1].
- **Weekly pool**--This pool holds the weekly media. The retention period equals the number of weekly media times seven, minus one [(# of weekly media * 7) - 1]. The number of save media is based on the number of weekly media in the GFS setup minus one [# of weekly media - 1].
- **Monthly pool**--This pool holds the monthly media. The retention period equals the number of monthly media times 29 minus five [(# of monthly media * 29) - 5]. The number of save media is based on the number of monthly media in the GFS setup minus one [# of monthly media - 1].

For more information on rotation schemes, including information on how to submit a rotation backup job, see the online help.

More information:

[Media Maximization in GFS Rotation Jobs](#) (see page 407)

Media Maximization in GFS Rotation Jobs

By default, CA ARCserve Backup enables the Media Maximization option, which lets you submit multiple GFS backup jobs using the same media pool. By sharing the same media pool, you can append multiple jobs to the same tape sets rather than creating new tape sets for each job. This drastically reduces the amount of media you use when submitting GFS Rotation jobs.

Note: To disable the Media Maximization option, set the NT registry DWORD value EnableMediaMaximization to 0. This registry key is as follows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve  
Backup\Base\Task\Backup
```

More information:

[GFS Media Pools](#) (see page 405)

How You Can Maximize the Use of Media

To take full advantage of the Media Maximization option, use the following guidelines when submitting GFS backup jobs using the same media pool:

- **Use the same Rotation Scheme**--GFS jobs that use different rotation schemes may need different tape names. To ensure that multiple GFS jobs will share the media, use the same rotation scheme.
- **Start GFS jobs on the same day**--The first day of a GFS job is a full backup. Jobs that start with different dates may not be able to share media during the first week. To ensure that multiple GFS jobs will share media during the first week, start GFS jobs on the same day. Otherwise, media sharing will begin after the weekend.
- **If you want to modify multiple GFS backup jobs to use a new media pool, modify them on the same day**--This ensures that all jobs will share the media right away. Otherwise, media sharing will begin after the weekend.
- **Modify existing GFS jobs to use the same media pool as other GFS jobs**--If the existing GFS jobs you modified use the same rotation scheme, media sharing should begin right away. However, if any of the jobs have been running for less than one week, media sharing may begin after the weekend.

Media Maximization Methods

There are two different methods you can use to maximize your media usage. The method depends on whether you enable the Append Media feature when submitting your GFS backup job. Both methods significantly reduce the amount of media required. The following is a description of each method.

GFS Rotation Jobs without Append Media Enabled

If you submit GFS rotation jobs without the Append Media feature enabled, you can maximize media usage by submitting multiple jobs using the same media pool.

For example, if you submit three GFS rotation jobs all using the same media pool and 5-day rotation scheme, all three jobs share the same set of tapes. On each day of the rotation scheme, all three jobs append to the same tape:

- Monday = One tape that includes full backup data from job 1(day 1), job 2(day 1), and job 3(day 1)
- Tuesday = One tape that includes incremental backup data from job1(day 2), job 2(day 2), and job 3(day 2)
- Wednesday = One tape that includes incremental backup data from job 1(day 3), job 2(day 3), and job 3(day 3)
- Thursday = One tape that includes incremental backup data from job 1(day 4), job 2(day 4), and job 3(day 4)
- Friday = One tape that includes weekly backup data from job 1(day 5), job 2(day 5), and job 3(day 5)

This results in five tapes for the week.

Without the Media Maximization option, each job would require its own tape:

- Monday = Three full backup tapes. One tape for job1(day 1), one tape for job 2(day 1), and one tape for job 3(day 1)
- Tuesday = Three incremental backup tapes. One tape for job1(day 2), one tape for job 2(day 2), and one tape for job 3(day 2).
- Wednesday = Three incremental backup tapes. One tape for job1(day 3), one tape for job 2(day 3), and one tape for job 3(day 3).
- Thursday = Three incremental backup tapes. One tape for job1(day 4), one tape for job 2(day 4), and one tape for job 3(day 4).
- Friday = Three Weekly backup tapes. One tape for job1(day 5), one tape for job 2(day 5), and one tape for job 3(day 5).

Without the Media Maximization option, you need 15 tapes for the week.

Note: When submitting multiple GFS Rotation Jobs with the same media pool without Append Media enabled, tapes can be shared only if the same Backup Method is used. For example, a tape that has data from a full backup job can be shared only with data from another full backup job. It cannot be shared with data from incremental, differential, weekly, or monthly backup jobs.

GFS Rotation Jobs with Append Media Enabled

Similar to submitting GFS Rotation jobs without the Append Media feature enabled, you can maximize media usage when you enable Append Media by submitting multiple jobs using the same media pool. In addition, enabling Append Media also lets you maximize media usage by allowing you to share tapes among different jobs, regardless of the backup method that was used. (The only exceptions to this is weekly and monthly backup jobs. Weekly and monthly backup jobs can never share tapes with full, incremental, and differential backup jobs.)

For example, when submitting multiple GFS rotation jobs with the same media pool without Append Media enabled, a tape that has data from a full backup job can be shared only with data from another full backup job. If you enable Append Media, a tape that has full backup data can be shared with full, incremental, and differential data.

To share tapes among different jobs with different backup methods, CA ARCserve Backup uses the same GFS rotation naming syntax, but it uses a different naming convention for backup types when the Append Media feature is enabled:

(backup type)-(user-defined media pool prefix)-(day-of-the-week)-(date)

Without Append Media	With Append Media
F - full backup	A - full backup
I - incremental backup	A - incremental backup
D - differential backup	A - differential backup
W - weekly backup	W - weekly backup
M - monthly backup	M - monthly backup

If you submit GFS rotation jobs with the Append Media feature enabled, you can maximize media usage by submitting multiple jobs using the same media pool and use the previous day's tape within the current week.

For example, if you submit three GFS rotation jobs all using the same media pool and 5-day rotation scheme, all three jobs share the same set of tapes. In addition, multiple days can share the same tape, drastically reducing the amount of tapes you use:

- Monday, Tuesday, Wednesday, Thursday = One tape that includes full backup data from job 1(day 1), job 2(day 1), and job 3(day 1), and incremental backup data from job 1 (days 2, 3, and 4), job 2(days 2,3, and 4), and job 3(days 2,3, and 4).
- Friday = One tape that includes weekly backup data from job 1(day 5), job 2(day 5), and job 3(day 5)

This results in two tapes for the week.

Without the Media Maximization option, each job requires its own set of tapes. Among these tapes, only the ones that include data from the same Backup Method can be shared:

- Monday = Three full backup tapes. One tape for job1(day 1), one tape for job 2(day 1), and one tape for job 3(day 1)
- Tuesday, Wednesday, Thursday = Three incremental backup tapes. One tape for job1(days 2, 3, and 4), one tape for job 2(days 2, 3, and 4), and one tape for job 3(days 2,3, and4).
- Friday = Three weekly backup tapes. One tape for job1(day 5), one tape for job 2(day 5), and one tape for job 3(day 5).

This results in nine tapes for the week.

Note: If you submit a GFS Rotation job with Append Media enabled and CA ARCserve Backup cannot use the previous day's media for some reason, it will format a media in the Scratch Set or a blank media using the "With Append Media" naming convention. To minimize the likelihood of this situation occurring, see Media Maximization Rules in this chapter.

Overlapping Media Rules

Because the Media Maximization option allows multiple GFS jobs using the same media pool to share tapes, you may encounter a situation where a media is busy because it is being used by another GFS job. If this occurs when submitting a GFS backup job without Append Media enabled, the job waits for the tape to become available before appending. The default wait time is 10 minutes. If the media is still busy after 10 minutes, the job uses another tape.

If this occurs when submitting a GFS backup job with Append Media enabled, CA ARCserve Backup tries to append to a previous day's media. If that media is busy, it waits 10 minutes. If the media is still busy after 10 minutes, the job uses the current date to generate another media and attempts to use it. If the new media is busy, the job waits 10 minutes. If this media is still busy after 10 minutes, the job formats another media with a new name.

Note: You can change the wait time by entering a new value for the Windows registry key GFSwaittime. This value is stored in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve  
Backup\Base\Task\Backup
```

Media Pool Manager

The Media Pool Manager allows you to create and maintain media pools. CA ARCserve Backup creates a catalog file on your media to improve performance for merge jobs and database backup jobs. The Media Pool Manager helps you to perform the following tasks:

- **Create a new media pool**--To assign media to a media pool, you first need to create the media pool. A media pool name can consist of up to 16 uppercase characters.
- **Delete an existing media pool**--To delete a media pool, you must first re-assign the media to another media pool.
- **Move media in a pool**--You can move media from one set to another. You can also move media from a Scratch Set to a Save Set and vice versa by using the Assign Media and Remove Media options.
- **Perform location maintenance**--You can enter information about a new location, modify information about an existing location, or assign media to a location.
- **Assign media to a media pool**--You can assign media to a media pool during the process of formatting. When you format media using Device Management, you define certain media pooling information that will be associated with the media.
- **Remove media from a media pool**--You can remove media from a media pool.

For more information on how to perform these tasks, see the online help.

Note: Media Pool operations, backup jobs using the Overwrite option, Tape Erase operations, and backup jobs involving Media Pools (such as GFS rotation jobs) are not supported on WORM (Write Once Read Many) media. These operations are either blocked or disabled in WORM support updates.

How You Can Create a Rotation

To create a rotation, select the Schedule object in the left pane of the MM Admin window, double-click it, and select a schedule from the list. Double-click the schedule to access the Rotation object. Right-click the Rotation object and select Create. The Create Rotation dialog appears where you can set the following:

- **Sequence Number**--MM Admin automatically generates a sequence number for your rotation. Vault cycles start with the lowest sequence number. The default for a new rotation is 10 and the next new rotation that follows is 20. If you would rather assign a particular sequence number, select the Sequence Number option and select a number.
- **Vault Name**--A vault name must be specified for each rotation. You can select the name of a vault from the drop-down vault list.
- In the Retention fields, set any of the following conditions:
 - **Hold Days**--The number of days you want tape volumes to be retained.
 - **Keep for Cycles**--The number of vault cycles you want tape volumes to be retained in this rotation.
 - **Days Elapsed from First Format Date**--Starting from the day the tape volumes were first formatted, enter the number of days you want tape volumes to remain in this rotation.
 - **By Date**--Tape volumes are retained in this rotation until the date you enter here is reached.
 - **By Tape Expiration Date**--Tape volumes are retained in this rotation until their expiration date passes.
 - **Permanent**--All tape volumes are retained in this rotation permanently.

If a tape volume meets one of these conditions, it remains in the same rotation. None of these conditions have priority over the other so if any condition is true, the media will stay in the vault--even if conditions appear to conflict. For example, if you select 60 in the Hold Days field but enter a date that is only 30 days away in the By Date field, the tape volume will stay for 60 days.

When you click Add, the new rotation is saved and added to the Rotation branch in the MM management window.

When the Retention period for a tape volume expires, the tape volume is unvaulted and returned to Tape Service to be re-used.

Media Management Administrator (MM Admin)

Note: To use the MM Admin, you must install the Enterprise Module.

MM Admin lets you protect, control, and manage your media resources. Using MM Admin, you can organize tape movement to off-site storage locations, define retention policies to ensure that your tapes are protected from being prematurely overwritten, secure access to tape-resident files, and maintain a comprehensive inventory of tape library resources.

MM Admin activities are recorded in the Activity Log. This includes information, warnings, and errors. This important function allows you to centrally keep track of all media management operations.

To manage media using MM Admin, you must create a vault, create a schedule, select a vault criteria descriptor, and define a rotation. The following sections include information on each of these steps and cover all topics associated with managing your media using MM Admin.

Media Management and Tape Service

In data centers with off-site storage locations, tape volumes are typically cycled out of the central tape library to more secure storage areas (vaults), and then cycled back into the central library. MM Admin works with Tape Service to provide additional media control, rotation, slot number assignment, and reporting on vaulted tape volumes so that you can physically route these tape volumes to off-site storage locations and back to the data center, as necessary.

You can define vaulting criteria using MM Admin. The criteria for holding tape volumes in vaults can be different for each schedule and for each vault. As tape volumes meet these criteria, they are checked out of Tape Service with the proper vault code and reports are generated indicating the current location and destination to where the tape volumes must be moved.

Media Management Administrator Terms

The following are important terms associated with the MMO:

- **Vault**--Any identifiable storage area or location you define.
- **Slot**--Virtual slots in a vault are assigned when a tape volume is vaulted. Each slot is used to store one tape volume. By default, there are 32000 slots in a vault, but you can designate a different maximum number of slots as you create a vault.

- **Schedule**--Determines when a tape volume is to be placed in or removed from a vault.
- **Rotation**--Determines when to move tape volumes, and is associated with a schedule. Each rotation you define points to a vault.
- **Vault Criteria Descriptor (VCD)**--Defines the controlling data set you want to use for the selected tape volume. You can choose the controlling data set by media name or file name, or you can select an individual media as the controlling data set.
- **Vault cycle**--The actual movement of tape volumes. You must describe the vault, the tape volumes, and the rules for tape volume movement under the MMO by creating a Vault Criteria Descriptor (VCD) record. The MMO uses this descriptive information to execute a vault cycle when movement is scheduled.
- **Reports**--Each time you execute a vault cycle or an estimated vault cycle, CA ARCserve Backup generates several reports before another vault cycle can be initiated. The Vault Selection Report contains a list of tape volumes to be selected for moving into the vaults through the VCD. The Shipping Report and the Receiving Report provide a reliable record of the result of the vault cycle and the current location of your tape volumes.

The Shipping Content Report and the Receiving Content Report provide you with basic session details—in addition to the information contained within the Shipping Report and the Receiving Report—such as the session number, source path, start date, size, and number of files.

An Inventory Report is also available, which you can generate at any time.

MM Admin Interface

The MM Admin interface is designed to make vault creation, scheduling, VCD creation, rotation, and report creation easy. The tools provided by MM Admin allow you to establish the vaulting policy needed for complete Media Management.

The MM Admin workspace includes a menu bar, the main MM Admin toolbar, and the MM management window. The left pane of the MM Management window displays the MM primary management server in a tree structure for easy navigation. The right pane displays information related to the object selected in the left pane. It also displays any output messages and reports generated during your MM Admin session.

MM Admin Toolbar

The following table describes tasks that you can perform using the Media Management Administrator (MM Admin). Click the corresponding toolbar button to start the task.

Button	Task
Initialize MM Database	Lets you Initialize the MM database.
Retrieve Data	Lets you retrieve data and display the latest information if the database fails.
Refresh	Lets you refresh and update the information displayed in the MM Admin window.
Start Vault Cycle	Lets you start the vault cycle process.
Simulate Vault Cycle	Lets you produces a Vault Selection Report that predicts how many tape volumes will be moved without actually updating location information.
Find Media in Vault	Lets you search for media by Tape Name or Serial Number.
Property	Lets you view the server's properties.
Print	Lets you print the information displayed in the right pane of the MM Admin window.
Print Preview	Lets you preview information before printing.

MM Admin Window

The objects in the left pane of the MM Admin window are arranged in an expandable tree. To view related information, double-click the branch you need. After you access a branch, you can add, modify, or delete objects from the tree structure using the available pop-up menus. Right-click any object to access pop-up menus.

When you open MM Admin, the MM primary management server is displayed at the top of the tree. Double-click the branch to expand it and access the following objects:

- **Current Server**--Displays information about the server you are currently using.
- **Vault**--Provides information about previously created vaults.
- **Schedule**--Lists the names of the previously created schedules, and allows you to access the Vault Criteria Descriptor and Rotation objects.
- **Reports**--Provides access to the seven available reports.
- **Status**--Allows you to view the status of the most recent operation.
- **Find Media in Vault**--Lets you access the Find Media dialog to locate a particular media.

Schedule Object

The Schedule object provides information about previously defined schedules and allows you to create new schedules. You must create a schedule before you define the Vault Criteria Descriptor and Rotation that determine selection and retention policies for your vault.

When you select the Schedule object, the right pane of the MM Admin window displays the names of previously defined schedules. These schedules are also listed under the Schedule object in the left pane. Right-click the Schedule object to create a new schedule. Right-click a specific schedule to delete it. For more information about creating or deleting a schedule, see the section *How You Can Schedule Tape Volume Movement*.

After you have named and created a schedule, the Vault Criteria Descriptor (VCD) and Rotation objects appear in the left pane of the MM Admin window.

Vault Criteria Descriptor Object

The Vault Criteria Descriptor (VCD) allows you to set source information that governs the tape volumes assigned to a vault. You can select a media pool name or a file name as the controlling data set. If you want to assign only one tape, select the Assigned by User option as the controlling data set. If you use this option, you must enter command line information. When this data set is vaulted, the tape volumes are assigned to slots in the vault.

When you select the Vault Criteria Descriptor object, the right pane of the MM Admin window displays columns listing the following information for existing VCDs:

- **VCD Name**--The name of the Vault Criteria Descriptor.
- **VCD Type**--Indicates whether the controlling data set is defined by media pool, file name, or by user.
- **Media Pool**--If the controlling data set is a media pool, the name of the media pool appears.
- **Host Name**--If the controlling data set is a file name, the host where the file resides appears in this column.
- **Path/File Name**--If the controlling data set is a file name, the full path and file name appear in this column.
- **Create Date**--The date the VCD was created.

In the right pane of the MM Admin window, right-click an existing VCD to update or delete it. Right-click the Vault Criteria Descriptor object in the left pane to create a new VCD. For more information about creating, updating, or deleting a VCD, see the section [How You Can Manage Tape Volumes and VCDs](#).

More information:

[How You Can Manage Tape Volumes and VCDs](#) (see page 425)

Rotation Object

Media management relies upon user-defined rotation policies to determine when and where tape volumes should be moved. Use the Rotation object to set or update the retention policies that determine when tapes will be moved or released from the vault and returned to Tape Service.

When you select the Rotation object, the right pane of the MM Admin interface lists the following information about previously defined rotations:

- **Rotation Name**--The name of the rotation.
- **Vault Name**--The name of the vault the rotation is associated with.
- **Retention Hold Days**--Starting from the Last Write date (the date the media was last written to), this indicates the number of days that the tape volumes will be held in this rotation.

Note: To view the Last Write date, expand the Vault object and highlight a media name in the top right-hand pane. The Last Write date appears in the lower right-hand pane.

- **Retention Keep for Cycles**--Indicates the specific number of vault cycles and tape volumes that are held in this rotation.

- **Retention Days Elapsed from First Format Date**--Indicates that tape volumes are held in this rotation until a specified number of days have elapsed since they were first formatted.
- **Retention Permanent**--Indicates that tape volumes will remain in this rotation permanently.
- **Retention By Tape Expiration Date**--Indicates that tape volumes remain in this rotation until the tape expiration dates have passed.
- **Retention By Date**--Indicates that tape volumes remain in this rotation until the specified date has passed.
- **Create Date**--The date the rotation was created.
- **Description**--A user-defined description of the rotation.

Existing rotations are also listed in the right pane of the MM Admin window under the Rotation object.

- To update an existing rotation, right-click the rotation name and select Update from the pop-up menu.
- To create a new rotation, right-click the Rotation object and select Create.

Reports Object

Although tape volume location information in the database is updated when you initiate a vault cycle, the physical movement of tape volumes is done manually. MM Admin generates reports indicating the current location and destination where the tape volumes must be moved so that you can route them to other storage locations and back to the data center, as necessary.

The Reports object provides access to the reports generated by the vault cycle process and the Inventory reports, which can be generated at any time. Expand the Reports object in the left pane of the MM Admin window to view the following report types:

- **Vault Selection Report**--Contains a list of tape volumes to be selected for moving into the vaults through the Vault Criteria Descriptor (VCD).
- **Shipping Report**--Contains a list of tape volumes to be pulled from each of the vaults.
- **Shipping Content Report**--Contains a list of tape volumes and sessions in each tape volume to be pulled from each of the vaults.
- **Receiving Report**--Contains a list of tape volumes to be distributed to the vaults.
- **Receiving Content Report**--Contains a list of tape volumes and sessions in each tape volume to be distributed to the vaults.
- **The Inventory Report, By Vault**--Lists tape volumes grouped by the vault where they reside.
- **The Inventory Report, By Media**--Lists tape volumes grouped by vault and shows Media name in front.

When you select a report type in the left pane of the MM Admin window, the right pane displays the contents, listing the available reports identified by date. Click a report to view it in the right lower pane. You can print any of these reports using the Print button on the MM Admin toolbar. At the time it is generated, you can also select to send a report by email if you configure the alert notification system to use Microsoft Exchange. For more information on sending reports using email, see *How the Media Management Process Works* in this chapter. For more information on using alerts, see the chapter "Using the Alert Manager."

The Inventory Reports are based on information in the Slot table, and can be generated at any time. The Shipping and Receiving Reports are based on movement records generated during a vaulting cycle, and are updated after each vault cycle process completes.

The Vault Selection Listing is produced each time the Start Vault Cycle command is executed. For each VCD processed, this listing identifies the first tape volume in the tape volume set and the controlling data set. This information is provided for all tape volume sets selected for the vaulting cycle.

Find Media in Vault Object

The Find Media in Vault object provides the quickest way to search vaults for a specific media, if, for example, you require that media to execute a restore job. You can choose to search for the media using its Tape Name or its Serial Number (case sensitive).

To open the Find Media in Vault dialog, right-click the Find Media in Vault object, and choose Find from the pop-up menu. Using this dialog you can set the criteria for your media search.

Status Object

MM Admin can run only one vault cycle at a time. To monitor the progress of the vault cycle, or to obtain current online status, double-click the Status object in the left pane of the MM Admin interface to view the following information:

- **Current Status**--The status of the current operation is displayed as either Active or Finished.
- **Last Operator**--The owner of the last operation executed.
- **Last Operation Type**--Operation types can be Ready, Vault Cycle, Commit, Browsing, Update, and Reset.
- **Last Operation Started At**--The date and time the last operation began.
- **Last Operation Finished At**--The date and time the last operation ended.

Reset the Status of Vault Processing

Use MM Admin to manually reset the status of Vault Processing if something goes wrong during the vault cycle, such as corruption of the MM Admin database. You can use the `ca_mmo` command line utility to reset the status. See `ca_mmo` Command in this chapter for more information about command line utilities for media management. After the status is reset, you can restart another vault cycle.

How the Media Management Process Works

The Media Management process includes setting a vaulting policy, scheduling tape volume movement, selecting tape volumes, defining retention policies, executing the vault cycle, and moving the media to the proper location.

After you set a vaulting policy and retention policies, the vaulting rotation process begins. You should run vault cycles as often as you run backup operations. For example, if you back up your data every day, you should also run a vault cycle every day. If you back up your data once a week, run a vault cycle once a week after your backup operation is complete.

The vault cycle process updates location information for tape volume sets, indicating movement into a vault or from a vault back to the Tape Service. You must initiate the process by clicking Start from the Vault Cycle menu on the MM Admin toolbar. You can also initiate the vault cycle using the `ca_mmo -start` or `-startAll` command at the DOS prompt.

Notes:

- When using Media Management Administrator (MM Admin), the vault cycle processes tapes for the primary server and all of the member servers.
- You must click the Start Vault Cycle button every time you want current information on the MM location of the media.

Execute the Start Vault Cycle process to generate reports detailing the movement of the tape volumes and location information. The slots that already contain tape volumes and the new slots that will be vaulted are grouped together by their common schedule. Beginning with the first rotation in the schedule, tape volume sets are assigned to a vault and its slots based on the expiration criteria. Slots are automatically created and tape volumes automatically vaulted during this process.

When the first rotation is satisfied, the next rotation in the schedule is processed, and so on through the entire schedule until all rotations have been exhausted. Media management then generates reports indicating the current location and destination where the tape volumes must be moved. If you do not want to remove these tapes manually, you can use the `ca_mmo -export` command at the DOS prompt so MM Admin automatically exports them. See Device Manager in this chapter for more information about command line utilities for media management.

You can use the Simulate Vault Cycle command to produce a Vault Selection Report. Use this command at any time to predict how many tape volumes will be moved without actually updating the location information. If you want to send the Vault Selection Report to someone by email, make sure your system is configured to send alerts using Microsoft Exchange and, from the Configuration menu, enable the option Send the report by E-mail. For more information on configuring alerts, see the chapter "Using the Alert Manager."

The vault cycle generates the Shipping and Receiving Reports, listing the old and new locations of the tape volume set, to provide you with the information you need to manage your media. These reports provide the following information:

- **Shipping Report**--tells you what media to pull manually, and where to send it.
- **Shipping Content Report**--lists all tape volumes and sessions in each tape volume to be pulled from each of the vaults.
- **Receiving Report**--tells you what media will be coming in to each particular vault.
- **Receiving Content Report**--lists all tape volumes and sessions in each tape volume to be distributed to the vaults.

If you want to send the shipping and receiving reports to someone by email, make sure your system is configured to send alerts using Microsoft Exchange and, from the Configuration menu, enable the option Send the report by E-mail. For more information on configuring alerts, see the chapter "Using the Alert Manager."

When a tape volume comes under Media Management control, Tape Service updates the tape volume's location status to OFF_SITE. To prevent a tape volume from being used while under Media Management control, the tape volume is automatically checked out, and the location is updated to reflect this. Because all vaulted tape volumes are placed in checked out status, if you need to retrieve tape volumes, they must be checked into Tape Service before they can be used.

Vault Management

The first step in establishing a vaulting policy is to create a vault. You can create vaults using MM Admin.

Create a Vault

This section describes how to create a vault.

When you create a vault, location information is automatically updated and integrated with the Location Maintenance feature in CA ARCserve Backup. If you select a vaulted tape through CA ARCserve Backup, vault location information appears. Location information is also updated in the Media Pool Manager. If you select a vaulted tape for restore, a message appears indicating that the tape is OFF_SITE.

To create a vault

1. From the CA ARCserve Backup Home page, open the MM Admin window.
2. Right-click the Vault object and select Create from the pop-up menu.

The Create Vault dialog opens.

3. Enter a name and description for the new vault.

Select the Use in Local option if this vault will not be moved to another location. If the tape volumes in this vault are to be maintained off site, do not select this option.

4. Click Add to save and add the vault to the Vault branch in the MM management window.

The vault is created.

Modify a Vault

Use the following steps when you want to modify the vault name, vault description, or Use in local option.

To modify a vault

1. From the Administration menu in the Navigation Bar on the Home Page, click MM Admin.

The Media Management Administrator window opens.

2. Browse to and double-click the Vault object in the left pane of the MM Admin window.

A list of existing vaults displays.

3. Right-click the vault you want to update from the list, and select Update from the pop-up menu.

The Edit Vault dialog opens

4. Make your changes and click OK.

The settings for the vault are modified.

Delete a Vault

Use the following steps to delete a vault from the MM Admin.

Note: Before you delete a vault, you must remove all media from the vault and ensure that there are no rotations associated with the vault.

To delete a vault

1. Open the MM Admin and browse to the vault that you want to delete.
Right-click the vault name and select Delete from the pop-up menu.
A delete confirmation message box opens.
2. If you are sure that you want to delete the vault, click Yes.
The vault is deleted.

Create a Schedule

Media Management relies upon a user-defined schedule to determine the tape volumes to move, and when and where to move them. When you select the Schedule object, you can view existing schedules in the right pane of the MM Admin window or you can define new rotation policies and vaulting criteria.

To create a schedule

1. Open the MM Admin, right-click the Schedule object in the left pane of the MM Admin window, and select Create from the pop-up menu.
The Create Schedule dialog opens
2. On the Create Schedule dialog, specify a name for the schedule and click Add.
3. The new schedule is saved and added to the Schedule branch in the MM management window. After you create a schedule, the Vault Criteria Descriptor (VCD) and Rotation objects appear in the left pane of the MM Admin window. These objects allow you to select media and retention policies.

Delete a Tape Volume Movement Schedule

Before you can delete a schedule, you must first ensure that any VCD and rotation for the schedule have been deleted.

To delete a tape volume movement schedule

1. Expand the list of schedules below the Schedule object.
2. Click the schedule you want to delete.
3. Delete the VCD and rotation for this schedule.
4. Right-click the schedule that you want to delete and choose Delete from the pop-up menu.
5. Click OK.

The schedule is deleted.

How You Can Manage Tape Volumes and VCDs

To assign media to vaults you must specify a VCD and rotation. You can select a media pool, file name, or an individual media for the controlling data set. When this data set is vaulted, its tape volume set is placed in slots in the vault. The assignment of slot numbers is based on the rotation records you defined.

More information:

[Vault Criteria Descriptor Object](#) (see page 416)

Create a Vault Criteria Descriptor

After you have created a schedule, you must describe the rules for media selection by creating a VCD.

To create a vault criteria descriptor

1. From the Administration menu in the Navigation Bar on the Home Page, click MM Admin.

The Media Management Administrator window opens.

2. Expand the Schedule object, expand a schedule, right-click Vault Criteria Descriptor object, and select Create from the pop-up menu.

The Create Vault Criteria Descriptor dialog appears.

3. Choose one of the following options:

Media Pool Name

To use a media pool name as the controlling data set, enter the name of the media pool or use the drop-down list to select a media pool name from the pool list. Only the media within the Save Set of the media pool can be vaulted. The media in the Scratch Set cannot be vaulted.

File name

To use a file name as the controlling data set, select the File Name option and enter the host name and the full path and file name from your backup, such as C:\DOC\Readme.txt, in the appropriate fields. Browse through the Database or Restore Manager to obtain path or file information. The MM Admin finds all tapes used for the backup of this directory or file.

Assigned by User

If you want to use an individual media as the controlling data set, select the Assign by User option. This is useful in emergencies when you need to use a specific tape. Because MM Admin lets you start a vault cycle only with local media, the media icon appears in yellow if the vaulted media is not a local media with a remote host name. To start a vault cycle with a remote media and members servers, you must execute the ca_mmo command line utility using the -startall argument.

Note: For more information about command line utilities for media management, see the *Command Line Reference Guide*.

4. Click Add.

The VCD is added to the Vault Criteria Descriptor branch in the Media Management Administrator window.

Modify a Vault Criteria Descriptor

Use the following steps to modify the media pool name, the file name, the assigned by user option associated with the vault criteria descriptor (VCD).

To modify a vault criteria descriptor

1. Open the MM Admin, expand the list of schedules under the Schedule object and select a schedule from the list.

Expand the schedule to display the Vault Criteria Descriptor and Rotation objects.

Right-click the Vault Criteria Descriptor object and select Update from the pop-up menu.

The Edit Vault Criteria Descriptor dialog opens.

2. Modify modify modify the Media Pool Name, the File Name, the Assigned by User option associated with the VCD and click OK.

The modified value is applied.

Delete a Vault Criteria Descriptor

To delete a schedule, you must first delete the associated rotation and VCD.

To delete a VCD

1. From the Schedule object, select the specific VCD from the list under the Vault Criteria Descriptor.
2. Right-click and select Delete from the pop-up menu.
3. Click OK.

Tape Volume Retention Policies

After you create a schedule, you must set the policies governing tape volume retention for your vault. To do this, use the Rotation object.

Note: The Rotation object appears in the left pane of the MM Admin window only after you create schedule.

Special Tape Volume Movement

Special circumstances may arise in which you need to move a particular tape volume. If this situation occurs, you have three options—Temporary Check In, Manual Check In, and Manual Check In and Retire. You also have the option to permanently vault a volume so that it does not return to Tape Service. The following sections describe each of these options.

Temporary Check In

The Temporary Check In option is useful for tracking media movement if you want to temporarily move a tape volume from a vault to use for a restore job, but want to return it back to the vault when the job is finished.

All tape volumes that are vaulted are in *checked out* status. Use the Temporary Check In option to change this status to *checked in* so that you can keep track of your tape volume while it is temporarily being used for a restore job. When you finish using the tape volume, the next vault cycle returns it to the vault and changes the status back to *checked out*.

Note: The Temporary Check In option is only for tracking tapes that are temporarily returned from the vault, and is not a requirement for the actual tape movement; if you do not use this option, you can still manually move a tape volume from a vault and return it when a job is finished. However, you should use this option because, if you do not use it and move a tape volume, there will be a discrepancy between the status of the tape volume that appears in the MM Admin and the actual location of the tape.

To use the Temporary Check In option, in the left pane of the MM Admin window, double-click the Vault object to see a list of existing vaults. Select a vault to display its information in the right pane. Select the name of the media you want to move, right-click, and select Temporary Check In.

Example: Temporary Check In

For example, to perform an emergency restore operation using a tape volume from one of the vaults, use the Temporary Check In feature to temporarily check the tape volume in to Tape Service, execute the restore operation, and then run a vault cycle to return the tape volume to the vault.

Check in a Tape Volume Manually

Use the Manual Check In option to check a tape volume back into Tape Service before the time it is scheduled to be checked in. When you manually check a tape volume back into Tape Service, it does not return to the vault.

To check in a tape volume manually

1. From the left pane of the MM Admin window, double-click the Vault object.
A list of existing vaults displays.
2. Select a vault to display its information in the right pane.
3. Select the name of the media you want to move, right-click, and select Manual Check In from the pop-up menu.

The tape volume is checked in.

Manual Check In and Retire

Use the Manual Check In and Retire option to check a tape volume back into Tape Service before the time it is scheduled to be checked in, and retire it so it is no longer used.

To use the Manual Check In and Retire option, in the left pane of the MM Admin window, double-click the Vault object to see a list of existing vaults. Select a vault to display its information in the right pane. Select the name of the media you want to move, right-click, and select Manual Check In and Retire.

Permanent Retention

Use the Permanent Retention option to permanently vault slots and the tape volumes they contain. If you use this option, when a tape volume is vaulted, it does not return to Tape Service. The only way to return it is to change the vault status back to the default.

To permanently check tape volumes out of Tape Service, select the Permanent Retention option on the Create Rotation dialog.

Modify a Rotation

Use the steps that follow to modify the movement of tape volumes associated with a schedule.

To modify a rotation

1. Expand the Schedule object in the left pane of the MM Admin window and select a schedule from the tree.
2. Double-click the schedule to access the Rotation object.
3. Double-click the Rotation object and select a rotation in the right pane.
4. Right-click the rotation and select Modify.

The Edit Rotation dialog appears

5. Apply your changes and click OK.

The new settings are saved.

Delete a Rotation

If you want to delete a schedule, you must first delete the associated rotation and VCD.

Delete a rotation

1. From the left pane of the MM Admin window, expand the schedule object, and the expand schedule for the rotation that you want to delete.

The rotation displays in the right pane of the MM Admin window.

2. From the right pane of the MM Admin window, select the rotation from the list.
3. Right-click the rotation that you want to delete and select Delete from the pop-up menu.

A confirmation message appears

4. Click Yes.

The rotation is deleted.

Slot Detail and Status Information

When tape volumes have been assigned to slots in a vault, MM Admin displays slot information for the vault. Select the Vault object in the left pane of the MM Admin window and expand it. When you select a particular vault from the list, the right pane of the MM Admin window displays a view of the vault and its slots.

This view provides the following information:

- **Media Name**--Lists the media name, ID, sequence number, and serial number.
- **Slot Status**--Either Active, Unvaulted, Temporary Check In, Manual Check In, or Manual Check In and Retire:
 - **Active**--The media has been sent to this vault.
 - **Unvaulted**--The media has not yet been sent to this vault.
 - **Temporary Check In**--The media will be checked in temporarily during the next vault cycle.
 - **Manual Check In**--The media will be checked in during the next vault cycle.
 - **Manual Check In and Retire**--The media will be checked in and retired during the next vault cycle.

- **Slot Name**--Lists the vault name and slot number.
- **Media Export Status**--Either Ready, Success, or Fail:
 - **Ready**--The default status. The media has been assigned to the vault, but has not been exported from the tape library to the mail slot.
 - **Success**--Appears once the media is successfully exported to the mail slot.
 - **Fail**--Appears if MM Admin failed to export the media to the mail slot.
- **Local**--Either Yes or No. Yes appears if the media belongs to a local machine. No appears if it belongs to a remote machine.
- **Create Date**--The date the slot was created.

When you highlight a media name, additional information appears in the Properties pane in the lower right-hand corner of the page. This information includes the media name, serial number, random ID, host name, slot status, slot name, media export status, media type, media class, last write, last read, and slot creation date. Because MM Admin lets you start a vault cycle only with local media, the media icon appears in yellow if the vaulted media is not a local media with a remote host name. If you want to start a vault cycle with a remote media and members servers, use the `ca_mmo -startall` command line utility.

Note: For more information about command line utilities for media management, see the *Command Line Reference Guide*.

Because slots are automatically created when a tape volume is vaulted, you typically have no reason to update slot information.

Find Specific Media in a Vault

To help you locate media in your vaults, MM Admin provides the Find Media in Vault feature. This feature is the fastest way to locate media in your vaults if you know the tape name or serial number of the tape volume you need. If you do not know this information, you can use the Database Manager to find the media.

To find a specific media in a vault

1. From the Administration menu in the Navigation Bar on the Home Page, click MM Admin.

The Media Management Administrator window opens.

2. From the Media Management Administrator window, right-click the Find Media in Vault object and select Find from the pop-up menu.

The Find Media in Vault dialog opens.

3. Select one of the following methods to find your media:

Find by Tape Name

Lets you enter the tape name, the random ID, and the sequence number to identify the tape you want CA ARCserve Backup to find.

Find by Serial Number

Lets you enter the serial number of the desired media.

CA ARCserve Backup completes the Find by Serial Number task using case-sensitive values. For example, the serial number ABC123 is different from the serial number abc123.

4. Click Find.

When the search is finished, the vault and slot information appears in the right pane of the Media Management Administrator window.

Chapter 7: Administering the Backup Server

This section provides you with information that you can use to administer, manage, and maintain the CA ARCserve Backup Server.

This section contains the following topics:

[How CA ARCserve Backup Engines Work](#) (see page 433)

[Configure CA ARCserve Backup Engines](#) (see page 450)

[Additional Server Admin Functions](#) (see page 478)

[Authentication Levels for CA ARCserve Backup Services, Components, and Applications](#) (see page 484)

[CA ARCserve Backup Domains](#) (see page 490)

[Re-initialize the CA ARCserve Backup Database](#) (see page 504)

[Restore the CA ARCserve Backup Job Queue](#) (see page 506)

[Manage ARCserve Servers Using the Server Configuration Wizard](#) (see page 509)

[Install and Uninstall CA ARCserve Backup Server Based Options](#) (see page 527)

[CA ARCserve Backup Agent Deployment](#) (see page 528)

[Discovery Configuration](#) (see page 541)

[Allow CA ARCserve Backup Services and Applications to Communicate Through the Windows Firewall](#) (see page 549)

[How to Configure Your Firewall to Optimize Communication](#) (see page 549)

How CA ARCserve Backup Engines Work

The CA ARCserve Backup Server consists of three functional engines:

- **The Job Engine**--This engine processes your jobs at their designated date and time. It scans the job queue for a job that is ready to run, then sends it to the appropriate handler.
- **The Tape Engine**--This engine communicates with, and controls, your storage devices. The Tape Engine selects the device needed for a job.

- **The Database Engine**--This engine maintains a history of:
 - Information about jobs processed by CA ARCserve Backup, such as the job type, the final result, the start and end time, submitter, and description.
 - Media used by CA ARCserve Backup, such as its type, its name, the date it was first formatted, its expiration date, and the sessions on it.
 - Files, directories, drives, and machines that CA ARCserve Backup has backed up or copied.

You can control these CA ARCserve Backup engines in the Server Admin. To view information about an individual engine, open the Server Admin from the Quick Start menu in the Navigation Bar on the Home Page. From the ARCserve domain directory tree, select the primary server, member server, or stand-alone where you want to obtain engine status information.

Important! To manage and configure CA ARCserve Backup engines, you must be logged in to CA ARCserve Backup with the caroot password or a CA ARCserve Backup Administrator account.

- **Job Engine**--Displays information about the jobs submitted, such as the total number of jobs and the number of ACTIVE, READY, HOLD, and DONE jobs. It also shows the queues, which ones are being scanned, and the scanning interval.
- **Tape Engine**--Displays information about jobs using the Tape Engine, such as the type of job, and who submitted it. It also displays information on media groups.
- **Database Engine**--Displays pruning information related to the ARCserve database.

How Engine Status Affects CA ARCserve Backup Operations

A stopped engine is an engine that is completely offline. This may be caused by errors, manual shutdown, or a new installation. Whatever the reason, it means that the services of that engine are not available.

The CA ARCserve Backup engines are designed to run independently of each other. For example, if you stop the Tape Engine, the Database Engine and the Job Engine are not affected. They continue to run, performing their services as configured. The Database Engine continues to log pertinent CA ARCserve Backup information in the database, and the Job Engine continues to scan the job queue and start jobs as required. If a job requires a storage device, the Job Engine launches the job, but the job fails because the Tape Engine is not able to communicate with the storage device. The Database Engine then logs this information.

Note: Although CA ARCserve Backup still functions if one or two engines are not running, CA ARCserve Backup needs all three engines running simultaneously to achieve complete functionality.

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.

Stopping and Starting CA ARCserve Backup Services

The following sections describe the methods that you can use to stop and start the CA ARCserve Backup services on primary, stand-alone, and member servers.

Stop and Start All CA ARCserve Backup Services Using Batch Files

There are two methods that you can use to manually stop and start the Job Engine, the Tape Engine, and the Database Engine.

One method is to open the Server Admin, select the server name from the domain tree, select the individual service that you want to stop or start, and then click the Stop or Start toolbar buttons. However, circumstances may arise that require you to stop all CA ARCserve Backup services. For example, you need to apply a patch or fix that was released by CA Support.

The `cstop` and the `cstart` commands let you shut down and restart all CA ARCserve Backup services sequentially, based upon their dependencies to the other CA ARCserve Backup services. This process ensures that there is no loss of data while the services are shutting down, and that all CA ARCserve Backup services are running properly when your system restarts.

To stop or start all CA ARCserve Backup services using a single command, use the file `cstop.bat` or `cstart.bat` located in the CA ARCserve Backup home directory.

When you run `cstop.bat`, CA ARCserve Backup stops the services in the following order:

1. CA ARCserve Communication Foundation
2. CASMgmtSvc
3. CASTapeEngine
4. CASJobEngine
5. CASDbEngine
6. CASMessageEngine
7. CASDiscovery
8. CasUnivDomainSvr
9. CasSvcControlSvr
10. CASportmapper
11. Alert Notification Server

When you run `cstart.bat`, CA ARCserve Backup starts the services in the following order:

1. Alert Notification Server
2. CASDiscovery
3. CASportmapper
4. CasSvcControlSvr
5. CasUnivDomainSvr
6. CASDbEngine
7. CASMessageEngine
8. CASTapeEngine
9. CASJobEngine
10. CASMgmtSvc
11. CA ARCserve Communication Foundation

Stop and Start Individual Services Using the Command Line

To stop or start the CA ARCserve Backup services using the command line

1. Start the Windows command line.
2. After the command line opens, enter one of the following commands: `NET START [enginename]` or `NET STOP [enginename]` and substitute one of the following for [enginename]:
 - CASJobEngine: Job Engine
 - CASTapeEngine: Tape Engine
 - CASDbEngine: Database Engine
 - CASMessageEngine: Message Engine
 - CASDiscovery: Discovery Service
 - CasSvcControlSvr: Service Controller
 - CasUnivDomainSvr: Domain Server
 - CASportmap: CA Remote Procedure call server
 - Alert Notification Server: Alert service

Note: For this service, you must provide quotation marks.

 - CA ARCserve Communication Foundation: CA ARCserve Backup Dashboard service

3. Repeat the previous step for each CA ARCserve Backup Server component.

Important! If you manually stop and restart the CA Remote Procedure Call service (CASportmap) using the Command Line (or the Computer Management console), the service cannot communicate with its port assignments properly. This can prevent a user account with caroot equivalence from logging in to the CA ARCserve Backup domain. To remedy the inability to log in to the CA ARCserve Backup domain, run the cstop command and then run the cstart command. This enables the service to communicate properly and lets the user account with caroot equivalence log in to the CA ARCserve Backup domain.

Stop and Start CA ARCserve Backup Services Using the Server Admin

Using the Server Admin, you can stop and start individual CA ARCserve Backup services that are running on a primary, stand-alone, and member server.

Use this method when you need to stop one or two CA ARCserve Backup services for a short period of time. For example, you need to stop and start the Tape Engine on the primary server so that it can detect a newly installed library.

When you need to stop and start all CA ARCserve Backup services, you should use the cstop and cstart batch files. These batch files let you stop and start all CA ARCserve Backup services sequentially, based on their dependencies to other CA ARCserve Backup services.

Note: For more information about stopping and starting all CA ARCserve Backup services, see Stop and Start All CA ARCserve Backup Services Using Batch Files. However, if you use the Server Admin to stop all services, the service status displays as unknown.

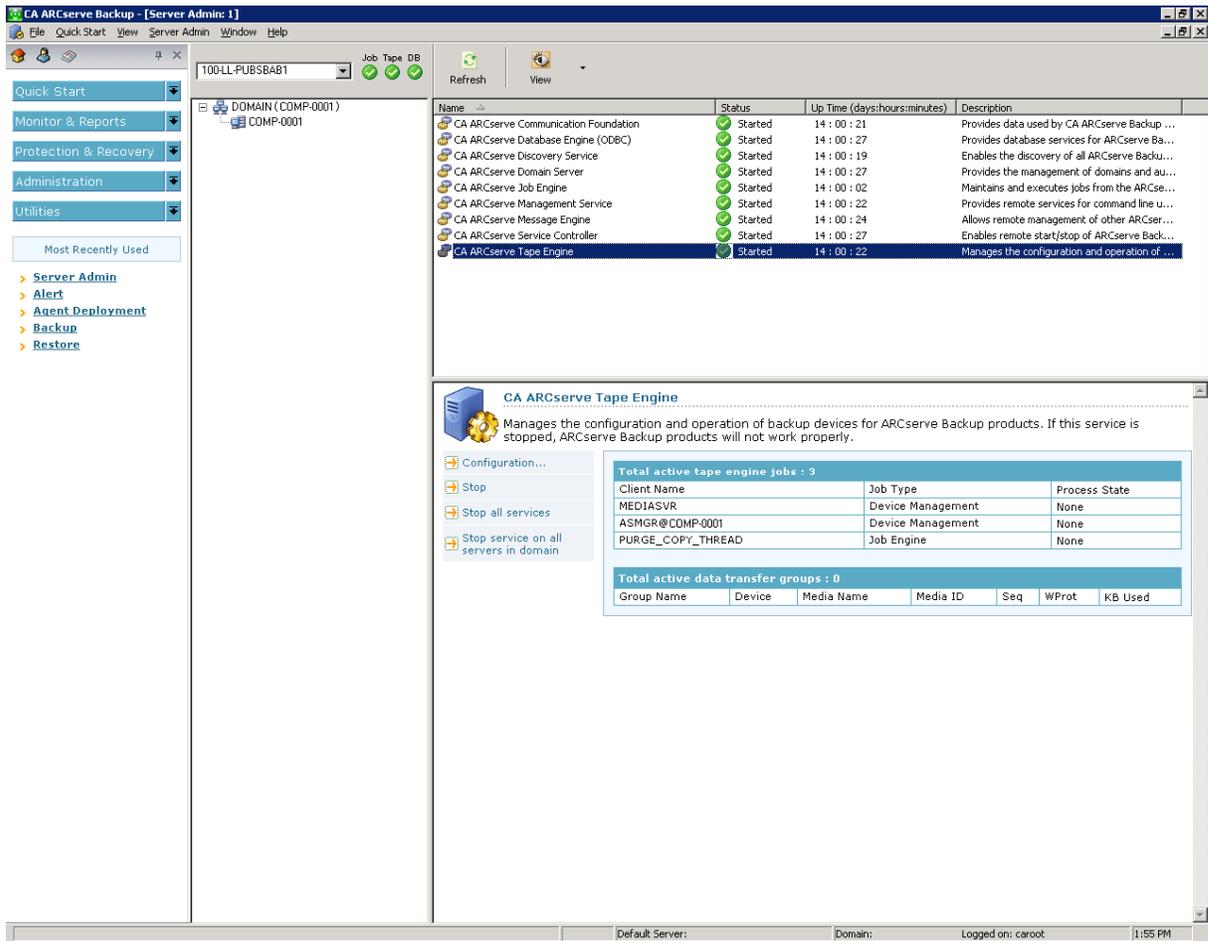
To stop and start CA ARCserve Backup services using the Server Admin

1. From the Quick Start menu in the Navigation Bar on the Home Page, click Server Admin.

The Server Admin opens.

2. Expand the domain directory tree and select the server where you want to stop or start CA ARCserve Backup services.

The CA ARCserve Backup services Name, Status, Up Time, and Description displays in the Server Admin window, as illustrated by the following diagram:



3. Select the service that you want to stop or start.
 - If the status is Started, click the Stop toolbar button.
 - If the status is Stopped, click the Start toolbar button.

The CA ARCserve Backup service stops or starts.

Note: To stop all services, highlight the server, right click and select Stop all services. To start all services, highlight the server, right click and select Start all services.

CA Antivirus Maintenance

CA ARCserve Backup provides the scanning and curing components of the CA Antivirus virus scan engine to protect your data.

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

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

InoDist.ini is the file you use when downloading updated virus signature files and program modules. This file contains preconfigured settings that specify how and when engine and signature updates are collected from a distribution source. The InoDist.ini file typically does not need modifications. However, you can make changes if necessary. The following section includes information on the InoDist.ini file and its various settings.

More information:

[Virus Signature Updates](#) (see page 441)

[INODIST Utility](#) (see page 444)

Virus Signature Updates

Using InoDist.ini, you can update virus signatures by using the Job Scheduler Wizard, the command prompt, or by running them directly from the Web. If you use the Job Scheduler Wizard, you have the added benefit of scheduling your virus signature updates.

More information:

[CA Antivirus Maintenance](#) (see page 441)

[INODIST Utility](#) (see page 444)

Obtain Virus Signature Updates Using the Job Scheduler Wizard

The Job Scheduler Wizard lets you automate the process of obtaining virus signature updates.

To use the Job Scheduler Wizard to update virus signatures

1. From the Utilities menu in the Navigation Bar on the Home Page, click Job Scheduler.
2. The Job Scheduler Wizard opens.
3. Click Next.

The Login Page dialog opens.

4. From the Login dialog, select the local server name for the machine you want to submit the job to.

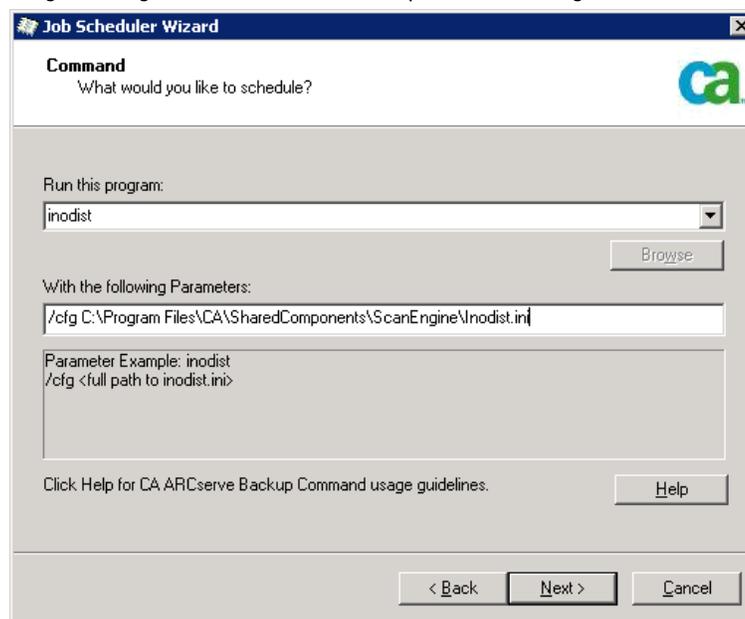
Enter your user name and password to log into the server, and then click Next.

The Command dialog opens.

5. From the Command dialog, in the Run this program field, select inodist from the drop-down list.

In the Parameters field enter /cfg (full path to InoDist.ini). For example:

```
/cfg C:\Program Files\CA\SharedComponents\ScanEngine\Inodist.ini
```



Click Next.

The Security dialog opens.

6. From the Security dialog, enter your user name and password, and then click Next.

The Schedule dialog opens.

7. From the Schedule dialog, select one of the following options:
 - Select Run Now to execute the job immediately.
 - Select Schedule to execute the job at a specific time and date or to schedule the job to repeat. If you want the job to repeat, select a Repeat Method and associated criteria.

When you finish scheduling the job, click Next.

The Summary dialog opens.

8. From the Summary dialog, verify your job selections and enter a description of this job in the Description field. This description appears in the Description column in the Job Queue and can be used to identify the job.

Click the Submit button.

First, a message indicating that the job was submitted successfully appears. The message includes the job number, which you can use to identify the job in the Job Queue. Then a message indicating the Generic Job was successful appears. Click OK to close both message boxes.

If the job fails, a message appears to indicate that the job failed and the error code. You can view a short message describing the error in the Activity Log. Click OK to close the error message box.

Obtain Virus Signature Updates Using the Command Prompt

To use the command prompt to update signatures, open a command window and enter the following command:

```
C:\Program Files\CA\SharedComponents\ScanEngine\inodist /cfg inodist.ini
```

Obtain Virus Signature Updates Via the CA Support Site

The following procedure lets you obtain virus signature updates via the CA Support site.

To obtain virus signature updates via the CA Support site

1. Open a browser window and access the following URL:
`http://etrustdownloads.ca.com/legacy/av`
2. Download and execute the following file:
`fi_nt86.exe`
3. The virus signature updates are applied to CA ARCserve Backup.

INODIST Utility

You can configure the CA Antivirus program to download updated virus signature files.

Syntax for the INODIST Utility

```
INODIST /cfg InoDist.ini
```

Signature Update Options in the InoDist.ini File

The InoDist.ini file contains sections that specify how, and when, engine and signature updates are collected from a distribution source. The InoDist.ini file is installed in C:\Program Files\CA\SharedComponents\ScanEngine. The directory can be viewed or edited using a text editor. The sections of the InoDist.ini file are described as follows:

[SOURCES]

The [SOURCES] section provides the name of the other sections in the InoDist.ini file that specify the connection for the signature download. There are three types of connections available from the user interface—FTP, UNC/Redistribution server, and Local Path. For more information about the options for each type of connection, see the following sections.

Important! The numeric values in the source list must be consecutive. Do not change the numeric order or create gaps in the numeric sequence.

Syntax for [SOURCES]

```
[SOURCES]
1 = SourceA
2 = SourceB
3 = SourceC
```

Options for [SOURCES]

The following options are required:

Option	Description
1 = SourceA	First source. For example, 1=UNC_0
2 = SourceB	Second source. For example, 2=UNC_1
3 = SourceC	Third source. For example, 3=FTP_0

Signature Source

For the signature sources described in the [SOURCES] section of the InoDist.ini file, a specific section exists to describe all of the information necessary to download from the remote site.

FTP Syntax

When FTP is selected as the download method, the following options are available:

```
[SourceA]
Method = FTP
HostName = ftpav.ca.com
UserName = anonymous
UserPassword = Somebody@somecompany.com
Fast Connection = 0
Proxy Name = UpdatePath = /pub/inoculan/scaneng/
```

FTP Syntax Options

The following options are required:

Option	Description
Method = FTP	Use FTP as the download method.
HostName = ftpav.ca.com	The host name address.
UserName = anonymous	The user name for the FTP connection.
UserPassword = Somebody@somecompany .com	The user password for the FTP connection.

UNC/Redistribution Server Syntax

When UNC is indicated as the download method, the following options are available:

```
[SourceB]  
Method = UNC  
Path = \\usprusd1\inoupd$  
UserName = anonymous  
UserPassword = Somebody@somecompany.com
```

UNC/Redistribution Server Options

The following options are required:

Option	Description
Method = UNC	Use UNC as the download method.
Path = \\usprusd1\inoupd\$	The UNC path.
UserName = anonymous	The UNC user name.
UserPassword = Somebody@somecompany .com	The user password.

Syntax for Local Download

When Local is selected as the download method, the following options are available:

```
[SourceC]  
Method = LOCAL  
Path = c:\test
```

Options for Local Download

The following options are required:

Option	Description
Method	Use the local server as the download method.
Path	The local path.

[GET]

If you set `UpdateLocalSignatures = 1` in the [POLICY] section, the [GET] section is empty. If you do not set `UpdateLocalSignatures = 1`, you can use the [GET] section to identify which platform or engine updates to download. You must set `UpdateLocalSignatures = 0` in the [POLICY] setting for the [GET] section to be active.

Syntax for [GET]

```
[GET]  
1 = SetA  
2 = SetB
```

Options for [GET]

The following options are required:

Option	Description
1 = SetA	Download Set A files.
2 = SetB	Download Set B files.

[POLICY]

Use the [POLICY] options to identify actions to take during and after the signature download.

Syntax for [POLICY]

[POLICY]
UpdateLocalSignatures = 1
SignatureHoldTime = 0
MakeIncDownloading = 1
IsDistributionServer = 0

Options for [POLICY]

The following options are required:

Option	Description
UpdateLocalSignatures = 1	1 = Download signature files required to update the local machine, and use them to update the local machine, regardless of their inclusion in the [GET] section. 0 = Only files listed in the [GET] section will be downloaded, and they will not be used to update the local machine.
SignatureHoldTime = 0	Specify the number of hours to hold new signatures before making them available for download to other machines on the network.
MakeIncDownloading = 1	You can indicate that only files that have changed should be downloaded. This results in a smaller signature update file, and is known as an incremental download. An incremental download provides complete virus protection but may be faster than a full download. 1 = The download program will determine if a full update is necessary or if an incremental update can be used. 0 = Perform a full download.

Option	Description
IsDistributionServer = 0	1 = Maintain both full and incremental signature updates by downloading both and synchronizing them. If set to 1, this setting overrides the selection in MakeIncDownloading. We recommend that all redistribution servers maintain both full and incremental update signatures.

[OSID]

The [OSID] options map the platform name with the identifiers used to post items on the website. The values specified in this section appear in the signature set item section, in the Siglist.txt file found on the server, and in the user interface through a Platform.ini file.

Items in this section are set automatically, based on the list of currently supported platforms. Do not change the items in the [OSID] section.

Syntax for [OSID]

```
[OSID]
Linux (Intel) = 8
Sun Solaris = 9
;Windows 3x/Netware = 2
Windows 9x/ME = 3
Windows NT/2000 (x86) = 4
```

[ENGINEID]

The [ENGINEID] options map the engine names listed in the signature set to an ID value.

Syntax for [ENGINEID]

```
[ENGINEID]
INOCULATEIT = 1
VET = 2
```

Configure CA ARCserve Backup Engines

The CA ARCserve Backup Server Admin allows you to configure each engine to suit your needs.

Important! To manage and configure CA ARCserve Backup engines, you must be logged in to CA ARCserve Backup with the caroot password or a CA ARCserve Backup Administrator account.

To configure CA ARCserve Backup engines

1. Open the CA ARCserve Backup Server Admin by clicking Server Admin in the Quick Start menu.

The Server Admin window opens.

2. Click the Configuration toolbar button.



The Server Admin Configuration dialog opens.

3. Select the desired engine tab and specify the settings that suit your needs.

More information:

[Job Engine Configuration](#) (see page 451)

[Tape Engine Configuration](#) (see page 462)

[Database Engine Configuration](#) (see page 472)

[Alert Configuration](#) (see page 476)

Job Engine Configuration

The CA ARCserve Backup Job Engine controls the execution time of jobs in the job queue. It scans the job queue regularly, starting jobs as their execution dates and times are reached. CA ARCserve Backup provides the following job engine options:

- **Job Queue Scanning Interval (seconds)**--The Job Engine constantly scans the job queue for jobs that should execute. By default, the job queue is scanned every 10 seconds. To change the time interval, specify a number from 1 - 9999.
- **Retention Time for DONE Job (hours)**--Jobs with a final status of DONE remain in the job queue for the time specified in this field. By default, CA ARCserve Backup keeps DONE jobs for 24 hours before they are deleted from the queue. To change the time, specify a number between 0 and 999.

Note: Single occurrence staging jobs (disk to disk to tape and disk to tape to tape) will be removed from the job queue after the migration phase of the job is complete and the length of time specified for this option has elapsed.

- **Database Polling Interval (minutes)**--The Job Engine periodically polls the CA ARCserve Backup database to discover copied and purged sessions on staging enabled devices. The value specified in this field determines the time interval between polls. The default value for this field is five (5) minutes, and the minimum value is one (1) minute.
- **Message Type in Activity Log**--The Activity Log contains information about all CA ARCserve Backup activities. By default, notes, warnings, and errors that occur when running CA ARCserve Backup appear in its Activity Log. To change the types of messages, specify one of the following values:

None

No messages appear.

Errors

Only errors that occur while running CA ARCserve Backup appear.

Warnings & Errors

Warnings and errors that occur while running CA ARCserve Backup appear.

Notes, Warnings & Errors (default)

Includes all notes, warnings, and errors that occur while running CA ARCserve Backup.

Debug

Includes debugging information and all notes, warnings, and errors that occur while running CA ARCserve Backup.

- **Network Shares**--By default, CA ARCserve Backup opens Use All Shares in the Browser. This means that both Default Shares and User Shares are available for selection as either your source or destination for a job. To change the type of shares that are displayed in the Browser, specify one of the following:

Use Default Shares Only

Only administrative shares are available.

Use Users Shares Only

Only shares that have been specifically set by users are displayed.

- **Buffer Size (K Bytes)**--Defines the buffer size used by CA ARCserve Backup.

Default value: 256 KB

All computers behave differently. Factors affecting their behavior can be related to backup server hardware, the total size of the backup job, and the number child jobs that a backup job spawns. You can increase or decrease the size of the buffer to optimize your system's performance while performing a backup.

Increasing or decreasing the buffer size does not necessary improve backup and restore performance. For example, if the backup server has abundant system resources, such as a large amount memory, access to a fast network, and fast disk I/O, increasing the buffer size can increase the system's backup and restore performance. Conversely, if the backup server has limited system resources, reducing the buffer size can increase the system's backup and restore performance.

Note: For a typical server, the best practice is to apply the default value of the buffer size.

- **Backup**--Allows you to customize additional options in your backup jobs:

Record Hard Links for NTFS Volumes

If you back up hard links files, this information is included and preserved by default.

Default value: ON

Confirm when Overwriting Media

Any time a media is to be overwritten, CA ARCserve Backup can prompt you to confirm that you really want to overwrite the media. By default, this option is disabled (OFF). If you set this option, a confirmation dialog is displayed. If you do not respond within five minutes, the job is cancelled.

Default value: OFF

Backup Registry key details when an entire machine is selected

You can turn on the option to back up the Registry key details for target machines by clicking on the Backup registry key details when an entire machine is selected check box.

Default value: OFF

Enable Media Maximization

Lets you optimize disk and tape usage in GFS and rotation jobs. For more information, see [Media Maximization](#) (see page 396).

You cannot change this value from a member server. Member servers inherit the value specified for this option from the CA ARCserve Backup primary server.

Default value: ON

- **Retry Crashed Jobs after Job Engine Restart**--This option is a checkpoint mechanism. CA ARCserve Backup attempts to restart a crashed job if this box is checked. It should only be turned on if a cluster environment is configured to allow for fail-over.
- **Submit Makeup Jobs on HOLD**--Use this option to place a hold status on a job rather than a ready status.
- **Block pop-ups when data migration jobs finish**--When a staging migration job is finished, pop-up messages display to inform you if a job was successful, failed, and so on. If you do not want pop-up messages to appear after the migration job is finished, enable this option.
- **Block pop-ups when any job finishes**--When a job is finished, pop-up messages display to inform you if a job was successful, failed, and so on. If you do not want pop-up messages to appear after a job is finished, enable this option.

More information:

[Job Status Types](#) (see page 304)

CA ARCserve Backup Services, Components, and Applications that Require the Highest Available Privileges

An account with the highest-available privileges is a basic user account and a power user account with run-as administrative privileges.

The following CA ARCserve Backup services, components, and applications require an account with the highest available privileges:

ACSCFG.EXE

Volume Configuration utility for StorageTek ACSLS Library.

ADMIN.EXE

ARCserve Backup Agent Admin utility.

ALERT.EXE

CA ARCserve Backup Alert Service.

ARCSERVEMGR.EXE

CA ARCserve Backup Manager Console.

ASWANSYNC.EXE

Lets CA XOssoft interface with the CA ARCserve Backup Client Agent for Windows.

ATLCFG.EXE

Volume Configuration utility for IBM 3949 Library.

BAOFCONFMIGRATION.EXE

Upgrade tool for migrating the configuration for the previous version of the Agent for Open Files to the current version (Unicode format).

BDAEMON2.EXE

Raima DB Daemon Application.

CA_AUTH.EXE

ca_auth command line utility.

CA_BACKUP.EXE

ca_backup command line utility.

CA_DBMGR.EXE

ca_dbmgr command line utility.

CA_DEVMGR.EXE

ca_devmgr command line utility.

CA_JOBSECMGR.EXE

ca_jobsecmgr command line utility.

CA_LOG.EXE

ca_log command line utility.

CA_MERGE.EXE

ca_merge command line utility.

CA_QMGR.EXE

ca_qmgr command line utility.

CA_RECOVERDB.EXE

ca_recoverdb command line utility.

CA_RESTORE.EXE

ca_restore command line utility.

CA_SCAN.EXE

ca_scan command line utility.

CAADVREPORTS.EXE

caadvreports command line utility.

CAAGSTART.EXE

Lets the Universal Agent start processes that launch database agents. This is in internal utility that is not exposed to the end user.

CAAUTHD.EXE

Authentication service.

CABKWIZ.EXE

CA ARCserve Backup Backup Wizard

CACLURST.EXE

caclurst utility.

CADIAGINFO.EXE

Lets the Diagnostic wizard collect diagnostic information about CA ARCserve Backup from remote systems. This utility stores the collected diagnostic data in a file with a .caz file extension.

CADIAGSUPPORT.EXE

Lets CA Support personnel and end users open and view diagnostic information saved in diagnostic data (.caz) files.

CADIAGWIZ.EXE

Lets CA ARCserve Backup collect Windows system and network information from local and remote systems as it relates to CA ARCserve Backup. CA support can use the collected information to troubleshoot an ARCserve server.

CADISCOVD.EXE

Domain Server application.

CADVWIZ.EXE

Device Configuration Wizard.

CADVWIZE.EXE

Device Wizard for configuring devices.

CALICNSE.EXE

License check application.

CAMINFO.EXE

License information display application.

CAREGIT.EXE

Product registration application.

CAREPORTS.EXE

careports Report Writer Command Line utility.

CARSWIZ.EXE

CA ARCserve Backup Restore Wizard.

CASDSCSVC.EXE

Discovery Service.

CASERVED.EXE

Service Controller.

CASISCHK.EXE

Single instance support application.

CATIRPC.EXE

CA ARCserve Portmapper.

CAVER.EXE

Lets CA ARCserve Backup display the version and build number details of the CA ARCserve Backup base product in a graphical user interface.

CDBMERGELOG.EXE

Lets CA ARCserve Backup merge activity log details from the local cache to the ARCserve database.

CONFIGBAF.EXE

BAF (Bright Agent frame) configuration utility. The installation wizard launches this utility to register agents into a configuration file that is used by the Universal agent.

CONFIGENCR.EXE

Encryption configuration utility.

CSTMSGBOX.EXE

Lets CA ARCserve Backup show message boxes. This is in internal utility that is not exposed to the end user.

DBACFG.EXE

Lets CA ARCserve Backup configure account details for database agents.

DBENG.EXE

CA ARCserve Backup Database Engine.

DBTOSQL.EXE

Lets CA ARCserve Backup migrate Raima VLDB database information and data to Microsoft SQL Server databases.

DBTOSQL_EXP.EXE

Lets CA ARCserve Backup migrate Raima VLDB database information and data to Microsoft SQL Server 2005 Express Edition databases.

DUMPDB.EXE

Lets CA ARCserve Backup dump session or export session passwords stored in the database to a specified target file or import session password stored in file to database.

DVCONFIG.EXE

Device Configuration utility.

ERRBOX.EXE

Custom pop-up error display application.

EXPTOSQL.EXE

Microsoft SQL Server 2005 Express Edition to Microsoft SQL Server conversion utility.

GROUPCONFIG.EXE

Device Group Configuration utility.

IMPORTNODEINFO.EXE

Imports node information to CA ARCserve Backup database during upgrade.

INSTALLALERT.EXE

Used for installing Alert Modules.

JOBENG.EXE

CA ARCserve Backup Job Engine.

JOBWINDOW.EXE

Job window configuration utility.

JOBWINUTIL.EXE

Job window.

JOBWIZARD.EXE

Generic Job Scheduler Wizard.

LDBSERVER.EXE

ONCRPC service to handle Database Engine queries.

LIC98LOG.EXE

One of the CA ARCserve Backup license services

LIC98SERVICE.EXE

One of the CA ARCserve Backup license services

LIC98VERSION.EXE

One of the CA ARCserve Backup license services

LICDEBUG.EXE

Enables debugging for the license application.

LICRCMD.EXE

Enables remote command execution for the license application.

LOGWATNT.EXE

License application for providing the license event log management function.

LQSERVER.EXE

ONCRPC service to handle Job Queue queries.

MERGEALIC.EXE

License management component.

MERGEAT.EXE

Merge Catalog utility.

MERGEOLF.EXE

License management component.

MERGEROLF.EXE

License management component.

MMOADMIN.EXE

Media Management Option user interface.

MSGENG.EXE

CA ARCserve Backup Message Engine.

PFC.EXE

Preflight Check utility.

RMANCFG.EXE

Lets you configure Oracle databases that you are protecting using the Agent for Oracle.

SERVMIGRATION.EXE

Lets CA ARCserve Backup migrate BrightStor ARCserve Backup r11.x database information to the current database configuration.

SETUPRD.EXE

RAID configuration command line utility.

SETUPSQL.EXE

Builds CA ARCserve Backup database (creates ODBC connection, sets user and password in database for the database and creates tables for the database).

SQLCLEAN.EXE

Lets CA ARCserve Backup clean all destroyed media information in a Microsoft SQL Server database. This component runs after you format or erase media that contains SQL Server data.

SQLCLEAN_EXP.EXE

Lets CA ARCserve Backup clean all destroyed media information in a Microsoft SQL Server 2005 Express Edition database, when the media is formatted or erased.

SQLTOSQL.EXE

Lets CA ARCserve Backup migrate database information from BrightStor ARCserve Backup r11.x and older versions of the Microsoft SQL Server database to the current release.

SVRLESS.EXE

Lets CA ARCserve Backup update the designated data mover associated with jobs processed using the Serverless Backup Option.

TAPECOMP.EXE

Tape Compare command line utility.

TAPECOPY.EXE

Tapecopy command line utility.

UNIVAGENT.EXE

CA ARCserve Backup Universal Agent.

UPGRADEUTIL.EXE

Lets CA ARCserve Backup back up and restore configuration files and registry entries during the installation process. This component runs when you perform a build to build upgrade.

VSERVICE.EXE

Lets CA ARCserve Backup validate customer access privileges to an Exchange server when you are installing the Agent for Microsoft Exchange. This is in internal utility that is not exposed to the end user.

W95AGENT.EXE

Client Agent for Windows on Windows 95 and Windows 98.

Tape Engine Configuration

The CA ARCserve Backup Tape Engine identifies all the backup devices that are connected to your system. The default configuration log options can be changed; for example, when you want to troubleshoot a hardware or Tape Engine specific problem.

To modify any of the options, settings, and parameters described in the following sections, start the CA ARCserve Backup Server Admin and select the Tape Engine tab.

Tape Engine Message Log Options

The following lists describe tape engine message log options:

- **Level**--If you keep the default (Summary), you do not need to specify any other options. The available values are:
 - **None**--No information is logged. Tape Engine logging is halted and the Tape Engine Log does not appear in the Job Status Manager.
 - **Summary**--(default) Logs critical messages and reduces the size of the tape log by excluding unnecessary information. For this option, the Tape.log is present in the Job Status Manager. The Tape.log file, by default, is generated and stored in the CA ARCserve Backup\Log folder. If the log path needs to be changed, you can do so by creating an alternate log path entry in the registry file. For more information on creating an alternate log path entry, see *Alternate Path to the Tape Engine Log* in this chapter.
 - **Detail**--This option logs all commands sent to the attached backup devices by CA ARCserve Backup. Reads/Writes and Test Unit Ready commands are excluded. Tape Engine specific information, which may be used by CA Support to help troubleshoot backup and restore issues, is also logged. The Tape.log file, by default, is generated and stored in the CA ARCserve Backup\Log folder. If the log path needs to be changed, you can do so by creating an alternate log path entry in the registry file.

The Tape.log file for this option can be viewed in the Job Status Manager by accessing the Tape Log tab.

- **Detail with Read/Writes**--Logs all commands sent to attached backup devices by CA ARCserve Backup. Unlike the "Detail" option, this option includes Reads/Writes and Test Unit Ready commands. Tape Engine specific information, which may be used by CA Support to help troubleshoot backup and restore issues, is also logged. The Tape.log file, by default, is generated and stored in the CA ARCserve Backup\Log folder. If the log path needs to be changed, you can do so by creating an alternate log path entry in the registry file.

For more information on creating an alternate log path entry, see *Alternate Path to the Tape Engine Log* in this chapter. The Tape.log file for this option can be viewed in the Job Status Manager by accessing the Tape Log tab.

Note: You may incur a potentially large log file size due to the Read/Write capability. The Read/Write logging may impede performance on the machine.

- **Output**--If you specified either "Summary," "Detail," or "Detail with Reads/Writes," you can define where you want the messages sent. Specify one of the following:
 - Both Screen and File--The messages are recorded in the Tape Engine Log as well as to a DOS box (the Tape Engine Message window).
 - Screen Only--The messages are sent to the Tape Engine Message window only.
 - File Only--(default) The messages are recorded in the Tape Engine log only. You can view the Tape Engine log in the Job Status Manager.

Important! If you select either option, Both Screen and File or Screen Only, you must configure the CA ARCserve Tape Engine service such that it can interact with your desktop and display the contents of the tape log in a DOS window. For more information, refer to the section [Enable Interaction with the Desktop](#) (see page 471).

Specify Tape Engine Log Options

The Limit Log Size section of the Tape Engine tab on the Server Admin Configuration dialog lets you direct how CA ARCserve Backup controls the behavior of the Tape Engine's log files.

To specify Tape Engine log options

1. From the CA ARCserve Backup Manager interface, select Server Admin from the Quick Start Menu in the Navigation Bar on the Home Page.

The Server Admin window opens.

2. From the Domain/Server directory tree, select the server that you want to configure.

Click the Configuration toolbar button.

The Configuration - *Server Name* dialog opens.

3. Click the Tape Engine tab.

From the **Limit log size** section, specify the following options as applicable to your requirements:

- **Limit log size by**--Check the Limit log size by check box to enable Circular Logging. In the Limit Log Size By field enter the value that you want to specify as the maximum total size of all chunked TAPE.LOG files.

The Limit log size by value divided by the Maximum log file count value represents the maximum size of all chunked log files. For example, if you specify a Limit log size by value of 100 MB and a Maximum log file count of 10, CA ARCserve Backup chunks TAPE.LOG when it reaches 10 MB ($100/10 = 10$).

The default value for the limit log size by option is 100 MB, and the range is between 1 and 2000 MB.

To disable Circular Logging, clear the limit log size by check box.

- **Prune logs older than**--Use this option to specify the number of days that must elapse before CA ARCserve Backup prunes the log files.

The default value for the Prune logs older than option is 100 days, and the range is between 1 and 365 days.

- **Log file split criterion**--The options in this section define the behavior of how CA ARCserve Backup splits the log files.
 - **Maximum log file count**--Specifies the number of chunked log files CA ARCserve Backup retains.

The default value for the Maximum log file count option is 10, and the range is between 3 and 32.

Note: You can modify this setting only if the Limit log file size by option is specified.

- **Maximum single log file size**--This option works in conjunction with the Prune logs older than option. When you specify the Maximum single log file size and Prune logs older than options, CA ARCserve Backup switches to Circular Logging mechanisms when the TAPE.LOG reaches its maximum size, and deletes chunked log files when their age is greater than the value specified under the Prune logs older than option.

The default value for the Maximum single log file size option is 10000 KB, and the range is between 1 and 100000 KB.

Note: You can modify this setting only if the Prune logs older than option is specified.

4. Click OK to apply the Tape Engine log options.

The Tape Engine Log options are applied.

Note: Click Cancel to discard your changes.

Tape Engine General Options

CA ARCserve Backup lets you specify the following general options:

- **Use Global Scratch Set**--If you select this option, CA ARCserve Backup uses a Global Scratch Set. The Global Scratch Set treats all of the scratch tapes in all media pools as one large Scratch Set. This ensures that backup jobs never fail if a scratch tape is not available in its own media pool.

When this option is enabled, the Media Pool Manager shows only the Save Set for each pool (not the Scratch Set), but adds an object called GlobalScratchSet. This object contains all of the media available in the scratch sets of all your media pools. If you right-click GlobalScratchSet and select Assign Media, you can move media from an unassigned set to the Scratch Set.

When you select a media in the Global Scratch Set, two extra properties appear as column headings on the top right-hand pane and on the Properties tab in the lower-right hand pane: Medium Type and Media Pool. If you click a column heading on the top right-hand pane, you can sort the list by that column. If the media you select in the Global Scratch Set is vaulted, it appears in a different color to indicate that it is inactive.

Note: If you enable the Global Scratch Set and submit a backup job using a specific media pool, CA ARCserve Backup first attempts to find media in that media pool's Scratch Set. If no media is available, the Global Scratch Set media will be used. Also, if you specify a media pool and submit a backup job that spans tapes, media in the Global Scratch Set can be used.

- **Show Tape Log on Job Status Manager**--Select this option to view the Tape Log in the Job Status Manager. If the Activity Log is open when you enable this option, you must click Refresh to update the manager.

Note: This option is available only on Windows computers.

- **Use TapeAlert**--Enables CA ARCserve Backup to detect and report TapeAlert flags asserted by your tape drives and libraries. If you do not want to receive TapeAlert-related messages, disable this option.
 - When you enable this option, CA ARCserve Backup queries all devices connected to CA ARCserve Backup for TapeAlert flags in one minute intervals. If CA ARCserve Backup detects a TapeAlert flag, it reports real-time details about the flag in the Activity Log and the Tape.log file.
 - When you disable this option, CA ARCserve Backup does not maintain a separate thread-querying mechanism for detecting and reporting TapeAlert flags. As a result, CA ARCserve Backup will not query for TapeAlert flags until the job is running and a SCSI error occurs. If CA ARCserve Backup detects a TapeAlert flag while the job is running, it reports the details about the flag in the Activity Log and the Tape.log file.

Event Log Configuration (Windows Servers)

The Log tab allows you to enable or disable confirmation messages and to specify which messages may be written to the Windows Event Log.

- **Enable Message Logging into Event Log**--By default, all messages are written only into the CA ARCserve Backup Activity Log. If you check this box, the following groups of check boxes become enabled:
- **Exclude Message Type From Logging Check Boxes**--Use these check boxes to select which type of message should be excluded from the Event Log.
- **Exclude Message Logging From Check Boxes**--Use these check boxes to exclude all messages from a particular CA ARCserve Backup module.

How CA ARCserve Backup Records Events in the Windows Event Viewer

Event Viewer is a Windows administrative tool that lets you monitor events that relate to application, security, and system logs. The information stored in Event Viewer can vary, based on the role of the computer to your environment and the applications that are running on the computer.

Note: To open Event Viewer, click Start on the Windows toolbar, select Programs, Administrative Tools, and click Event Viewer.

The Server Admin lets you specify the type of CA ARCserve Backup event information that you want to record in Event Viewer. For more information, see [Event Log Configuration](#) (see page 467).

The list that follows describes the event codes for CA ARCserve Backup information, warning, and error events that appear in Windows Event Viewer.

- **500**--Most information events and agent information events
- **600**--Agent warning events
- **700**--Agent error events
- **900**--Audit events
- **Unique event codes**--resource ID of the message

The diagram that follows displays CA ARCserve Backup events in Windows Event Viewer.

Type	Date	Time	Source	Category	Event	User	Computer
Information	9/22/2008	11:45:19 ...	CA ARCserve Backup	(55)	500	N/A	SHADA07-...
Information	9/22/2008	11:45:19 ...	CA ARCserve Backup	(55)	500	N/A	SHADA07-...
Information	9/22/2008	11:45:07 ...	CA ARCserve Backup	(55)	500	N/A	SHADA07-...
Information	9/22/2008	11:45:07 ...	CA ARCserve Backup	(55)	500	N/A	SHADA07-...
Information	9/22/2008	11:45:07 ...	CA ARCserve Backup	(55)	500	N/A	SHADA07-...
Information	9/22/2008	11:45:01 ...	CA ARCserve Backup	(55)	500	N/A	SHADA07-...
Information	9/22/2008	11:44:37 ...	CA ARCserve Backup	(55)	1406	N/A	SHADA07-...
Warning	9/22/2008	11:33:17 ...	CA ARCserve Backup	(50)	600	N/A	SHADA07-...
Warning	9/22/2008	11:33:17 ...	CA ARCserve Backup	(30)	600	N/A	SHADA07-...
Information	9/22/2008	11:33:17 ...	CA ARCserve Backup	(55)	500	N/A	SHADA07-...
Information	9/22/2008	11:33:17 ...	CA ARCserve Backup	(25)	500	N/A	SHADA07-...
Error	9/22/2008	11:33:17 ...	CA ARCserve Backup	(20)	700	N/A	SHADA07-...
Error	9/22/2008	11:33:17 ...	CA ARCserve Backup	(55)	700	N/A	SHADA07-...
Information	9/22/2008	11:28:54 ...	CA ARCserve Backup	(30)	7101	N/A	SHADA07-...
Error	9/22/2008	11:28:24 ...	CA ARCserve Backup	(15)	1303	N/A	SHADA07-...
Error	9/22/2008	11:27:58 ...	CA ARCserve Backup	(15)	1301	N/A	SHADA07-...
Information	9/22/2008	11:24:09 ...	CA ARCserve Backup	(50)	900	N/A	SHADA07-...
Information	9/22/2008	11:23:08 ...	CA ARCserve Backup	(50)	900	N/A	SHADA07-...
Information	9/22/2008	11:00:17 ...	CA ARCserve Backup	(50)	900	N/A	SHADA07-...

More information:

[Event Log Configuration \(Windows Servers\)](#) (see page 467)

Alternate Path to the Tape Engine Log

You can change the default tape log path if, for example, you want to move the log to a volume with more space. You can create an alternate location for the file by configuring a registry setting in the Windows NT registry. Create a String Value called "LogPath" under the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\Base\TapeEngine\Debug

Set the value to the local drive path you want to use as the new log file location (for example, D:\temp\log). After the log path is established, you can enable it by either restarting the Tape Engine or changing one of the logging options described earlier. To change the tape log path back to the default, you can remove the "LogPath" value and restart the Tape Engine.

Note: Alternate paths can only be local drives as mapped drives are not supported for redirecting the log.

Circular Logging

Circular Logging is a process that lets you control the size and behavior of the Tape Engine log file. Using this feature, you can set a size limit that directs CA ARCserve Backup to chunk the log file into smaller log files when a user-specified size limit is exceeded. Additionally, you can specify a retention period, total count, or both for log files. After the retention period elapses, CA ARCserve Backup deletes the chunked log files.

The Tape Engine log file is labeled TAPE.LOG. It can be found in the CA\ARCserve Backup\LOG directory.

To configure and use Circular Logging, start the Server Admin from the Quick Start menu on the CA ARCserve Backup Home Page. For more information see [Specify Circular Logging Settings](#) (see page 470).

Log File Names

If you do not specify Circular Logging settings, CA ARCserve Backup uses the default file name, TAPE.LOG. If you do specify settings, TAPE.LOG is still generated, but it is chunked into smaller files and the smaller files are named using the following format:

TAPE.LOG.####

where #### represents the sequential log number created on a given day.

Example: Log File Names

For example, on a given day, the Tape Engine generates three log files based upon a file size limit of 100 MB. The log file names are as follows:

TAPE.LOG
TAPE.LOG.0001
TAPE.LOG.0002

How CA ARCserve Backup Labels Log Files

To create the log files, CA ARCserve Backup labels the log files using the following guidelines:

1. If TAPE.LOG reaches a specified value, CA ARCserve Backup renames TAPE.LOG to TAPE.LOG.0001, and creates a new TAPE.LOG file.
2. If TAPE.LOG reaches a specified value for the second time, CA ARCserve Backup renames TAPE.LOG.0001 to TAPE.LOG.0002, renames TAPE.LOG to TAPE.LOG.0001, and creates a new TAPE.LOG file.
3. If TAPE.LOG reaches a specified value for the third time, CA ARCserve Backup renames TAPE.LOG.0002 to TAPE.LOG.0003, renames TAPE.LOG.0001 to TAPE.LOG.0002, renames TAPE.LOG to TAPE.LOG.0001, and creates a new TAPE.LOG file.

This process continues in a cyclical manner. CA ARCserve Backup always retains the latest three log files.

Important! CA ARCserve Backup calculates the value in which a new log file is created based upon the amounts that you specify in the Limit Log Size By and Log File Count options. For example, if you specify a Log Limit Size By amount of 500 MB and a Log File Count of 10, CA ARCserve Backup creates a new log file when the current log size exceeds (500 divided by 10) 50 MB.

Specify Circular Logging Settings

Circular Logging lets you customize the characteristics of log files generated by the Tape Engine.

To specify Circular Logging settings

1. From the CA ARCserve Backup Home Page, click the Quick Start menu and select Server Admin.
The CA ARCserve Backup Server Admin dialog opens.
2. From the Admin menu, select Configuration.
The Configuration dialog opens.
3. Click the Tape Engine tab.
4. To enable Circular logging, click the Limit Log Size By option in the Limit Log Size section of this dialog, and then specify then maximum size in MB. This amount represents the maximum size of all log files.
5. In the Log File Count field, select the number of log files that you want CA ARCserve Backup to retain. This amount represents the maximum number of TAPE.LOG files that CA ARCserve Backup will retain.

6. Click OK to apply the settings.

Note: After the log file count exceeds the number specified using the Log File Count option, CA ARCserve Backup deletes the oldest log files.

Prune Log Files

To specify log file pruning only:

1. Disable the Limit Log Size By option.
2. Click the Prune Logs Older Than option and specify the number of days that you want to elapse before CA ARCserve Backup prunes log files.
3. (Optional) In the Single Log File Size field, enter a size in KB to specify a size limit for a single log file. If you do not specify a value in the Single Log File Size field, CA ARCserve Backup uses the default value, 10000 KB, as the size limitation for each single log file.
4. Click OK to apply the settings.

Important! If you enable both Limit Log Size options (Limit Log Size By and Prune Logs Older Than), CA ARCserve Backup prunes log files if either the total number of log files exceeds the Log File Count, or the date of the log files exceeds the number of days specified under the Prune Log Files Older Than option. You cannot specify a Single Log File Size—CA ARCserve Backup uses the formula Total Log Size divided by Log File Count to calculate the Log File Size setting.

Enable Interaction with the Desktop

This section describes how to enable the CA ARCserve Backup Tape Engine to interact with the desktop. However, these steps can be used when you want to allow any CA ARCserve Backup service or engine to interact with the desktop.

To enable interaction with the desktop

1. From the Windows Start menu, select Programs (or All Programs), Administrative Tools, and select Component Services.

The Component Services dialog opens.

2. From the object tree, select the Services (Local) object.

In the Services list, locate, right-click CA ARCserve Tape Engine (for example), and select Properties from the pop-up menu.

The CA ARCserve Tape Engine Properties (Local Computer) dialog opens.

3. Select the Log On tab.
Under Local System account, select the Allow service to interact with desktop option and click Apply.
Click OK to close the CA ARCserve Tape Engine Properties (Local Computer) dialog.
4. Stop and then restart the CA ARCserve Tape Engine service.
The Tape Engine can interact with the desktop.
5. Close the Windows Component Services dialog.

Database Engine Configuration

The CA ARCserve Backup Database Engine stores the following types of statistical information for all jobs processed.

- Files and directories that have been backed up, copied, and restored.
- Jobs that CA ARCserve Backup has processed.
- Storage devices and media used for CA ARCserve Backup operations.

CA ARCserve Backup provides the following database engine options:

- **Enable auto pruning**--When database pruning is enabled, information about the files and directories that were backed up or copied in a session is deleted. By default, this option is selected to free up space in the database file. It can be useful to disable this option to maintain the detailed information for restoring purposes, but be aware that your database can become very large if you do not prune it.
 - **Run Pruning at**--This field is active only if the Enable Database Pruning option is on. Specify when you want the pruning operation to run.
Default value: If enabled, will occur at 12:00 p.m.
 - **Prune database records older than**--This field is active only if the Enable Database Pruning option is on. Specify how long records should be kept in the database before CA ARCserve Backup prunes them.
Default value: If pruning is enabled, 30 days.
Range: 1 to 999 days.

- **Delete Re-Formatted or Erased Media-Related database Records when Pruning**--When you reformat or erase a media, CA ARCserve Backup also deletes the records in the database that pertain to the media. Performing this extra step, however, can be a time-consuming process. Select this option to postpone deleting these records until pruning is performed.
- **Prune activity logs older than**--Specify how long activity logs should be kept in the database before CA ARCserve Backup prunes them.
Default value: 14 days
Range: 1 to 999 days.
- **Prune catalog files older than**--Specify how long catalog files should be kept in the database before CA ARCserve Backup prunes them.
Default value: 60 days.
Range: 1 to 999 days.

- **Database Maintenance Operations**--The following options apply to maintenance operations that can be performed on the CA ARCserve Backup database.

When you enable the following options, CA ARCserve Backup performs the specified task the next time the Database Pruning Job runs. If the Database Pruning Job is scheduled to run on a daily basis, the specified operations are performed when the pruning job runs. To schedule the database maintenance operations to run without the dependence of the Database Pruning Job, you can use the Job Scheduler Wizard to create individual jobs that use the `ca_dbmgr` command line utility to facilitate the database maintenance operations.

Note: For more information, see the *Command Line Reference Guide*, the Online Help, or [How You Can Use the Job Scheduler Wizard to Schedule Jobs](#) (see page 322).

- **Update statistics**--This option lets CA ARCserve Backup update table and index statistics. With correct and up-to-date statistical information, SQL Server and SQL Server 2005 Express can determine the best execution plan for queries, which improves query performance.

You should update the statistics on a daily basis.

- **Re-build indexes**--This option lets CA ARCserve Backup remove fragmentation (by compacting the pages based on the specified or existing fill factor setting) and reorder the index rows in contiguous pages. As a result, CA ARCserve Backup improves query performance and reclaims disk space.

You should rebuild the indexes on a weekly basis.

- **Check DB integrity**--This option lets CA ARCserve Backup check the allocation, structural, and logical integrity of all the objects in the ARCserve database.

You should check the integrity of the database on a weekly basis and allocate a sufficient amount of time for this task to run.

- **Reduce DB size**--This option lets CA ARCserve Backup reclaim disk space on your system by reducing the size of the data files in the ARCserve database.

You should reduce the size of the database on an as-needed basis.

- **Submit Prune Job**--Select this option to submit the pruning job now.
- **Submit ARCserve DB protection job**--This option lets you recreate the CA ARCserve Backup Database Protection Job because the original job was deleted. For more information, see [Recreate the CA ARCserve Backup Database Protection Job](#) (see page 573).

- Catalog Database

- **Catalog database folder--**This option let you specify the location of the CA ARCserve Backup catalog database folder. Click the ellipsis button to browse and select a different location for the catalog database folder.

By default, the catalog database folder will be located on the Primary Server at:

C:\Program Files\CA\ARCserve Backup\CATALOG.DB\

- **Compress catalog transfer on the following member servers--** This option lets CA ARCserve Backup compress catalog information when the data is transferred from a member server to the primary server.

If the Primary Server has any associated Member Servers, the "Compress catalog transfer on the following member servers" field will be enabled, displaying the names of the Member Servers.

By default, this option is disabled. With this option disabled, CA ARCserve Backup will not compress the catalog information when it is transferred from the Member Server to the Primary Server.

- **Minimum disk free space threshold--**This option lets you specify the minimum percentage of free disk space when CA ARCserve Backup deletes catalog files.

Default value: 10 %

Range: 1% to 99%

Note: CA ARCserve Backup periodically checks the free disk space percentage on the volume where the catalog database folder is located. If the detected free space is lower than the specified percentage, a warning message will be sent to the activity log and it would automatically begin to delete catalog database files (minimum of 7 days old and starting with the oldest first) from the disk until the detected free space percentage is greater than the threshold setting.

Example: If the detected free space is lower than the 10%, a warning message is sent to the activity log and it would automatically begin to delete catalog database files (minimum of 7 days old and starting with the oldest first) from the disk until the detected free space percentage is greater than 10%.

- **Enable Media Pool Maintenance**--When selected, all media scheduled to be moved from a media pool's Save Set to its Scratch Set are automatically moved any time a prune job is run.
- **Maximum Database Server Memory**--This applies to Microsoft SQL Express only. Used to ensure that the size of the Microsoft SQL Express memory usage does not exceed this limit.

Default value: 1024 MB

Range: 256 MB to 1024 MB

More information:

[How to Protect the CA ARCserve Backup Database](#) (see page 555)

[How the Catalog Database Works](#) (see page 597)

Alert Configuration

Alert is a notification system that sends messages to people in your organization using various methods of communication. Alert does not generate its own messages. You must tell Alert what information you want to communicate and where you want to send it.

If you configure Alert from Server Admin, you can generate notifications for non-job related events, such as starting or stopping the Tape Engine. To do this, enter the words or phrases you want to communicate in exactly the same format as they appear in the Activity Log and click Add.

Or, if you want to send all activity log messages, enter an asterisk and click Add. Alert generates notification messages and sends them to the appropriate recipients. For information on selecting recipients and configuring methods to transmit Alert notifications, see the chapter "Using the Alert Manager."

Add and Remove Alert Notifications

CA ARCserve Backup lets you configure notifications Alert notifications for non-job related events (for example, starting and stopping the Tape Engine and the successful completion of operations) using the Server Admin Manager.

The procedure that follows describes how to add Alert notifications for non-job related events.

To add alert notifications

1. Open the CA ARCserve Backup Server Admin Manager.

Click the CA ARCserve Backup primary server or stand-alone server in the directory tree, and then click Configuration on the toolbar.

The Configuration dialog opens.

2. Click the Alert tab.

In the Alert list field, enter the text for the event for which you want to receive an Alert notification.

You can enter a complete phrase, or only a part of it (even a single keyword). The Alert engine tries to match the keyword or phrase to the text of each generated event. However, you should be as specific as possible, in order to avoid receiving unwanted Alert notifications.

Examples:

- To receive an Alert notification when the Tape Engine starts, enter engine in the Alert list to have Alert detect the event. However, the Alert engine then sends notifications for any events that related to engine, such as Database engine started.
- To receive Alert notifications for all activity log messages, enter '*'.
- To receive Alert notifications for Audit log events, enter the following in the Alert list field:
 - [Auditlog]--Sends an Alert notification for all Audit Log events.
 - [Auditlog][Success]--Sends an Alert notification for all successful Audit Log events.
 - [Auditlog][Failure]--Sends an Alert notification for all failed Audit Log events.

Note: The keywords for Audit Log events are case-sensitive and square brackets are required.

3. Click Add to add the search text.
4. Click OK.

When the text of an event matches one of the keywords you have entered, the Alert engine generates Alert notifications for all recipients previously configured using the Alert Manager.

The procedure that follows describes how to remove Alert notifications.

To remove Alert notifications

1. Open the CA ARCserve Backup Server Admin Manager.

Click the CA ARCserve Backup primary server or stand-alone server in the directory tree, and then click Configuration on the toolbar.

The Configuration dialog opens.

2. Click the Alert tab.

From the Alert list, click the event for which you no longer want to receive Alert notifications, and then click Delete.

The Alert notification is deleted.

Note: To delete all Alert notifications from the Alert list, click Delete All.

3. Click OK to close the Configuration dialog.

Additional Server Admin Functions

You can use the Server Admin to perform the following functions:

- Change the system account
- Configure multiple NIC cards
- Manage licenses centrally

Change or Modify the CA ARCserve Backup System Account

The CA ARCserve Backup Server requires a valid user account on the host Windows machine (initially entered during installation). You can change the login credentials for the system account at any time, using the Server Admin.

If you are using a Windows domain user account to serve as the credentials for the CA ARCserve Backup server system account, you must update CA ARCserve Backup with the new password when you change your Windows domain password.

To change or modify the System Account

1. From the CA ARCserve Backup Home Page, open the Server Admin by selecting Server Admin from the Quick Start menu.

The CA ARCserve Backup Server Admin window opens.

2. Select CA ARCserve Backup System Account from the Server Admin menu.

The CA ARCserve Backup System Account dialog opens.

3. Complete the following fields, as required:

- Server
- User Name
- Password
- Domain

4. Click OK.

The credentials for the System Account are changed.

Reconfigure Node Tier Assignments

You can use the CA ARCserve Backup Server Admin to change the assigned priority classifications of your CA ARCserve Backup the nodes. The priority classifications are divided into three tier groupings (Tier 1, Tier 2, and Tier 3), with Tier 1 representing the high-priority (business-critical) nodes and Tier 3 representing low-priority nodes. These tiers are used to filter the information displayed on the CA ARCserve Backup Dashboard by the priority level of the monitored nodes.

The Node Tier Configuration dialog contains three priority categories, and is automatically populated when a node is added to your system and browsed. By default, Tier 1 is configured to include all CA ARCserve Backup servers (Primary and Member) and any nodes with CA ARCserve Backup application agents installed (such as Oracle, Microsoft Exchange, Microsoft SQL Server, Microsoft Sharepoint, and so on), and Tier 3 is configured to include all other nodes (having file system agents installed). Tier 2 is not configured to include any nodes, and is available for customized use.

The node assignments for each tier can be reconfigured and customized to meet your individual needs by using the Node Tier Configuration dialog, which is accessed from the CA ARCserve Backup Server Admin or from the Backup Manager (right click 'Windows systems' in Source tab).

To reconfigure node tier assignments

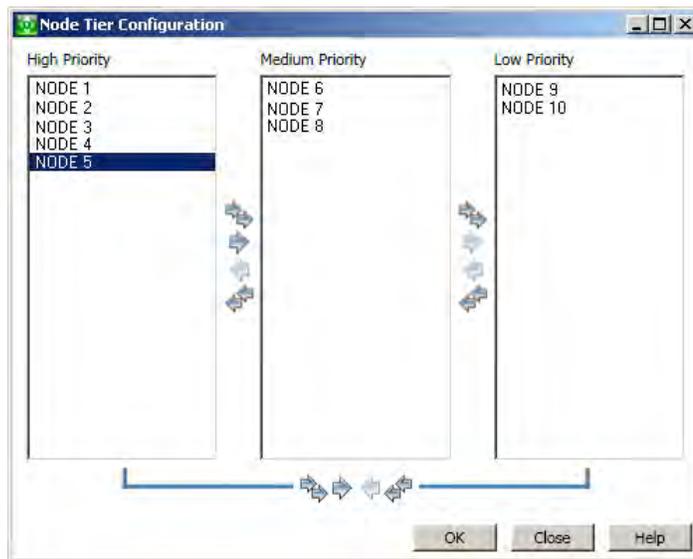
1. Open the CA ARCserve Backup Server Admin by clicking Server Admin on the Quick Start menu on the Home Page.

The Server Admin window opens.

2. Expand the domain directory tree and select a server that you want to view or reconfigure the node tier assignments.

3. Select the Node Tier Configuration option from the Admin menu.

The Node Tier Configuration dialog opens, displaying the nodes assigned to each Tier category (Tier 1, Tier 2, and Tier 3).



4. Select the node(s) that you want to reassign to a different tier category and click on the corresponding arrow icon to move the selected node(s) from one tier to another.

Note: Multiple nodes can be selected for tier assignment by using the "CTRL" or "SHIFT" key combinations.



The single arrow icon will move just the selected node(s).



The double arrow icon will move all nodes within that tier.

5. Click OK when done.

The node tier assignments have been changed to meet your individual needs.

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 primary server, stand-alone server, member servers, and agent servers in a CA ARCserve Backup domain.
- Identify the total number of licenses installed and the number of active licenses for each component in a CA ARCserve Backup domain.
- View the names of the servers using the component licenses in a CA ARCserve Backup domain.
- Release licenses from servers to make the licenses available to other servers in your domain.

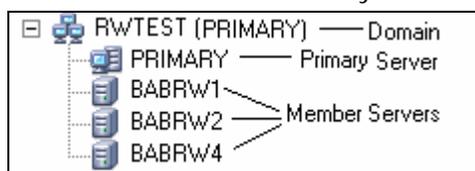
Note: For information about releasing licenses from servers, see [Release Licenses from Servers](#) (see page 483).

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:

Products Installed: 10		
Product Name	Version	Build
CA ARCserve Backup	12.5	5665
Central Management Option	12.5	5665
Tape Library Option	12.5	5665
Disk to Disk to Tape Option	12.5	5665
Agent for Microsoft SQL Server	12.5	5665
Enterprise Module	12.5	5665
Disaster Recovery Option	12.5	5665
NDMP NAS Option	12.5	5665
Client Agent for Windows	12.5	5665

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

The License Management dialog opens.

The License Management dialog provides you with the following information:

License status

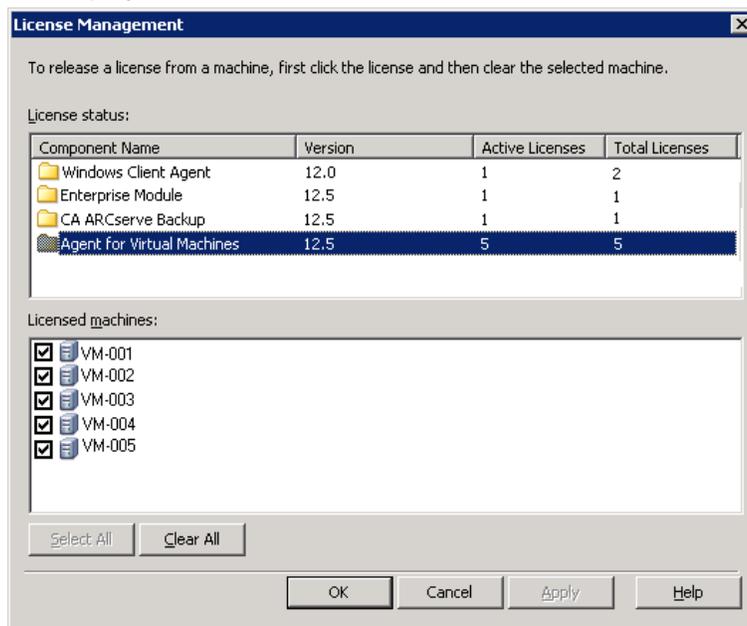
Specifies the version (release number), the number of active licenses, and the total number of licenses installed for each CA ARCserve Backup component in your CA ARCserve Backup domain.

Licensed machines

Specifies the names of the servers using an active license for the selected CA ARCserve Backup component.

Example:

For example, the following dialog illustrates that there are five total licenses and five active licenses for the Agent for Virtual Machines. The host names of the machines using the Agent for Virtual Machines display in the Licensed machines field.



More information:

[Central License Management](#) (see page 54)

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.

Configure Multiple Network Interface Cards

If the CA ARCserve Backup server has more than one network connection, CA ARCserve Backup can be configured to use a specific network interface card for its backup and restore operations. If you configure CA ARCserve Backup in this manner, it will not interfere with the other cards that are attached to the system.

You can configure CA ARCserve Backup to use a set of network interface cards, which it effectively uses when performing multistreaming backups. You can also configure CA ARCserve Backup to use an appropriate card from the configured set of network interface cards when connecting to a client agent.

To configure multiple network interface cards

1. From the CA ARCserve Backup Home Page, open the Server Admin by selecting Server Admin from the Quick Start menu.
The CA ARCserve Backup Server Admin window opens.
2. Select Multiple Network Cards from the Server Admin menu.
The Multiple Network Cards settings dialog opens.
3. Select one of the following options:
 - **OS decide which network card to be used (default)**--Lets the operating system decide which network interface card is to be used.
 - **Use selected network card**--Lets you specify the network interface cards that you want to use from the list. When configured in this manner, any job that CA ARCserve Backup executes defaults to the first network interface card. When you are using multistreaming, and more than one process is created, each subsequent process will use the next configured network interface card.
4. Click OK.
The network card settings are applied.

Authentication Levels for CA ARCserve Backup Services, Components, and Applications

An administrative account or an account with the highest available permissions is required to run various CA ARCserve Backup services, components, and applications on Windows Vista and Windows Server 2008 operating systems. The binaries corresponding to these services, components, and applications contain CA ARCserve Backup specific functionality that is not available to a basic user account. As a result, Windows will prompt you to confirm an operation by specifying your password or by using an account with administrative privileges to complete the operation.

The following sections describe the authentication levels required for CA ARCserve Backup components.

CA ARCserve Backup Services, Components, and Applications that Require Administrative Privileges

The administrative profile or an account with administrative privileges has read, write, and execute permissions to all Windows and system resources.

The following CA ARCserve Backup services, components, and applications require administrative privileges:

_HTMSETUP.exe

Shows the html page during Setup.

AGENTDEPLOY.exe

Agent Deployment application.

AGLFPROB.exe

Dashboard SRM (storage resource management) back-end service for collecting the agent storage resource information for Dashboard.

ALADMIN.exe

Alert administration application.

ARCSERVECFG.exe

Server Configuration Wizard.

ASREMSVC.exe

Lets you install CA ARCserve Backup on a remote system.

AUTHSETUP.exe

Authentication Setup command line utility.

BABHA.exe

Lets you configure CA ARCserve Backup for high availability. This component is commonly used with Microsoft Cluster Service installations.

BACKINT.exe

Backup integration module for the Agent for SAP R/3 for Oracle.

BACKINTCONFIG.exe

Configuration utility for the Agent for SAP R/3 for Oracle.

BCONFIG.exe

Lets CA ARCserve Backup configure server information (for example, a primary server, a member server, or a stand-alone server) as it relates to the type of ARCserve database and the caroot password. This component runs when you are installing or upgrading CA ARCserve Backup.

BDELOBJ.exe

Lets the uninstallation process delete temporary and dynamic files from a system where you are uninstalling CA ARCserve Backup. The uninstallation process copies this application to the target system.

BDELOBJ_BAB.exe

Lets the installation process delete temporary and dynamic files from a system where you are upgrading CA ARCserve Backup from a previous release. The uninstallation process copies and replaces this application to the target system.

CABATCH.exe

cabatch command line utility.

CABATCHNW.exe

Lets you submit jobs and other tasks to systems running CA ARCserve Backup products on NetWare-based systems.

CALICENSE.exe

CA ARCserve Backup License Application for monitoring each option's License account number.

CAREGIT.exe

Product registration application.

CARUNJOB.exe

Local backup and restore utility.

CHECKIA64.exe

Lets the installation process detect information about operating systems and applications running on IA64 supported operating systems.

CHGTEST.exe

Test Changer utility.

DBACONFIG.exe

Lets CA ARCserve Backup configure database instances during the installation process for the following agents:

- Agent for Microsoft SQL Server
- Agent for Oracle
- Agent for SAP R/3 for Oracle
- Agent for Informix
- Agent for Sybase
- Agent for Lotus Notes

Lets you configure database instances after the installation process is complete for the following agents:

- Agent for Microsoft SQL Server
- Agent for Oracle
- Agent for SAP R/3 for Oracle
- Agent for Informix
- Agent for Lotus Notes

DELETEME.exe

Lets the installation process delete temporary files from remote systems when installing CA ARCserve Backup components on a remote system. This component runs on the local and remote system.

DELETEOPT_W2K.exe

Lets CA ARCserve Backup remove residual files from a Windows 2000 system after CA ARCserve Backup is uninstalled from the system.

DEPLOYDUMMY.exe

Agent Deployment application pre-load module.

DSCONFIG.exe

Discovery Configuration utility.

EMCONFIG.exe

Enterprise Module Configuration utility.

ETPKI_SETUP.exe

ETPKI encryption/decryption library installation utility.

INSTSQL2005E.exe

Lets the installation process install Microsoft .NET Framework and Microsoft SQL Server 2005 Express when you specify Microsoft SQL Server 2005 Express Edition during the installation process.

LICCHECK.exe

Lets the CA ARCserve Backup Agent for Lotus Domino and the CA ARCserve Backup Agent for Informix check the status of their licenses.

MASTERSETUP.exe

Lets the installation process launch Windows Installer 3.1 and VC8 SP1 redistribute package.

MASTERSETUP_MAIN.exe

Lets the installation process display the installation wizard dialogs, configure, and call individual products when you are installing CA ARCserve Backup.

MEDIASVR.exe

Proxy for Tape Engine Communication.

ORAUPGRADE.exe

Upgrades Oracle Agent used during the upgrade of an old version of CA ARCserve Backup to the current version.

RAIDTEST.exe

Lets you configure and test RAID devices using a Windows command line utility. You can configure and tape RAID and tape changer RAID devices, not actual RAID.

RMLIC.exe

Module that uninstalls License Modules.

SETUP.exe

Installation Wizard.

SETUPFW.exe

Windows Firewall Configuration utility.

SETUPSQL.exe

Lets CA ARCserve Backup create the ARCserve database with Microsoft SQL Server when you are installing or upgrading CA ARCserve Backup.

SETUPSQL_EXP.exe

Lets CA ARCserve Backup create the ARCserve database with Microsoft SQL Server 2005 Express Edition when you are installing or upgrading CA ARCserve Backup.

SILENT.exe

CA ARCserve Backup License Application.

SIMULATE.exe

Lets CA ARCserve Backup configure fictitious SCSI devices (for example, tape drives and tape libraries) based on their filesystem. This CA ARCserve Backup component is a command line utility.

SMPLEMON.exe

Dashboard component for collecting storage resource utilization at the Agent node.

SPS012UPGRADE.exe

Upgrades the CA ARCserve Backup Agent for SharePoint 2007 used during the upgrade of an old version of CA ARCserve Backup to the current version.

SPADMIN.exe

Agent for SharePoint 2003 installation wizard.

SQLAGENTRMTINST.exe

Agent for Microsoft SQL Server installation wizard.

SQLCONFIG.exe

Agent for Microsoft SQL Server configuration utility.

TAPEENG.exe

CA ARCserve Backup Tape Engine.

TAPETEST.exe

Test Tape Drive utility.

UNINSTALLER.exe

Application that uninstalls the ETPKI component.

UPDATECFG.exe

Saves the configuration file during upgrade.

<CD_ROOT>\IntelINT\Exchange.DBA\SETUP.exe

Lets CA ARCserve Backup launch the following executables:

IntelINT\Exchange.DBA\Exchange.DBA\SETUP.exe

Installs the Agent for Microsoft Exchange for database level backups.

IntelINT\Exchange.DBA\ExchangeD.DBA\SETUP.exe

Installs the Agent for Microsoft Exchange for document level backups.

<CD_ROOT>\IntelINT\EO\SETUP.exe

Lets CA ARCserve Backup launch the Windows installer labeled MSIEXEC.exe to install the MSI package.

<CD_ROOT>\SETUP.exe

Lets CA ARCserve Backup launch the CD browser so that you can install or upgrade CA ARCserve Backup.

UPDATECFG.exe

Lets CA ARCserve Backup back up the registry and file entries from previous BrightStor ARCserve Backup and CA ARCserve Backup installations when you are upgrading from a previous release.

CA ARCserve Backup Domains

CA ARCserve Backup domains are a logical grouping of CA ARCserve Backup domain primary and member servers that allow easier administration of CA ARCserve Backup servers and users. In addition to providing a single sign-on to multiple CA ARCserve Backup servers, it also provides the same access level (privileges) on all the servers for the same user.

A CA ARCserve Backup domain has a name and a collection of one primary and one or more member servers. This allows you to manage any server from the CA ARCserve Backup domain to perform database management, tape and device management, and backup policy and schedule management without requiring logging in to each CA ARCserve Backup server separately.

Primary servers dispatch instructions about jobs and tasks to member servers in a CA ARCserve Backup domain. If a primary server becomes disabled or unavailable for a period time, tasks such as executing scheduled jobs and authenticating licenses on member servers will not function properly.

Each domain has a name, a mandatory designated primary server, and optional member servers. From the primary server, you can start and stop CA ARCserve Backup services on any member server in the domain.

When configuring the primary and member servers in a domain, the CA ARCserve Backup domain name must be the same on all computers in the domain. You must define the CA ARCserve Backup domain name when you install the primary server. You can reconfigure the domain name using the Server Configuration Wizard to change the domain membership. This wizard configures the CA ARCserve Backup domain name for all of the domain.

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.

Manage Domain Users and Groups Using the ca_auth Command Line Utility

To manage the domain user and groups, CA ARCserve Backup provides a command line utility called ca_auth.

For more information about domain user management, type ca_auth under the command prompt, or see *Command Line Reference Guide*.

Create caroot Equivalence

By default, CA ARCserve Backup creates a caroot equivalency for the administrator user on the primary and all member servers during setup. However, it does not create this equivalency for any other users on the member servers and all other member users. Hence, prior to using the command line utilities in a CA ARCserve Backup domain, you must create this equivalency.

By creating an equivalence list, all clients can use CA ARCserve Backup without the user logging into the Domain. CA ARCserve Backup can validate if the current user has equivalent access to the domain. The access rights to the operating system ensure a particular access level to the CA ARCserve Backup domain.

For more information about creating equivalence, see the section about ca_auth in the *Command Line Reference Guide*.

More information:

[Equivalence](#) (see page 36)

[Equivalency and the System Account](#) (see page 37)

Manage User Profiles Using the User Profile Utility

The CA ARCserve Backup User Profile utility lets the CA ARCserve Backup administrator control user access to CA ARCserve Backup.

The following sections describe how to:

- Add a user profile.
- Delete a user profile.
- Change a user's password.
- Assign a user to a group.

Add a User Using the User Profile Utility

A default user is created when CA ARCserve Backup is installed. The default user name is caroot.

To add a new user profile

1. Select User Profile from the Utilities menu on the CA ARCserve Backup Manager Home Page.
The Profile Manager opens.
2. Click the Add User toolbar button.
The Add User dialog opens.
3. Enter a user name and password in the appropriate fields, and then re-enter the user's password to confirm the first entry.
4. Click OK.

Delete a User Using the User Profile Utility

To delete a user profile

Note: You cannot delete the default CA ARCserve Backup user name.

1. Select User Profile from the Utilities menu on the CA ARCserve Backup Manager Home Page.
The Profile Manager opens.
2. Select the user profile that you want to modify and click the Delete User toolbar button.
3. Click OK to confirm.

Change a User Password Using the User Profile Utility

To change a user password

1. Select User Profile from the Utilities menu on the CA ARCserve Backup Manager Home Page.
The Profile Manager opens.
2. Select the user that you want to modify and click the Password toolbar button.
The Change User Password dialog opens.
3. Enter the old password, the new password, and then re-enter the new password.
4. Click OK.
The user's password is changed.

Assign a User to a Group Using the User Profile Utility

To assign a user to a group

1. Select User Profile from the Utilities menu on the CA ARCserve Backup Manager Home Page.
The Profile Manager opens.
2. Select user that you want to modify and click the Assign Group toolbar button.
The Assign Groups dialog opens.
3. Select the group to which you want to assign this user and click OK.

How to Process Computer Name Changes in an ARCserve Domain

The computer name is a name that your computer uses to identify itself in a network or a domain. In a centralized management environment, an ARCserve domain can consist of a primary server and one or more member servers, or a stand-alone server. You establish the names of the ARCserve domain, the computer name of the primary server, and the computer names of the member servers when you install CA ARCserve Backup.

CA ARCserve Backup uses the computer names of the primary server and the member servers to establish communication between the servers. CA ARCserve Backup specifies the computer name of the primary server in the Discovery.cfg configuration file. The Discovery.cfg configuration file resides on the primary server and the member servers.

Note: The ARCserve domain name and the computer name of the primary server can be different. However, both names must not exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.

When you change the computer name of the primary server or the member servers, the servers cannot communicate with each other in the ARCserve domain.

In an ARCserve domain, the following scenarios exist when you change the computer name of an ARCserve server:

- The computer name of the primary server in an ARCserve domain was changed.

To ensure that the primary server and the member servers can communicate, see [Change the Computer Name of the Primary Server on the Primary Server](#) (see page 495), and [Change the Computer Name of the Primary Server on a Member Server](#) (see page 500).
- The computer name of a member server in an ARCserve domain was changed.

To ensure that the member server can communicate in the ARCserve domain, see [Change the Computer Name on a Member Server](#) (see page 502).
- The computer name of a stand-alone server was changed.

To ensure that a stand-alone server can communicate in an ARCserve domain, see [Change the Computer Name on a Stand-alone Server](#) (see page 504).
- The computer name of a server that is running the Manager Console was changed.

To ensure that a server that is running the Manager Console can communicate in an ARCserve domain, see [Change the Computer Name on a Server that is Running the Manager Console](#) (see page 504).

More information:

[Discovery.cfg Configuration File](#) (see page 502)

Change the Computer Name of the Primary Server on the Primary Server

The following procedure ensures that the primary server and member servers in an ARCserve domain can communicate after you change the computer name of the primary server.

You must change the computer name of the primary server before you complete these steps.

Note: You can use this procedure when you change the computer name of a stand-alone server.

If you are using only Microsoft SQL Server 2005 Express for CA ARCserve Backup without any other SQL instance installed, you may also need to:

- Install Microsoft SQL Server Management Studio Express (SSMSE) onto this machine, if it is not already installed. SSMSE is a graphical tool for managing SQL Server 2005 Express Edition, and for managing instances of the SQL Server Database Engine created by any edition of SQL Server 2005. For more information, see Microsoft SQL Server Management Studio Express on the Microsoft Download Center website.
- Be familiar with the sqlcmd utility, which is used to enter Transact-SQL statements, system procedures, and script files at the command prompt. For more information, see sqlcmd Utility on the Microsoft Developer Network website.

For more information about renaming systems hosting Microsoft SQL Server databases, see the following topics on the Microsoft Developer Network website:

- How to Rename a Computer that Hosts a Stand-Alone Instance of SQL Server 2005.
- How to Rename a SQL Server 2005 Virtual Server.
- Installing SQL Server (SQL Server 2000) Renaming a Server.

To change the computer name of the primary server on the primary server

1. Restart the target system to complete the Windows computer name change process.

2. Log in to the primary server.

Note: Do not open the Manager Console or log in to CA ARCserve Backup.

3. Open the Windows Command Line and change the directory to the following directory:

%ARCSERVE_HOME%

Execute the following command, to stop all ARCserve services:

```
cstop
```

All ARCserve services stop.

Note: Do not close the Windows Command Line.

4. Using a text editing application, such as Notepad, open the discovery.cfg configuration file located in the following directory on the primary server:

%ARCSERVE_HOME%\config\discovery.cfg

In the PRIMARY field, change the name of the primary server as required for your environment.

Important! Do not modify the ARCserve Domain Name in the discovery.cfg configuration file. When you change the ARCserve Domain Name in the discovery.cfg configuration file, the password for the caroot account is deleted. Use the discovery.cfg configuration file only for the purposes of changing the host name of the primary server, a member server, and a stand-alone server.

Close the file and save your changes.

For more information, see [Discovery.cfg Configuration File](#) (see page 502).

5. From the Windows Command Line that you opened earlier, execute the following command to start all ARCserve services:

```
cstart
```

All ARCserve services start.

Note: Do not close the Windows Command Line.

6. From the Windows Start menu, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens and the Select Options dialog appears.

7. From the Select Options dialog, click the Select Database option, and click Next.

The Check caroot dialog opens.

8. Click Next.

Important! You must specify the caroot password to complete this task.

The System Account dialog opens.

9. Complete the following fields on the System Account dialog and click Next.

- **User Name**--Specify the Windows user name required to log in to the primary server.
- **Domain**--Specify the Windows domain name or host name of the new primary server.
- **Password**--Specify the password for the Windows user name required to log in to the primary server.

10. From the Select Database Options dialog, complete the fields and follow the prompts, as required, for your current database installation and click Next.

Note: The subsequent dialogs that open will vary, based on whether you are running Microsoft SQL Server or Microsoft SQL Server 2005 Express in your current environment.

Important! The Server Configuration Wizard prompts you to overwrite the existing ARCserve_DB instance, and, by default, the option is enabled. To retain your previous data, such as job history, activity logs, and so on, you must clear the check mark from the Overwrite the existing "ARCserve_DB" instance option.

11. After the Server Configuration Wizard completes the updates, click Finish.

12. From the Windows Command Line that you opened earlier, execute the following commands to stop and restart all ARCserve services:

```
cstop  
cstart
```

All ARCserve services stop and restart. The primary server functions using the new computer name.

Note: Do not close the Windows Command Line.

13. You must now create equivalence for the caroot user account.

From the Windows Command Line, execute the ca_auth command using the following syntax:

Note: Do not include angle brackets <> with your arguments.

```
ca_auth -cahost <new primary server host name> -equiv add <user name> <new  
primary server host name> caroot caroot <password>
```

Equivalence is applied to the caroot user account.

14. If your ARCserve domain consists of member servers, complete the steps in [Change the Computer Name of the Primary Server on a Member Server](#) (see page 500).

15. If you are running Microsoft SQL Server 2005 Express as the CA ARCserve Backup database, note that SQL Express is installed as a named instance. As described in Microsoft document MS143799, execute the following commands using SSMSE to link the named instance to the new computer name:

```
sp_dropserver <old_name\instancename>  
GO  
sp_addserver <new_name\instancename>,local  
GO
```

Restart the SQL Server instance.

16. Run the Microsoft SQL Agent Account Configuration utility to update the ODBC communication settings if any of the following conditions are met:
- The server is the primary server with a locally installed CA ARCserve Backup database,
 - The server is a standalone server with a locally installed CA ARCserve Backup database,
 - The server is the primary server, a standalone server, or a member server AND CA ARCserve Backup database or the Agent for Microsoft SQL Server is installed on the same machine.

To start the Microsoft SQL Agent Account Configuration utility, click Start from the Windows Taskbar, choose All Programs, CA, ARCserve Backup, and Microsoft SQL Agent Account Configuration.

After you start the utility, follow the prompts and accept all settings.

17. Verify the renaming operation.

To verify the renaming operation has successfully completed, select information from either @@servername or sys.servers. The @@servername function returns the new name, and sys.servers table shows the new name.

Note: After a computer has been renamed, any connections that used the old computer name must connect using the new name.

18. Release all CA ARCserve Backup licenses registered to the former primary server.

Note: For more information, see [Release Licenses from Servers](#) (see page 483).

19. Update the CA ARCserve Backup System account. To do this, open the CA ARCserve Backup Manager Console and then open the Server Admin Manager.

Select the CA ARCserve Backup server and click CA ARCserve Backup System Account as illustrated by the following:



The CA ARCserve Backup System Account dialog opens.

20. Complete the fields that follow:

- Microsoft Windows User Account
- Password
- Microsoft Windows Domain

Click OK.

21. Open the Job Status Manager and complete the following tasks:

- Delete and re-create the Database Pruning Job.

Note: For more information, see [Deleted CA ARCserve Backup Database Pruning Jobs](#) (see page 309).

- Modify the Database Protection Job and any other backup jobs that are set to run on the renamed server, to update the Staging and Destination locations.

Note: For more information, see [Modify or Create a Custom Database Protection Job](#) (see page 562).

22. Perform a full backup of the CA ARCserve Backup database.

More information:

[Manage ARCserve Servers Using the Server Configuration Wizard](#) (see page 509)

Change the Computer Name of the Primary Server on a Member Server

The following procedure ensures that the primary server and member servers in an ARCserve domain can communicate after you change the computer name of the primary server.

Be aware of the following considerations:

- You must change the computer name of the primary server before you complete this task.

Note: For more information, see [Change the Computer Name of the Primary Server on the Primary Server](#) (see page 495).

- You must complete this task on all member servers in the ARCserve domain.
- The Server Configuration Wizard may display the following messages while you are completing this task:
 - CA ARCserve Backup is unable to connect to the original primary server. You can safely click Continue to clear this message.
 - CA ARCserve Backup is unable to unregister the member server. You can safely click Yes to clear this message.

To change the computer name of the primary server on a member server

1. Log in to the member server.

Note: You do not need to start CA ARCserve Backup to complete this task.

2. From the Windows Start menu on the member server, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

3. From the Select Options dialog, click Move this server to another CA ARCserve Backup domain and click Next.

The Check caroot dialog opens.

4. Specify the password for the caroot account and click Next.

5. In the Add to another CA ARCserve Backup domain dialog, specify the new hostname for the primary server, specify the password for the caroot account and click Next.

The System Account dialog opens.

6. In the System Account dialog, complete the following fields:

User Name

Lets you specify the Windows user name that is required to log in to the primary server.

Domain

Lets you specify the Windows domain name or host name of the new primary server.

Password

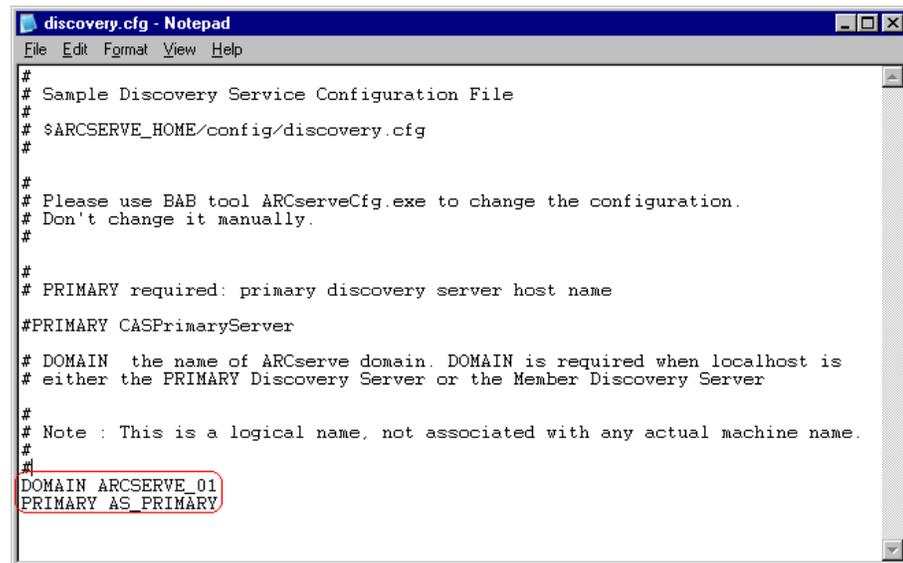
Lets you specify the password for the Windows user name that is required to log in to the primary server.

Click Next and follow the on-screen instructions to complete the configuration.

7. Repeat Steps 1 through 6 for all member servers in the ARCserve domain.

Discovery.cfg Configuration File

The discovery.cfg configuration file specifies the name of the ARCserve domain and the computer name of the primary server, as illustrated by the following example:



```
discovery.cfg - Notepad
File Edit Format View Help
#
# Sample Discovery Service Configuration File
#
# $ARCSERVE_HOME/config/discovery.cfg
#
#
# Please use BAB tool ARCserveCfg.exe to change the configuration.
# Don't change it manually.
#
#
# PRIMARY required: primary discovery server host name
#PRIMARY CASPrimaryServer
#
# DOMAIN the name of ARCserve domain. DOMAIN is required when localhost is
# either the PRIMARY Discovery Server or the Member Discovery Server
#
# Note : This is a logical name, not associated with any actual machine name.
#
#
DOMAIN ARCSERVE_01
PRIMARY AS_PRIMARY
```

The discovery.cfg configuration file is located in the following directory on the primary and member servers:

```
%ARCSERVE_HOME%\config\discovery.cfg
```

Important! Do not modify the ARCserve Domain Name in the discovery.cfg configuration file. When you change the ARCserve Domain Name in the discovery.cfg configuration file, the password for the caroot account is deleted. Use the discovery.cfg configuration file only for the purposes of changing the host name of the primary server, a member server, and a stand-alone server.

Change the Computer Name of a Member Server

The following procedure ensures that the member servers in an ARCserve domain can communicate with the primary server after you change the computer name of the member server.

You must change the computer name of the member server before you complete this procedure.

To change the computer name of a member server

1. Log in to the member server.

Note: Do not open the Manager Console or log in to CA ARCserve Backup.

2. Open the Windows Command Line and change the directory to the following directory:

```
%ARCSERVE_HOME%
```

Execute the following commands, to stop and start all ARCserve services:

```
cstop  
cstart
```

All ARCserve services stop and restart.

Note: Do not close the Windows Command Line.

3. From the Windows Start menu, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens and the Select Options dialog appears.

4. Click the Move this server to another CA ARCserve Backup domain option and click Next.

The Add to Another CA ARCserve Backup Domain dialog opens.

5. On the Add to Another CA ARCserve Backup Domain dialog, complete the following fields and click Next.

- **Primary Server Name**--Specify the name of the primary server.

- **Password**--Specify the password for the caroot user account.

The System Account dialog opens.

6. Complete the following fields on the System Account dialog and click Next.

- **User Name**--Specify the Windows user name required to log in to the member server.

- **Domain**--Specify the Windows domain name name or host name of the new member server.

- **Password**--Specify the password for the Windows user name required to log in to the member server.

The CA ARCserve Backup Data Migration dialog opens.

7. On the CA ARCserve Backup Data Migration dialog, click Next.

The Migrate Server Data Dialog opens.

8. On the Migrate Server Data Dialog, click Start.

The Complete dialog opens after the data migration process starts and completes.

9. On the Complete dialog, click Next, and then click Finish.
10. To verify the changes, open the Manager Console, open the Backup Manager, and select the Source tab.

Expand the Windows Systems object in the Source directory tree.

The member server, with its new host name, appears under the Windows Systems object.

More information:

[Manage ARCserve Servers Using the Server Configuration Wizard](#) (see page 509)

Change the Computer Name of a Stand-alone Server

A stand-alone server is an ARCserve server that resides in an ARCserve domain that does not manage member servers.

The procedure to change the computer name of a stand-alone server is identical to that of changing the computer name of a primary server.

Note: For more information, see [Change the Computer Name of the Primary Server on the Primary Server](#) (see page 495).

Change the Computer Name of a Server that is Running the Manager Console

When you change the computer name of a server that is running the Manager Console, you do not need to process modifications to the primary server, a stand-alone server, a member server, or the server that is running the Manage Console.

Re-initialize the CA ARCserve Backup Database

The following procedure describes how to re-initialize the CA ARCserve Backup database. The CA ARCserve Backup database may not initialize under the following scenarios:

- The CA ARCserve Backup database could not be recovered from a disaster using the `ca_recoverdb` command.
- The CA ARCserve Backup database could not be started for various reasons.

When you execute this procedure, the Server Configuration Wizard overwrites the existing CA ARCserve Backup database instance, which allows you to re-initialize the CA ARCserve Backup database.

Important! The re-initialization process overwrites your CA ARCserve Backup database and you will lose backup data. Ensure that the CA ARCserve Backup database is corrupt before you complete this task.

You can perform this task with Microsoft SQL Server databases and Microsoft SQL Server 2005 Express Edition databases.

To re-initialize the CA ARCserve Backup database

1. From the CA ARCserve Backup primary or stand-alone server, start the Server Configuration Wizard.

Note: To start the Server Configuration Wizard, click Start, point to All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens with the Select Options dialog.

2. Choose Select Database and click Next.

The Check caroot dialog opens.

3. Specify the caroot password and click Next.

The System Account dialog opens.

4. Specify the system account information and click Next.

The Select Database dialog opens.

5. In the Select Database dialog, accept the default options and click Next.

A message appears warning you that certain information will not be migrated.

6. Click OK to clear the message.

7. Do one of the following:

- If the CA ARCserve Backup database is a Microsoft SQL Server 2005 Express Edition database, continue to the next step.
- If the CA ARCserve Backup database is a Microsoft SQL Server database, the SQL Database System Account dialog opens. Accept the default options on the SQL Database System Account dialog and click Next.

8. In the Select database installation path dialog, ensure that the Overwrite DB option is enabled.

Note: Enabling this option is essential for re-initializing the database.

Click Next.

The CA ARCserve Backup database is re-initialized.

9. Click Finish when database re-initialization process is complete.

Restore the CA ARCserve Backup Job Queue

You can protect the Job Queue by backing it up using the following methods:

- Back up the Job Queue using the Database Protection Job.
- Back up the CA ARCserve Backup primary server or stand-alone server and include the directory that contains the CA ARCserve Backup database with the backup.
- Back up data and specify the Job Scripts option on the Operations section of the Global Options dialog.

In all of these methods, the Job Queue is one of the last few objects backed up during the job. If you used the Database Protection Job, or included the CA ARCserve Backup database in the same backup job, the CA ARCserve Backup database and Job Queue will reside on the same backup media, and the Job Queue sessions will be between one and six sessions before the CA ARCserve Backup database.

In the event the CA ARCserve Backup Job Queue is damaged or is deleted in error, use the following steps to restore the Job Queue to the last backup.

To restore the CA ARCserve Backup Job Queue

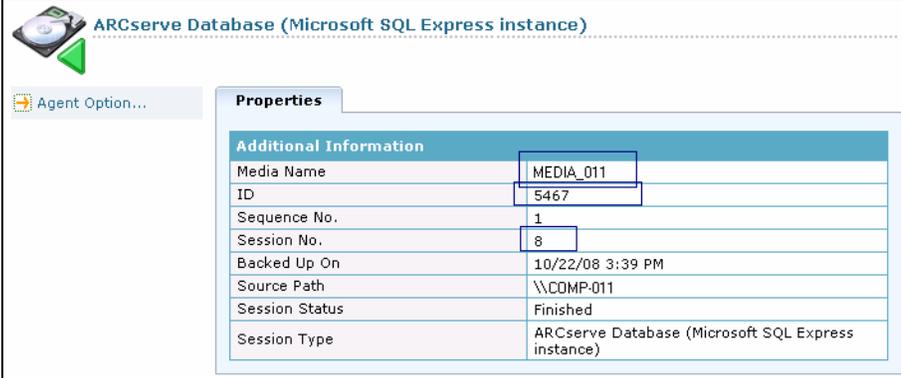
1. Ensure that there are no jobs running on any CA ARCserve Backup server in the affected CA ARCserve Backup domain.

- Open the Restore Manager and select Restore by Tree from the methods drop-down list.

Expand the Windows Systems object and locate the CA ARCserve Backup server, or the remote server where the CA ARCserve Backup database is located.

Expand the CA ARCserve Backup server, locate and click the CA ARCserve Backup database.

From Properties on the Restore Manager window, locate and notate the Media Name, the ID, and the Session Number for the CA ARCserve Backup database.



Additional Information	
Media Name	MEDIA_011
ID	5467
Sequence No.	1
Session No.	8
Backed Up On	10/22/08 3:39 PM
Source Path	\\COMP-011
Session Status	Finished
Session Type	ARCserve Database (Microsoft SQL Express instance)

Select Restore by Session from the restore methods drop-down list.

The Session directory tree opens.

- From the Session directory tree, locate and expand the Backup Media containing the CA ARCserve Backup database backup data.

Locate the session that contains the CA ARCserve Backup database, and start searching upward from there. The session path of the Job Queue backup session will end in 00000001.QSD, and the Session Type will be ARCserve Job Queue. Locate the session that contains the Job Queue backup session, as illustrated below.



<input checked="" type="checkbox"/>	Session 000000005 : \\COMP_011 {C:\Program Files\CA\ARCserve Backup\00000001.QSD}
<input type="checkbox"/>	Session 000000006 : \\COMP_011 {C:\Program Files\CA\ARCserve Backup\CATALOG.DB}
<input type="checkbox"/>	Session 000000007 : \\COMP_011 {sqlldr@ARCserve_DB}
<input type="checkbox"/>	Session 000000008 : \\COMP_011 {dbasql@ARCserve_DB}

Click the check box next to the session containing the Job Queue backup session.

- Click the Destination tab.

5. Clear the check mark next to Restore files to their original location, and specify an alternate location to restore the Job Queue backup session.

Note: The Client Agent for Windows must be installed on the system containing the alternate location and the alternate location must be an empty directory (For example, C:\Temp). The best practice is to specify directory on the CA ARCserve Backup primary or stand-alone server.

Submit the job.

6. Closed the Restore Manager window.
7. After the restore job is complete, open the Server Admin and stop all CA ARCserve Backup services by doing the following:
 - a. Locate and select the primary server or stand-alone server.
 - b. Right-click the CA ARCserve Backup server and select Stop All Services from the pop-up menu.

All services stop on the primary or stand-alone server.

8. Browse to directory where you restored the Job Queue backup session.

Copy all Job Queue files under the folder that you restored to the following directory:

ARCserve_HOME\00000001.qsd

Note: <ARCserve_HOME> represents the directory where you installed CA ARCserve Backup. By default, CA ARCserve Backup is installed in the directory that follows:

C:\Program Files\CA\ARCserve Backup

9. Open the Server Admin and restart all CA ARCserve Backup services by doing the following:
 - a. Locate and select the primary server or stand-alone server.
 - b. Right-click the CA ARCserve Backup up server and select Start All Services from the pop-up menu.

All CA ARCserve Backup services restart on the primary or stand-alone server.

Open the Job Queue Manager and you will see that the job queue has been restored to its original form. The CA ARCserve Backup Job Queue is restored, and you can resume normal operation.

Manage ARCserve Servers Using the Server Configuration Wizard

The Server Configuration Wizard lets you manage how CA ARCserve Backup servers function. Using the Server Configuration Wizard, you can perform the following tasks:

- Manage the roles of the servers in your CA ARCserve Backup domain. For example, you can:
 - Promote a CA ARCserve Backup member server to a CA ARCserve Backup primary server.
 - Demote a CA ARCserve Backup primary server to a CA ARCserve Backup member server.
 - Allow a member server to separate from one CA ARCserve Backup domain and join a different CA ARCserve Backup domain.

- Select the application that you want to use to manage the CA ARCserve Backup database.

For Microsoft SQL Server 2005 Express installations, the database must be installed on the primary server. If you require remote database communication, you must use Microsoft SQL Server to host the ARCserve database.

- Move the CA ARCserve Backup database to other systems or use a different SQL Server database instance in your environment.
- Repair the ARCserve database connection to a primary server and member servers.

- Register a member server with a CA ARCserve Backup domain primary server.

To register a member server with a domain primary server, you must provide valid credentials (for example, the user name and password). After CA ARCserve Backup authenticates your credentials, the member server is registered into the CA ARCserve Backup database.

CA ARCserve Backup lets you register the member server with the CA ARCserve Backup primary server when you install CA ARCserve Backup. If the registration process fails when you are installing CA ARCserve Backup, Setup displays messages to notify you that an error occurred.

- Specify the CA ARCserve Backup Domain Administrator (caroot) password on a primary server.
- Correct installation failures.

When you install CA ARCserve Backup, the installation process can fail under the following scenarios:

- CA ARCserve Backup cannot communicate or authenticate properly with the CA ARCserve Backup database.
- CA ARCserve Backup cannot authenticate the caroot account or a system account.

If a database communication error or user authentication error occurs, the installation wizard displays an error message. To remedy the problem, run the Server Configuration Wizard.

More information:

[Tasks You Can Perform Using the Server Configuration Wizard](#) (see page 511)
[Start the Server Configuration Wizard](#) (see page 514)

Tasks You Can Perform Using the Server Configuration Wizard

Using the Server Configuration Wizard you can perform the following tasks:

Primary Server and Stand-alone Server Tasks

You can perform the following tasks on primary and stand-alone servers:

- Modify the CA ARCserve Backup Domain Administrator (caroot) account password.

The caroot account password lets you log in to the CA ARCserve Backup Manager Console to perform administrative tasks.

- Specify the application that you want to use to host the CA ARCserve Backup database.

You can specify Microsoft SQL Server 2005 Express or Microsoft SQL Server as the ARCserve database application. SQL Server 2005 Express must be installed locally to the CA ARCserve Backup primary server. SQL Server can be installed locally or remotely to the CA ARCserve Backup primary server.

- Move the CA ARCserve Backup database to a different system, instance, or both.
- Repair database connections with member servers.
- Re-initialize the CA ARCserve Backup database.
- Specify SQL Server collation to ensure that you can search and sort backup data that contains Unicode-based characters.
- Correct installation failures.
- Demote a primary server to a member server.

Important! CA ARCserve Backup does not support migrating CA ARCserve Backup database information from multiple CA ARCserve Backup domains into a single CA ARCserve Backup domain. Although you can demote a primary server and allow it to join a different CA ARCserve Backup domain, joining a different domain will result in the loss of the backup job history from the demoted primary server, and you will not be able to view media and session details in the Restore Manager on the demoted server.

Note: For more information, see [Data Migration Limitations in an ARCserve Domain](#) (see page 512).

Member Server Tasks

You can perform the following tasks on member servers:

- Assign the member server to a different CA ARCserve Backup domain.
- Promote a member server to a primary server or stand-alone server.

Note: To enable central management capabilities, you must install the Central Management Option on the new primary server after the promotion process is complete.

- Repair the database connection.
- Correct installation failures.

Note: Use the Server Admin to modify the CA ARCserve Backup System Account on a primary server and a member server (for example, user name, password, and so on). For more information, see [Change or Modify the CA ARCserve Backup System Account](#) (see page 478).

Data Migration Limitations in a CA ARCserve Backup Domain

The Server Configuration Wizard lets you define the roles of the servers in an ARCserve domain and specify the application that you want to use to host the ARCserve database instance.

CA ARCserve Backup lets you migrate ARCserve database instance data as described by the following scenarios.

Scenario 1:

You exchange the roles of the primary server and a member server in an ARCserve domain. You can successfully migrate data under the following conditions:

- The original primary server hosted the ARCserve database instance using Microsoft SQL Server 2005 Express Edition and new primary server is hosting the ARCserve database instance using Microsoft SQL Server 2005 Express Edition.
- The original primary server hosted the ARCserve database instance using Microsoft SQL Server and new primary server is hosting the ARCserve database instance using Microsoft SQL Server.

Important! CA ARCserve Backup does not support data migration when the original primary server hosted the ARCserve database with Microsoft SQL Server and the new primary is hosting the ARCserve database with Microsoft SQL Server 2005 Express Edition.

To accomplish a successful data migration, you must complete the following steps:

1. From the primary server that you want to demote, back up the ARCserve database using the Database Protection Job.
Note: Allow the Database Protection Job to finish before continuing.
2. Promote the member server to a primary server.
3. Demote the original primary server and allow it to join new primary server's domain.
4. From the [Agent Restore Options dialog](#) (see page 576) on the new primary server, specify the following options:
 - Use current ASDB as original location.
 - Preserve current ARCserve domain memberships.
5. Restore the original ARCserve database to the new primary server.

Scenario 2:

You modify the application hosting the ARCserve database from Microsoft SQL Server 2005 Express Edition to Microsoft SQL Server.

Note: This scenario applies to ARCserve primary server and ARCserve stand-alone server installations.

To accomplish a successful data migration, you must complete the following steps.

1. Run the [Server Configuration Wizard](#) (see page 514) on the primary or stand-alone server and specify the Select database option.
After the database modification and configuration process is complete, the Server Configuration Wizard prompts you to migrate the data from the old database instance to the new database instance.
2. Migrate the data from the Microsoft SQL Server 2005 Express Edition instance to the Microsoft SQL Server instance.

Scenario 3:

You exchange the roles of the primary server and a member server in an ARCserve domain. The original primary server hosted the ARCserve database instance using Microsoft SQL Server 2005 Express Edition and new primary server is hosting the ARCserve database instance using Microsoft SQL Server.

Note: In this scenario you must convert the ARCserve database from a Microsoft SQL Server 2005 Express Edition instance to a Microsoft SQL Server instance on the primary server that you want to demote before you back up the ARCserve database instance.

To accomplish a successful data migration, you must complete the following steps:

1. Run the Server Configuration Wizard on the primary server and specify the Select database option.

After the database modification and configuration process is complete, the Server Configuration Wizard prompts you to migrate the data from the old database instance to the new database instance.

2. Migrate the data from the Microsoft SQL Server 2005 Express Edition instance to the Microsoft SQL Server instance.
3. From the primary server that you want to demote, back up the ARCserve database using the Database Protection Job.

Note: Allow the Database Protection Job to finish before continuing.

4. Promote the member server to a primary server.
5. Demote the original primary server and allow it to join new primary server's domain.
6. From the [Agent Restore Options dialog](#) (see page 576) on the new primary server, specify the following options:
 - Use current ASDB as original location.
 - Preserve current ARCserve domain memberships.
7. Restore the original ARCserve database to the new primary server.

Start the Server Configuration Wizard

The Server Configuration Wizard lets you manage how CA ARCserve Backup servers function.

To start the Server Configuration Wizard

1. From the Windows Start menu, select Programs (or All Programs), CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

2. Select the task that you want to perform, click Next, and follow the on-screen procedures to complete your configurations.

Promote a Member Server to a Primary Server

Using the Server Configuration Wizard, you can promote a CA ARCserve Backup member server to a CA ARCserve Backup primary server.

Before you promote a member server to a primary server, the following considerations apply:

- All jobs must be stopped on the member server before the upgrade process starts. 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.
- During the upgrade process, you will be prompted to specify a CA ARCserve Backup database application. You can specify Microsoft SQL Server 2005 Express Edition or Microsoft SQL Server.

Microsoft SQL Server 2005 Express Installations

- You must install the database local to the primary server.

Microsoft SQL Server Installations

- You can install the CA ARCserve Backup database local or remote to the primary server.
- Microsoft SQL Server does not support local installations when CA ARCserve Backup is installed in NEC CLUSTERPRO environments.
- For remote Microsoft SQL Server database installations, the primary server must have a system account that properly authenticates with SQL Server and communicates via ODBC before you start the upgrade process.

To specify ODBC communication, do the following:

1. Open the Windows Control Panel, select Administrative Tools, Data Sources (ODBC), and System DSN.
2. Add a System Data Source labeled as follows:
Name: ASNT
Server: MachineName\InstanceName
3. Follow the on-screen instructions to test and complete the configuration.

- To enable central management capabilities, you must install the Central Management Option on the new primary server after the promotion process is complete.
 - **Note:** Use the Server Admin to install CA ARCserve Backup options, such as the Central Management Option, on the new primary server after the promotion process is complete. For more information, see [Install and Uninstall CA ARCserve Backup Server Based Options](#) (see page 527).

Promote a member server to a primary server

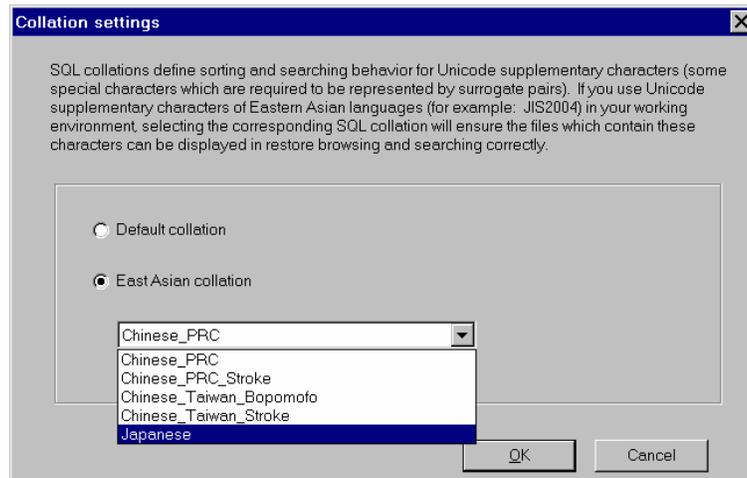
1. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

2. Click the **Promote this server to primary server** option and then click **Next**.
3. Follow the on-screen instructions to complete the configuration.

Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that you can search and sort the data. To do this, click Language Support Options on the SQL Server Express Instance dialog and follow the on-screen instructions to complete the configuration.

If you are hosting the CA ARCserve Backup database with Microsoft SQL Server, you click Language Support Options on the Select Database Installation Path dialog.)



After the configuration is complete, you must install the CA ARCserve Backup database protection agent on the system hosting the CA ARCserve Backup database.

4. To install the ARCserve database protection agent, do one of the following:
 - If the SQL Server database is installed on the CA ARCserve Backup primary server, open Windows Explorer and browse to the following directory:
C:\Program Files\CA\ARCserve Backup\Packages\ASDBSQLAgent
 - If the SQL server database is not installed on the CA ARCserve Backup primary server, open Windows Explorer and browse to the following directory:
C:\Program Files\CA\ARCserve Backup\Packages\ASDBSQLAgent
Copy the contents of the ASDBSQLAgent directory to any location on the system hosting the SQL Server database installation.
5. In the ASDBSQLAgent directory, double-click the following file:
SQLAgentRmtInst.exe
The **ARCserve Backup Agent for SQL Setup** dialog appears.
6. Complete the following fields, as required, for your installation:
 - SQL Instance Name
Specify the name of the SQL instance that you want to protect.
 - Auth Mode
Specify the authentication mode that the agent will use to communicate with and protect the ARCserve database.
If you specify SQL Authentication as the authentication mode, complete the following fields:
 - SQL SA Name
Specify the SQL system account name.
 - SQL SA Password
Specify the SQL system account password.
7. Click **Install** and follow the on-screen instructions to complete the installation.

Demote a Primary Server or Stand-alone Server to a Member Server

Using the Server Configuration Wizard you can demote a CA ARCserve Backup primary server and a CA ARCserve Backup stand-alone server to a CA ARCserve Backup member server.

Before you demote a primary server to a member server, the following considerations apply:

- All jobs must be stopped on the primary server before the demotion process starts. 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 demotion process pauses until all jobs in progress are complete.
- You must specify CA ARCserve Backup authentication credentials to allow the demoted primary server to join the domain of another primary server (for example, *caroot* and your CA ARCserve Backup password). The process of allowing a member server to join a CA ARCserve Backup domain does not support using Windows authentication.
- If the primary server contains member server relationships, the Server Configuration Wizard presents you with list of member servers that the primary server is managing server and the following options:
 - Demote the primary server.
 - Demote the primary server and allow the member servers it is managing to join the new domain.

Note: If the primary server is managing member servers, the best practice is to promote the members servers or move them to a different domain before you demote the primary server.

- If the demoted primary server is joining a CA ARCserve Backup domain that is running a remote Microsoft SQL Server database installation, and the primary server communicates with the SQL Server database using Windows authentication, the new member server must have a system account that uses Windows authentication and communicates via ODBC before you start the demotion process.

- All registered licenses will be removed from the demoted primary server.
- If you set up jobs using a different caroot user account before the demotion, you must manage the migrated jobs on the primary server in the domain that the new member server joins using the original caroot account and password as the job owner for all migrated jobs.
- The table that follows describes database migration scenarios and the type of data that CA ARCserve Backup migrates from the demoted primary server to the domain that the new member server (demoted primary server) joins:

Database on Demoted Primary Server	Database on New Primary Server	Database Data Migrates?	Job and Job History Data Migrates?	Authentication Data Migrates?
Microsoft SQL Server	Microsoft SQL Server Express Edition	No	No	No
Microsoft SQL Server Express Edition	Microsoft SQL Server Express Edition	No	No	No
Microsoft SQL Server	Microsoft SQL Server	Yes	Yes Note: If you set up jobs using a different caroot user account before the demotion, you must manage the migrated jobs on the primary server in the domain that the new member server joins using the original caroot account and password as the job owner for all migrated jobs.	No
Microsoft SQL Server Express Edition	Microsoft SQL Server	Yes	Yes Note: If you set up jobs using a different caroot user account before the	No

Database on Demoted Primary Server	Database on New Primary Server	Database Data Migrates?	Job and Job History Data Migrates?	Authentication Data Migrates?
			<p>demotion, you must manage the migrated jobs on the primary server in the domain that the new member server joins using the original caroot account and password as the job owner for all migrated jobs.</p>	

To demote a primary server or stand-alone server to a member server

1. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.
The Server Configuration Wizard opens.
2. Click Demote this server to member server and then click Next.
3. Follow the on-screen instructions to complete the configuration.
4. (Optional) After the configuration is complete, you can uninstall the ARCserve database protection agent from the server that you demoted by doing the following:
 - From the Windows Control Panel, open Add and Remove Programs.
 - Browse to and select CA ARCserve Backup Agent for Microsoft SQL.
 - Click the Remove button to uninstall the agent.

The Uninstall Agent message box appears.

5. Select the Agent for ARCserve Database option and click OK.
Follow the on-screen instructions to complete the uninstallation.
6. (Optional) To move the CA licenses from the demoted primary server to a different CA ARCserve Backup primary server, do the following:
 - a. On the demoted primary server, locate the file labeled ca.olf in the following directory:
`c:\program files\ca\SharedComponents\ca_lic`
 - b. Save ca.olf as ca.old.
 - c. Copy ca.old from the demoted primary server to the following directory on the other primary server:
`c:\program files\ca\SharedComponents\ca_lic`
 - d. On the other CA ARCserve Backup Primary server, open a Command Line window and open the following utility.
`c:\program files\ca\SharedComponents\ca_lic\mergeolf.exe`
For more information about using the MergeOLF command, see the *Command Line Reference Guide*.
7. Restart the primary server in the domain that the member server (demoted primary server or stand-alone server) joined. This step helps to ensure that the information about backup data associated with the member server is accurate on the primary server.

Note: If you need to uninstall CA ARCserve Backup options on the new member server, you can uninstall them using the Server Admin. For more information, see [Install and Uninstall CA ARCserve Backup Server Based Options](#) (see page 527).

Important! The Database Protection Job remains with the demoted server after the demotion process is complete. To eliminate the Database Protection Job, you must delete it manually. For more information, see [Delete the CA ARCserve Backup Database Protection Job](#) (see page 572).

Move a Member Server to a Different CA ARCserve Backup Domain

Using the Server Configuration Wizard, you can move a member server to a different CA ARCserve Backup domain.

Before you move a member server to a different CA ARCserve Backup domain, the following considerations apply:

- All jobs must be stopped on the member server before the move process starts. 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 move process pauses until all jobs in progress are complete.
- After the member server joins a different CA ARCserve Backup domain, the jobs associated with the previous domain will migrate to the new domain. However, all database information relating to the member server will remain with the previous domain.

To move a member server to a different CA ARCserve Backup domain

1. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

2. Click the **Move this server to another CA ARCserve Backup domain** option and then click **Next**.
3. Follow the on-screen instructions to complete the configuration.

Change the Password for the CA ARCserve Backup Domain Administrator (caroot) Account

Using the Server Configuration Wizard, you can change the password for the CA ARCserve Backup Domain Administrator (caroot) account. The Domain Administrator account lets you log in to the CA ARCserve Backup Manager Console to perform administrative tasks.

Before you change the password for the CA ARCserve Backup system account, you must be logged in to a CA ARCserve Backup primary server.

Note: Use the Server Admin to change the password to the system account on a member server. For more information, see [Change or Modify the CA ARCserve Backup System Account](#) (see page 478).

To change the password for the CA ARCserve Backup Domain Administrator (caroot) account

1. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

2. Click the **Password for Backup Server Logon and Administration** option and then click **Next**.
3. Follow the on-screen instructions to complete the configuration.

Repair the CA ARCserve Backup Configuration

Installation errors can occur when you install and upgrade CA ARCserve Backup from a previous release on a primary server or a member server. For example, an incomplete installation occurred.

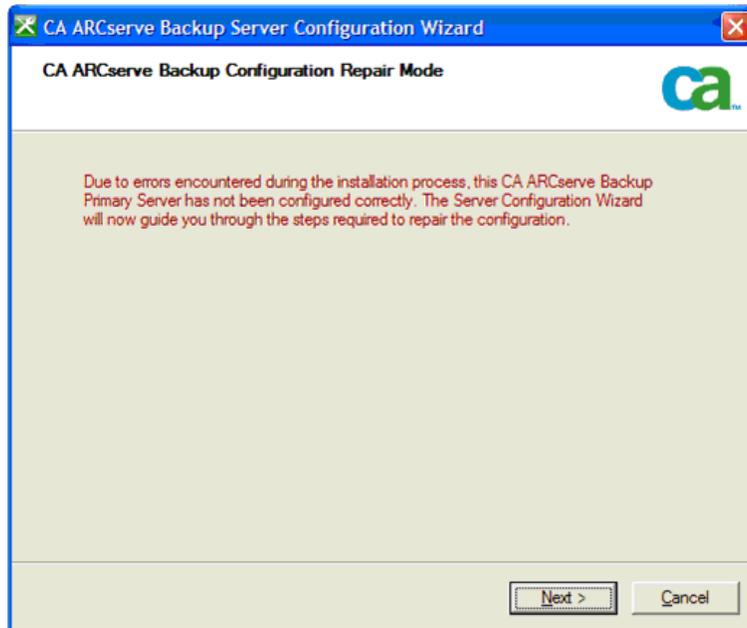
If the installation wizard detects errors, the Server Configuration Wizard prompts you to correct the installation errors.

The following procedure describes how to correct the CA ARCserve Backup configuration.

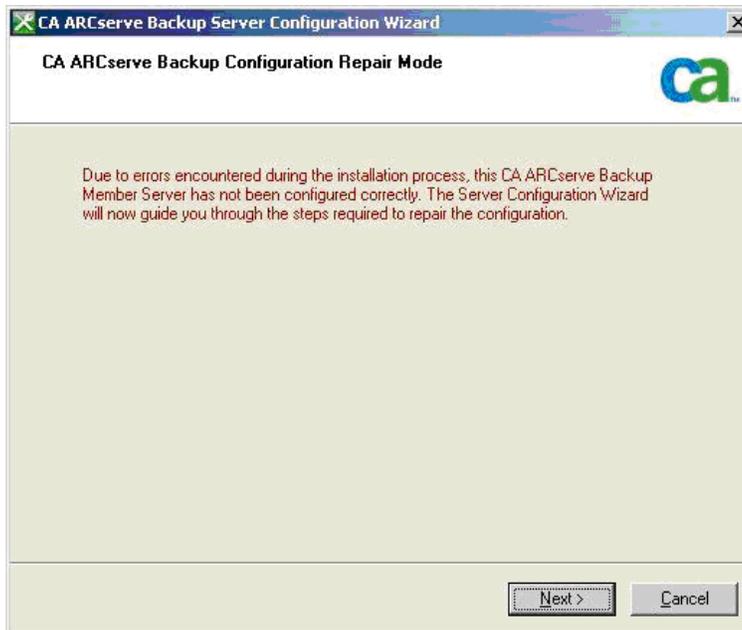
To repair the CA ARCserve Backup configuration

1. Install CA ARCserve Backup or upgrade CA ARCserve Backup from a previous release.

If the installation wizard detects installation errors with a primary server, the Repair CA ARCserve Backup Configuration dialog appears as illustrated by the following screen:



If the installation wizard detects installation errors with a member server, the Repair CA ARCserve Backup Configuration dialog appears as illustrated by the following screen:



2. Click Next.

The Server Configuration Wizard starts in repair mode.

Follow the prompts and complete the required fields on the subsequent dialogs to repair the CA ARCserve Backup configuration.

Repair the ARCserve Database Connection on a Primary Server

This task lets you repair Open Database Connectivity (ODBC) communication between a primary server an ARCserve database instance that is hosted with Microsoft SQL Server, and register member servers with the primary server.

The Repair database connection option is disabled on stand-alone server installations or when you are hosting the ARCserve database using Microsoft SQL Server 2005 Express Edition.

ODBC is the most efficient method for the Database Engine to communicate with a Microsoft SQL Server instance that communicates through a network. Occasionally, network communication problems, Microsoft SQL Server communication settings problems, or both, can cause the Database Engine to communicate with the ARCserve database instance using Remote Procedure Call (RPC) communication. As a result, RPC communication will adversely affect the performance of the ARCserve database.

To remedy this problem, troubleshoot and repair the communication using the SQL Server Configuration Manager and then use the Server Configuration Wizard to repair ODBC communication between the Database engine and the ARCserve database instance.

To repair the ARCserve database connection on a primary server

1. Log in to the primary or stand-alone server where CA ARCserve Backup is installed.

Note: Do not open the Manager Console.

2. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

3. Select the Repair database connection for member server(s) option and click Next.
4. Follow the prompts and complete all required fields on the subsequent dialogs to repair the database connection.

Note: When you repair the database connection on a primary server that is managing member servers, the Server Configuration Wizard attempts to repair the database connection on all member servers in the ARCserve domain.

Repair the ARCserve Database Connection on a Member Server

This task lets you repair Open Database Connectivity (ODBC) communication between a member server and an ARCserve database instance that is hosted with Microsoft SQL Server.

ODBC is the most efficient method for the Database Engine to communicate with a Microsoft SQL Server instance that communicates through a network. Occasionally, network communication problems, Microsoft SQL Server communication settings problems, or both, can cause the Database Engine to communicate with the ARCserve database instance using Remote Procedure Call (RPC) communication. As a result, RPC communication will adversely affect the performance of the ARCserve database.

To remedy this problem, troubleshoot and repair the communication using the SQL Server Configuration Manager and then use the Server Configuration Wizard to repair ODBC communication between the Database engine and the ARCserve database instance.

To repair the ARCserve database connection on a member server

1. Log in to the member server where CA ARCserve Backup is installed.

Note: Do not open the Manager Console.

2. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

3. Select the Repair database connection option and click Next.
4. Follow the prompts and complete all required fields on the subsequent dialogs to repair the database connection.

Install and Uninstall CA ARCserve Backup Server Based Options

From a primary and stand-alone CA ARCserve Backup server, you can use the Server Admin to install and uninstall the following CA ARCserve Backup options:

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

Before you install and uninstall CA ARCserve Backup server based options, the following considerations apply:

- You can install and uninstall options only on a primary or stand-alone CA ARCserve Backup server.
- The CA ARCserve Backup options that display in the Install/Uninstall Options dialog will vary depending on the type of CA ARCserve Backup server you are configuring.
- If you are installing server based options, ensure that all external devices (for example, libraries) are connected to the primary servers, member servers, and the SAN in your environment. CA ARCserve Backup automatically detects supported devices and configures them for use automatically when the tape engine starts.

You must manually configure devices that CA ARCserve Backup does not automatically detect.

To install and uninstall CA ARCserve Backup server based options

1. From the Quick Start menu in the Navigation Bar on the Home Page, click Server Admin.

The Server Admin opens.

2. Expand the domain directory tree and click the primary or stand-alone server where you want to install or uninstall options.

The domain directory tree is illustrated by the following:



3. Right-click the server where you want to install and uninstall options and select Install/Uninstall Options from the pop-up menu.

The Install/Uninstall Options dialog opens.

4. From the Product Name list on the Install/Uninstall Options dialog, place a check mark next to the options that you want to install and clear the check mark next to the options that you want to uninstall.
5. Click OK and follow the on-screen instructions to complete the installation, uninstallation, or both.

CA ARCserve Backup Agent Deployment

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

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

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

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

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

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

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

Note: For information about how to deploy agents to remote hosts using Automatic upgrade see [Deploy Agents to Remote Hosts Using Automatic Upgrade](#) (see page 532).

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

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

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

Note: For information about how to deploy agents to remote hosts using Custom deployment, see [Deploy Agents to Remote Hosts Using Custom Deployment](#) (see page 535).

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

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

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

Note: For information about how to deploy agents to remote hosts using Custom installation, see [Deploy Agents to VMs Using Virtual Machine Deployment](#) (see page 538).

Review the considerations that follow before you use Agent Deployment:

- Agent Deployment lets you deploy the CA ARCserve Backup products that follow:
 - CA ARCserve Backup Agent for Microsoft Exchange
 - CA ARCserve Backup Agent for Microsoft SQL Server
 - CA ARCserve Backup Agent for Microsoft SharePoint
 - CA ARCserve Backup Agent for Open Files
 - CA ARCserve Backup Agent for Oracle
 - CA ARCserve Backup Agent for Virtual Machines
 - CA ARCserve Backup Client Agent for Windows
 - CA ARCserve Backup Diagnostic Utilities

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

- Agent Deployment requires you to specify the host names of the target systems. CA ARCserve Backup does not support specifying IP addresses when you are deploying agents to remote systems.
- Agent Deployment installs the agents into their default installation path. For example, Agent Deployment installs or upgrades the Client Agent for Windows in the path that follows (x86 systems):

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

- You must log in to your computer with an administrative account or an account with administrative privileges to deploy agents to remote hosts.
- You should ensure that the administrative share on the remote hosts (for example, C\$, Admin\$, and so on) is accessible from the server that pushes the agents.

- You should ensure that the firewall exception rule for File and Printing Service on the remote hosts is enabled. You must complete this task on Windows Server 2008 systems because, by default, Windows Server 2008 firewall policy blocks File and Printing Service communication.
- To prevent the Windows firewall from blocking File and Print Sharing communication, you should use Domain level group policy to enable an exception to File and Print Sharing communication on all servers in your backup environment.
- You must disable simple file sharing on Windows XP systems to ensure that you can successfully install agents on remote hosts. Use the steps that follow to disable simple file sharing on remote hosts:
 1. Log in to the remote Windows XP host system.

Double-click My Computer on the desktop.

My Computer opens.
 2. Click Folder Options on the Tools menu.

The Folder Options dialog opens.
 3. Click the View tab.

Locate Use simple file sharing (recommended).

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

Simple file sharing is disabled.

Deploy Agents to Remote Hosts Using Automatic Upgrade

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

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

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

1. Open the CA ARCserve Backup Manager Console.
From the Quick Start Menu select Administration and click Agent Deployment.
CA ARCserve Backup Agent Deployment starts and the Login Server dialog opens.
2. Complete the required fields on the Login Server dialog and click Next.
The Methods dialog opens.
3. From the Methods dialog, click Automatic upgrade and click Next.
The Components dialog opens displays a list of hosts detected by Agent Deployment that are running CA ARCserve Backup agents from a previous release.
4. Click Next.
The Host Information dialog opens and populates the Hosts and Credentials list with the host names, user names, and passwords for the detected hosts.

5. Specify the User Name and Password for the hosts by doing the following:
 - a. Specify the user name in the User field (<domain>\<user name>) and specify the password in the Password field.
 - b. Ensure that the check box next to the target host is checked. To specify all hosts, click the Select all check box.

CA ARCserve Backup Agent Deployment

Host Information

Methods
Components
→ **Host Information**
Setup Summary
Installation Status
Installation Report

[Support Website](#)
[View Readme](#)

Import Host List
You can import host names from a text file. The host names must be separated by a new line delimiter in the text file.

Hosts and Credentials
New Host:

<input checked="" type="checkbox"/>	Host	UserName	Password	Status
<input checked="" type="checkbox"/>	comp-001	user-01	*****	Pending
<input checked="" type="checkbox"/>	comp-002	user-01	*****	Pending
<input checked="" type="checkbox"/>	server-001	user-01	*****	Pending
<input checked="" type="checkbox"/>	server-002	user-01	*****	Pending
<input type="checkbox"/>				

For all selected hosts:

User: Password:

< Back Next > Cancel

- c. Click Apply Credentials.

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

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

Click Next to continue.

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

Click Next.

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

The Setup Summary dialog opens.

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

Click Next.

The Installation Status dialog opens.

8. From the Installation Status dialog, click Install.

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

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

Click Next.

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

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

Click Restart.

Agent Deployment restarts all remote hosts now.

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

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

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

More information:

[CA ARCserve Backup Agent Deployment](#) (see page 528)

[Deploy Agents to Remote Hosts Using Custom Deployment](#) (see page 535)

Deploy Agents to Remote Hosts Using Custom Deployment

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

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

1. Open the CA ARCserve Backup Manager Console.
From the Quick Start Menu select Administration and click Agent Deployment.
CA ARCserve Backup Agent Deployment starts and the Login Server dialog opens.
2. Complete the required fields on the Login Server dialog and click Next.
The Methods dialogs opens.
3. From the Methods dialog, click Custom installation and click Next.
The Components dialog opens.
4. From the Components dialog, select the agents that you want to install on all remote hosts and click Next.
The Host Information dialog opens.
5. Specify the names of remote hosts by doing one of the following:
 - Click Import to import a list of remote hosts from a text file.
Note: The host names must be separated the new line delimiter. You can import multiple text files, however, the total number of remote hosts must be less than or equal to 1000.
After the host names appear in the Host column, continue to the next step.
 - Specify the remote host name in the Host Name field and click Add.
Repeat this step as necessary until all required host names appear in the Host column.
After the host names appear in the Host column, continue to the next step.
Note: You can specify up to 1000 remote hosts. To deploy agents to more than 1000 remote hosts, you can restart Agent Deployment and repeat this task, or, run Agent Deployment from an alternate CA ARCserve Backup primary server or stand-alone server.

6. Specify the user name and password for the remote hosts by doing the following:
 - a. Click the UserName field (next to the host name) and specify the user name using the following format:
`<domain>\<user name>`
 - b. Click the Password field and specify the corresponding password.
 - c. Repeat this step as required until you specify the user name and password for all remote hosts.

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

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

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

Click Next to continue.

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

Click Next.

7. After the Status field for all hosts displays Pending or Verified, click Next.
The Setup Summary dialog opens.
8. From the Setup Summary dialog, verify the components and the host names specified.

Click Next.

The Installation Status dialog opens.

9. From the Installation Status dialog, click Install.

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

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

10. Do one of the following:

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

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

Click Restart.

Continue to the next step.

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

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

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

Click Restart.

Agent Deployment restarts all remote hosts now.

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

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

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

More information:

[CA ARCserve Backup Agent Deployment](#) (see page 528)

[Deploy Agents to Remote Hosts Using Automatic Upgrade](#) (see page 532)

Deploy Agents to VMs Using Virtual Machine Deployment

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

Be aware of the considerations that follow:

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

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

1. Open the CA ARCserve Backup Manager Console.
From the Quick Start Menu select Administration and click Agent Deployment.
CA ARCserve Backup Agent Deployment starts and the Login Server dialog opens.
2. Complete the required fields on the Login Server dialog and click Next.
The Methods dialog opens.
3. From the Methods dialog, select Virtual Machine deployment and click Next.
The Components dialog opens.
4. From the Components dialog, select the agents that you want to install on all remote hosts and click Next.
The Host Information dialog opens.

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

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

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

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

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

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

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

Note: Repeat this step as necessary until all required host names appear in the Host column.

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

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

6. Specify the user name and password for the remote hosts by doing the following:
 - a. Click the UserName field (next to the host name) and specify the user name using the following format:
`<domain>\<user name>`
 - b. Click the Password field and specify the corresponding password.
 - c. Repeat this step as required until you specify the user name and password for all remote hosts.

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

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

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

Click Next to continue.

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

Click Next.

7. After the Status field for all hosts displays Pending or Verified, click Next.
The Setup Summary dialog opens.
8. From the Setup Summary dialog, verify the components and the host names specified.

Click Next.

The Installation Status dialog opens.

9. From the Installation Status dialog, click Install.
Agent Deployment installs or upgrades the CA ARCserve Backup agents on the specified hosts.
After all installations and upgrades are complete, the Installation Report dialog opens.
10. Do one of the following:
 - If there are remote hosts that require a restart, click Next.
The Restart dialog opens to identify the remote hosts that require a restart.
Click Restart.
Continue to the next step.
 - If there are no remote hosts that require a restart, click Finish to complete this task.
11. From the Restart dialog, click the check box next to the remote host that you want to restart now.
Optionally, you can click the All check box to restart all remote hosts now.
Click Restart.
Agent Deployment restarts all remote hosts now.
Note: If you want to create a list of remote hosts that require a restart, click Export Restart Report.
12. After the Status field for all remote hosts displays complete, click Finish.
The CA ARCserve Backup agents are deployed on the VMs.

Discovery Configuration

Discovery Configuration is a service that you can use to periodically discover computers in your network for newly added or upgraded CA ARCserve Backup software. A Discovery server runs as a background process that collects information from all other Discovery servers installed with CA products across the corporate network.

Discovery Configuration allows you to distribute discovered network target information to remote servers. This capability allows administrators to decrease network traffic load created by Discovery servers to discover Windows domains or IP subnet addresses.

The Discovery Configuration allows you to perform the following tasks:

- Start or stop the discovery service
- Distribute tables with discovered network targets
- Add, remove or modify information in any of the three tables created by Discovery Configuration (IP subnets, IP subnet masks, and Windows domains)
- Set or modify Discovery Configuration parameters

You can open the Discovery Configuration at the command line or from Windows Explorer:

- **Command line**--Start dsconfig.exe from the following directory:
C:\Program Files\CA\SharedComponents\ARCserve Backup\CADS
- **Windows Explorer**--Double-click dsconfig.exe located in the CA ARCserve Backup Shared Components directory. For example:
C:\Program Files\CA\SharedComponents\ARCserve Backup\CADS

Note: See the online help for procedures on how to start or stop the service or distribute tables with discovered network targets.

How the Discovery Service Detects Other Computers

A Discovery server is implemented as a Windows service. As soon as a Discovery server starts, it enumerates the list of products to create a behavior mask. Based on this mask, the Discovery server initializes the following required components:

- The Listen/Serialize component is initialized first and starts listening on a particular port (or Mailslot) for incoming packets (messages) from other Discovery servers. When a message is received, the Discovery server writes data (if any) into the repository (registry, for example) and then notifies the Query/Advertise component.
- The Query/Advertise component sends the message received from the Listen/Serialize component, (prepared with the product's list) directly to the Discovery server, which requested the data. The Query/Advertise component can also send messages as a broadcast message to the selected network targets (the list of IP Subnets or Windows Domains) if it is scheduled or initiated manually. It does this in order to query other Discovery servers across the network, and advertise its own list of CA ARCserve Backup products.

Discovery Service Configuration Options

You can specify the transport protocol used to broadcast queries by choosing configuration options that meet your needs. Select the Configuration button in the Discovery Configuration.

In the Network tab, you can choose the protocols to discover and define the TCP/IP subnet sweep. Choose to enable discovery of CA ARCserve Backup products if you want the discovery service to broadcast queries repeatedly with a specified interval.

Choose to enable network discovery if you want the Discovery server to run a process of discovering new Windows domains and IP subnets. By default, the Discovery server runs this process only when the discovery service is restarted. You can also modify the interval, depending on how dynamic your network environment is.

Note: It is not recommended that this option be run at all times because it continually broadcasts queries which can increase network traffic.

You can direct the Discovery Configuration application to clean its tables as the Discovery service starts. Discovery tables store information about computers with a CA ARCserve Backup product installed. When you enable this option, the Discovery service purges the data from its tables, discovers computers with a CA ARCserve Backup product installed, and then updates the tables with current, accurate data.

Important! The Clean Up Discovery Table on Startup option is enabled by default. If you disable this option and uninstall CA ARCserve Backup applications from systems from your environment, the details about these computers will remain in the tables when the Discovery service restarts.

Discovery Configuration Dialog

You can use the Discovery Configuration dialog to perform the following tasks:

- Specify the transport protocol used to broadcast queries.
- Enable Discovery of CA ARCserve Backup Products allows the Discovery Service (DS) to broadcast queries repeatedly, with a specified interval.

It is not recommended that this be run at all times because it continually broadcasts queries which could increase network traffic.

- Enable Network Discovery allows the DS to run a process of discovering new Windows domains and IP Subnets.

By default, the DS runs this process only when the Discovery Service is restarted. You can also modify the interval, depending on how dynamic your network environment is.

Network Tab

Use the Network tab to configure the following options:

- Specify the Protocols used to Discover.
- Specify the Protocols used to Reply.
- Enable Discovery of CA ARCserve Backup Products.
- Enable Discovery using TCP/IP Subnet Sweep.
- Enable Network Discovery and specify the time interval.
- Specify CA ARCserve Backup NetWare discovery settings.
- Direct the Discovery Service to clean the discovery tables on startup .

Adapters Tab

- Select IP address to Run Discovery.

IP Subnets/Windows Domains Discovery

In order to query and advertise, the Discovery Configuration needs the list of network targets to broadcast. For example, you might want to discover CA ARCserve Backup products in only one IP subnet on a TCP/IP enabled network or in a list of subnets located physically in the same country.

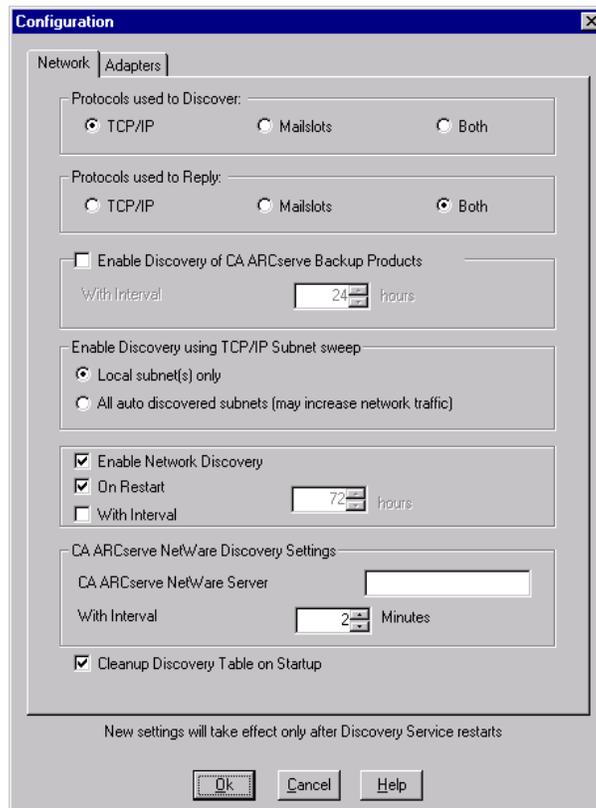
In another scenario, you might want to enumerate the entire corporate network to find all possible subnets and then filter some of them out. The discovery process runs in the background, and enumerates Windows network's resources. A list of Windows domains for subsequent Mailslot broadcasting or a listing of IP subnets for UDP broadcasting is created.

Note: This process may take some time, depending on the size of your network. It is recommended that the IP subnets and domains discovery be run during a time of minimum network traffic.

For information on starting and stopping the discovery service, see the online help.

Enable Discovery Using TCP/IP Subnet Sweep

You can configure to use a local or remote subnet sweep. The default setting is for a local subnet.

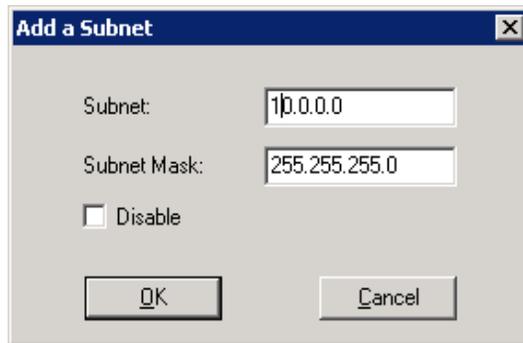


The discovery service broadcasts and retrieves all the information of the local subnet machines as well as manually-defined subnets and manually-defined machines. To add a machine name (IP address) manually, start Discovery and click the Add button on the Windows Domain tab.

Enter the IP address of the machine and click OK. The discovery service can then ping, publish, and return a product list from the specified machine.

Note: You can limit the discovery range by disabling any auto-discovered machine or Windows domain, which can reduce network traffic. Check the Disable box for an existing machine or Windows domain.

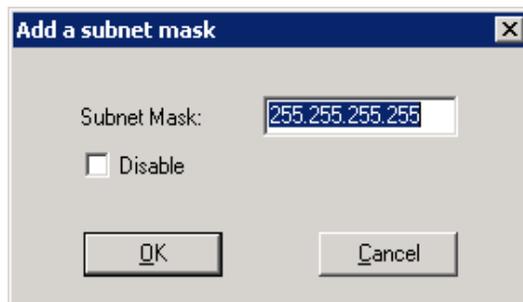
To add a remote subnet, start Discovery and click the Add button on the Subnet tab. The Add a Subnet dialog opens as shown in the following example:



Enter the Subnet and Subnet Mask and click OK. This enables the discovery service publish its product list to each machine to the specific subnet and also return product information for every machine in this subnet.

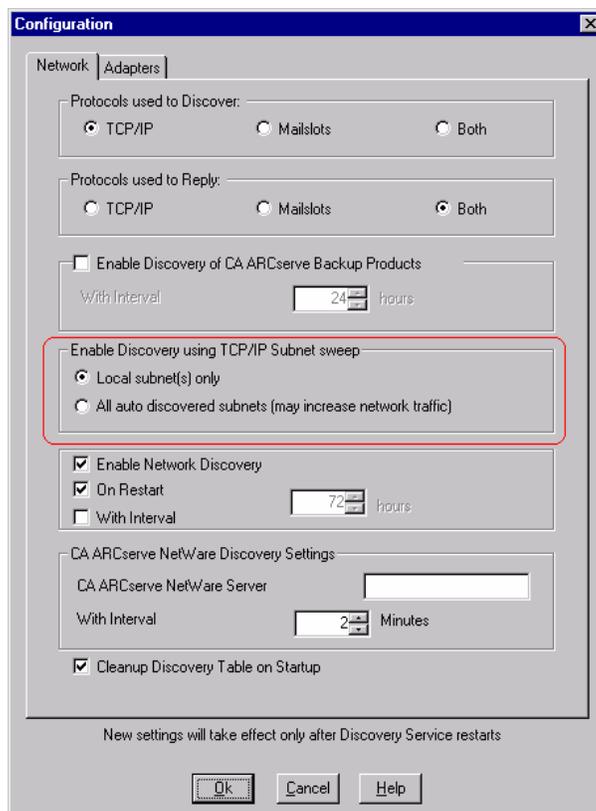
Note: You can limit the discovery range by disabling any auto-discovered machine or Windows domain, which can reduce network traffic. Check the Disable box for an existing machine or Windows domain.

If specific subnets use a different subnet mask you can add a subnet mask manually by starting Discovery and clicking the Add button on the Subnet Mask tab. The Add a Subnet Mask dialog opens as shown in the following example:



If you choose to perform an auto discovery, the discovery service will ping and publish a product list to each machine in each subnet listed in the Discovery Configuration Subnet tab and retrieve the product information from the remote machine.

To do this, start Discovery and click the Configure button on the Summary tab. The Configuration dialog opens as shown in the following example:



The Discovery server initiates an IP address sweep for remote subnets by using the auto-discovered subnets, subnet masks, machine, or Windows domains along with the manually-configured subnets, subnet masks, machines or Windows domains. Selecting this option may increase network traffic and can take a considerable amount of time to complete, depending on the size of your network. We recommend that you run this option during a time of minimum network traffic.

Note: If you choose to discover CA ARCserve Backup products in remote subnets, the discovery service does not rely on a UDP broadcast to locate remote instances. You need to know the size of the subnet and range of IP addresses using a subnet mask.

Discovery Configuration for the SAN Option

The Discovery service configuration for servers in a SAN environment require additional modifications in order for all servers to be discovered. To ensure that all SAN servers are enabled for discovery, one of the following options are available:

- Select the "All auto discovered subnets (may increase network traffic)" option in the Enable Discovery using TCP/IP Subnet sweep field in the Configuration dialog.
- Add other remote SAN machine names/IP addresses by accessing the Windows Domain tab.

Note: The configuration for each remote SAN server must be consistent to ensure accurate discovery. If you only configure one SAN server, other servers may still fail in discovery.

Discover Client Agent Systems with Non-default IP Addresses

If you select a non-default IP address for a client agent node, you must perform the following procedure to update the IP address to the new address, to allow you to add machines using AutoDiscovery.

To discover client agent systems with non-default IP addresses

1. On the agent machine, restart the discovery service using dsconfig.exe.
2. From the Backup Manager of the base server, delete the old machine object.
3. On the base server, restart the discovery service or launch AutoDiscovery using dsconfig.exe.
4. From the Backup Manager, add the machine with the new IP address using AutoDiscovery.
5. If you have a scheduled job in the queue, delete that job and recreate it to ensure that it runs properly.

Allow CA ARCserve Backup Services and Applications to Communicate Through the Windows Firewall

During the installation or upgrade process, the installation wizard configures your Windows firewall such that CA ARCserve Backup services and applications can communicate properly. The installation wizard performs the configuration task only if the Windows firewall was in the On state when you installed CA ARCserve Backup.

If the Windows firewall was in the Off state when you installed CA ARCserve Backup, and then turned on the Windows firewall at any time after you installed CA ARCserve Backup, the ARCserve services and applications will not be able to communicate through the Windows firewall.

The following procedure lets you allow CA ARCserve Backup services and applications to communicate if the Windows firewall was in the Off state when you installed CA ARCserve Backup.

To allow CA ARCserve Backup services and applications to communicate through the Windows firewall

1. Open the Windows Command Line, and change to the following directory:

```
c:\Program Files\CA\SharedComponents\ARCserve Backup\
```

2. Execute the following command:

```
setupfw.exe /INSTALL
```

CA ARCserve Backup services and applications are added to the Windows firewall exception list. CA ARCserve Backup services and applications can now communicate through the Windows firewall.

How to Configure Your Firewall to Optimize Communication

For information about configuring firewalls to optimize CA ARCserve Backup communication, see the *Implementation Guide*.

Chapter 8: Managing the Database and Reporting

This section contains the following topics:

[How to Manage the Database and Reports](#) (see page 551)

[Database Manager](#) (see page 552)

[How to Protect the CA ARCserve Backup Database](#) (see page 555)

[How the Catalog Database Works](#) (see page 597)

[Using Microsoft SQL Server as the CA ARCserve Backup Database](#) (see page 605)

[Specify a CA ARCserve Backup Database Application](#) (see page 609)

[CA ARCserve Backup Logs and Reports](#) (see page 617)

[CA ARCserve Backup Diagnostic Utility](#) (see page 632)

How to Manage the Database and Reports

The CA ARCserve Backup database maintains job, media, and device information on your system. CA ARCserve Backup stores the following types of information in the database:

- Detailed information about all jobs.
- Session details for all backup jobs.
- Information about the media used for all backup jobs.
- Detailed information about each file and directory that was backed up to media when you perform a restore.

When you want to restore a specific file, the database determines which media a file is stored on.

- Detailed information about media pools and media location.

The database information is also used to generate many types of reports.

Database Manager

The Database Manager lets you to:

- Keep track of the location of your media.
- Determine the session number of your backup.
- Determine if media should be retired.
- View log information about jobs you have run.
- Delete old records from the database.
- Visually compare the size of your database to the total available disk space.

Note for Microsoft SQL Server databases: The total database size reported by the CA ARCserve Backup Database Manager is the size of the data device. You can obtain more information by browsing through the Microsoft SQL Server Enterprise Manager.

Database Views

When you open the Database Manager, the left panel displays the following options:

- **Summary**--Space the database used on your hard disk, database type, and other settings.
- **Job Records**--Jobs processed by CA ARCserve Backup.
- **Media Records**--Media used by CA ARCserve Backup.
- **Device Records**--Devices used by CA ARCserve Backup.

Sort Order

To change the sort order of records displayed in the Job, Media, and Device Records view, click on the field name you want to sort.

Database Pruning

You can set CA ARCserve Backup to remove old records from the database. For more information, see the chapter "Administering the Backup Server."

When You Should Rebuild the SQL Indexes

Note: This section only applies when using Microsoft SQL as the CA ARCserve Backup database.

You should rebuild the SQL Server index periodically to keep the index size manageable and at optimal performance. The best practice is to rebuild the index once or twice per month, or when the ARCserve database performs slowly.

The process of updating the SQL Server indexes can take a lot of time. If you do not have enough time to update all the indexes, you should update the key indexes: IX_astpdat_1, IX_astpdat_2, X_astpdat_3, K_pathname, and PK_filename. These indexes play an important role and affect the browsing speed in the Restore Manager and Database Manager.

For information about how to rebuild the SQL Server indexes, see the Microsoft SQL Server documentation.

Types of Errors Reported

The following statistical information is recorded in the database:

- **Media Errors**--Indicates data corruption occurred on the media preventing the read or write operation from successfully completing.
- **Soft Read Errors**--An error occurred while reading the media. CA ARCserve Backup attempted to correct the problem in real-time. A higher number of soft read errors indicate possible defective media. Media should be replaced for any future backups.
- **Soft Write Errors**--A write error occurred during the backup. CA ARCserve Backup is correcting the media problem in real time. A high number of soft write errors indicates the media should be replaced for future backups. Make sure the drive heads are cleaned after the current backup session is completed.

Device Error Records

If a drive has a critical error, the error log may contain some of the following information:

- **Time**--Time the error occurred.
- **Sense Info**--SCSI error code.
- **Media**--Number of media errors that occurred during the job.
- **Soft Write**--Number of soft write errors

- **Soft Read**--Number of soft read errors that occurred during the job.
- **Media Usage**--Amount of time the media was used during the job.
- **KB written**--Amount of data written to the media during the job.
- **Times Formatted**--Number of times media has been formatted.

Last CA ARCserve Backup Database Backup Information

Every time the CA ARCserve Backup database is backed up successfully, the backup media information is retained in a series of log files labeled ASDBBackups.txt and ASDBBackups.n.txt. The log files are stored in the CA ARCserve Backup home directory.

Each of these log files contains the detail information about the complete backup history of the CA ARCserve Backup database. For example, the log files contain detail information about the following items:

Note: This is not an exhaustive list.

- Tape name, serial number, and sequence number
- Session GUID, session ID, session type
- Backup method (for example, full, incremental, differential)
- Backup date
- Type of database
- Path of the instance

Note: The log files do not contain descriptive text or comments.

CA ARCserve Backup references the log files when you need to restore the CA ARCserve Backup database because it is not in a usable state or corrupt. The CA ARCserve Backup Disaster Recovery Option and the `ca_recoverdb` command reference ASDBBackups.txt to determine the media that contains the latest CA ARCserve Backup database backup data.

CA ARCserve Backup manages the log files using the following logic:

1. The information for the most recent full, incremental, and differential backup of the CA ARCserve Backup database is always stored in the file labeled ASDBBackups.txt.
2. After the second full backup of the CA ARCserve Backup database is complete, ASDBBackups.txt is renamed ASDBBackups.1.txt and then a new ASDBBackups.txt is created.
3. After the third full backup is complete, ASDBBackups.1.txt is renamed ASDBBackups.2.txt, ASDBBackups.txt is renamed ASDBBackups.1.txt and then a new ASDBBackups.txt is created.
4. The log file renaming and creating process continues until CA ARCserve Backup creates a log file named ASDBBackups.10.txt.
5. If a log file labeled ASDBBackups.10.txt exists after the full backup is complete, CA ARCserve Backup deletes ASDBBackups.10.txt, renames the older log files, and then creates a new ASDBBackups.txt log file.

If ASDBBackups.txt is corrupt, you can rename any of the files labeled ASDBBackups.n.txt to ASDBBackups.txt and use the renamed log file to recover the CA ARCserve Backup database.

Enable Media Pool Maintenance

Using the Enable Media Pool Maintenance option you can allow daily maintenance of the media pool. CA ARCserve Backup performs media pool maintenance tasks according to the Prune job schedule.

To enable media pool maintenance

1. Open the Server Admin Manager and click the Configuration toolbar button.
The Configuration dialog opens.
2. Select the Database Engine tab.
The Database Engine dialog appears displaying the media pool maintenance option at the bottom of the dialog.
3. Click Enable Media Pool Maintenance and click OK.
Media pool maintenance is enabled.

How to Protect the CA ARCserve Backup Database

The following sections describe how to back up and restore the CA ARCserve Backup database.

Agent for ARCserve Database

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

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

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 must copy the "ASDBSQLAgent" folder to the system where you are installing the agent, and run the utility on that machine.

Access Requirements

When you submit a job that includes remote Windows database servers, CA ARCserve Backup prompts you for a default user name and password for the system on which the database resides. CA ARCserve Backup accesses the remote servers using this user name and password.

A Microsoft SQL Server native user name and password are also required to access some database servers. When prompted by the system, enter the Microsoft SQL Server user ID and the password of the system administrator (sa), or enter a user ID and password with equivalent privileges. This user may be a Windows user, depending on security settings.

Note that there are two different data transfer mechanisms available to the agent, and that they have different permission requirements. A backup using Named Pipes only requires the Backup Operator permission for the specific database being backed up, and the Database Creator role to perform the database. A backup using Virtual Devices, however, requires the System Administrator role.

Note: A user in the Backup Operator Group does not have rights to access the CA ARCserve Backup database. As a result member servers are not visible, to the user, in the Backup Manager.

Configure Backup and Restore Parameters for the Agent for Microsoft SQL Server

Use the Microsoft SQL Agent Configuration utility to configure the Agent for Microsoft SQL Server backup and restore parameters for Microsoft SQL Server 7.0, 2000, 2005, and 2008. The parameters include settings for Microsoft Virtual Device Interface (VDI) objects and remote communication.

To configure backup and restore parameters for the Agent for Microsoft SQL Server

1. Open Windows Explorer and browse to the following directory:
C:\Program Files\CA\SharedComponents\ARCserve Backup\UniAgent
2. Double-click the file labeled admin.exe
The ARCserve Backup Agent Admin window opens.
3. From the pull-down list, select CA ARCserve Backup Agent for Microsoft SQL Server and click the Configuration button on the toolbar.
The SQL Server DBAgent Configuration dialog opens.

- Click the Common Settings tab and specify the level of detail and synchronized recording under Agent Log Settings as follows:

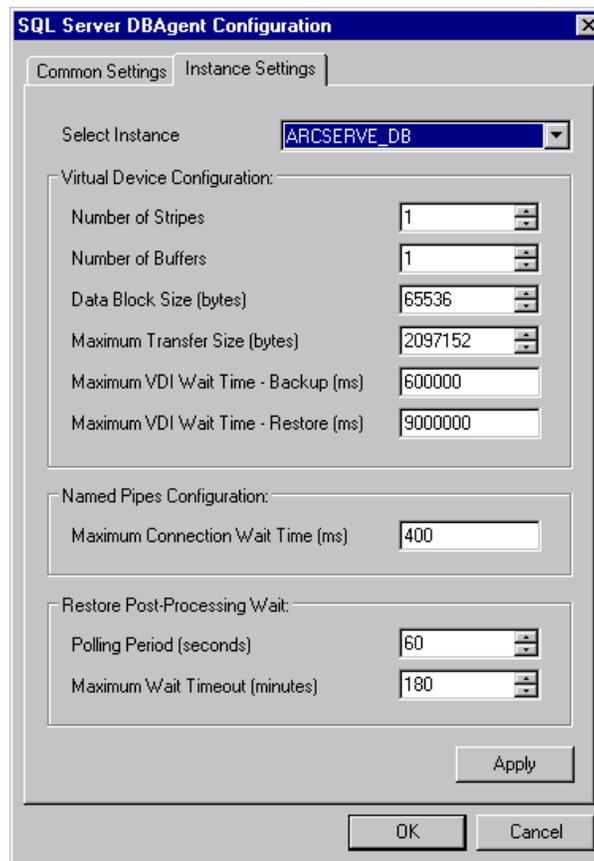
Level of Detail

Controls the settings for level of detail of the agent's Activity Log and Debugging Log. For the Activity Log settings, a Level of Detail setting of Normal (0) includes basic information about agent activity. A setting of Detail (1) includes more detailed information about agent activity. A setting of Debug (2) enables the Debugging Log at a moderate level of detail. A setting of Trace (3) enables the Debugging Log at a very high level of detail. The Activity Log is localized for your reference. The Debugging Log is for CA Support use, and is not available in multiple languages.

Synchronized Recording

Forces the log messages to be written to the Activity Log as they are posted. You can disable this option to improve the performance on high-load systems by caching several messages and writing them as a group.

- Click the Instance Settings tab. The following screen appears:



6. Select the default instance (MSSQLSERVER) or the name of the instance (for Microsoft SQL Server 2000 and SQL Server 2005) for which the Agent for Microsoft SQL Server configuration is to be changed.

7. Set the parameters under Virtual Device Configuration as follows:

Number of Stripes

Determines the number of CPUs used to perform backups. Set this value to match the number of CPUs in the database server for the fastest backup performance. The default setting is 1 and the maximum value is 32.

Number of Buffers

The total number of VDI buffers (of maximum transfer size) used to back up and restore. The default setting is 1. This number cannot be less than the number of stripes.

Data Block Size (in bytes)

All data transfer sizes are multiples of this value. Values must be a power of 2 between 512 bytes and 64 KB inclusive. The default is 65536 or 64 KB.

Maximum transfer size

The maximum input or output request issued by Microsoft SQL Server to the device. This is the data portion of the buffer. This parameter value must be a multiple of 64 KB. The range is from 64 KB to 4 MB. The default setting is 2097152 or 2 MB.

Maximum VDI Wait Time - Backup (ms)

The time, in milliseconds, a Virtual Device object waits for a response from Microsoft SQL Server during a backup operation. This setting is also used by the agent when waiting for parallel operations to synchronize or background operations to complete, including during some parts of restore operations. The default setting is 60000 ms (ten minutes).

Maximum VDI Wait Time - Restore (ms)

The time, in milliseconds, a Virtual Device object waits for a response from Microsoft SQL Server during a restore. Increase this time if the database to be restored contains very large data files. The default setting is 9000000 ms (2.5 hours).

8. Under Named Pipes Configuration specify the Maximum Connection Wait Time (ms) time, in milliseconds, the Agent for Microsoft SQL Server should wait to close a named pipe if a remote connection fails. The default setting is 400 ms.

9. Set the parameters under Restore Post-Processing Wait as follows:

Polling Period (seconds)

The amount of time to wait between checks of the database status. The default setting is 60 seconds (one minute).

Maximum Wait Timeout (minutes)

The total amount of time to wait before abandoning the waiting process. If this timeout elapses and the job contains additional Transaction Log sessions to be restored, then those additional sessions may fail to restore because SQL Server is not yet ready. The default setting is 180 minutes (three hours).

10. Click Apply to apply the changes to that Instance.

If you want to change the settings for another instance, select the next instance from the drop-down list, and go to step 4.

How the Database Protection Job Works

CA ARCserve Backup lets you use Microsoft SQL Server 2005 Express Edition or Microsoft SQL Server for the CA ARCserve Backup database. Microsoft SQL Server 2005 Express Edition is a free, lightweight version of Microsoft SQL Server. Although these applications are quite different from each other, with respect to architecture and scalability, you can easily protect either version using the CA ARCserve Backup default Database Protection Job.

After you install CA ARCserve Backup, the Database Protection Job maintains a status of Hold. To protect the CA ARCserve Backup database, you must change the status of the Database Protection Job from Hold to Ready. For more information see, [Start the CA ARCserve Backup Database Protection Job](#) (see page 571).

If you accept the default Database Protection Job, the job schedule will contain the following values:

- **Schedule Name**--5-day weekly incremental backup, full backup on Friday
- **Execution Time**--11:00AM
- **Rotation Rules**--Overwrite media
- **Media Pool Used**--ASDBPROTJOB

Note: The default retention time of six days allows you to have recovery points of at least a week. If you want more than that, you can increase the retention time from the media pool property, ASDBPROTJOB, manually.

Important! After you start the Database Protection Job, the Tape Engine will connect to a blank media in the first group that Tape Engine detects, and assign the media pool labeled ASDBPROTJOB. If the Tape Engine cannot connect to a blank media in the first group within five minutes, the Tape Engine will try to connect with blank media in the other groups sequentially. If the Tape Engine cannot connect to blank media, in any group, the job will fail.

More information:

[Modify, Create, and Submit a Custom Database Protection Job](#) (see page 562)

How to Back Up the CA ARCserve Backup Database

There are two approaches that you can use to back up the CA ARCserve Backup database.

- Create a backup job as you would create any other backup job and include the CA ARCserve Backup database objects with the source selections for the job.

This method requires that you know if you are running SQL Server 2005 Express or SQL Server in your environment. With this knowledge you must specify the proper source selections and Global Backup Operation options for the job to ensure that the required metadata and related items for each database type are backed up.

This approach lets you back up the affected databases, files, or both, when the backup up job is complete.

- **Modify an existing CA ARCserve Backup Database Protection Job.**
When you modify an existing Database Protection Job, CA ARCserve Backup detects the type of database that is running in your environment.
With this approach, CA ARCserve Backup selects the proper source selections and specifies the required Global Backup Operation options to ensure that the required metadata and related items for each database type are backed up.

Important! You should not protect the ARCserve database using multiple backup servers that do not reside in the domain that is using the ARCserve database.

Modify, Create, and Submit a Custom Database Protection Job

This section describes how to modify or create a custom Database Protection Job from an existing Database Protection Job. This task helps to ensure that your CA ARCserve Backup is backed up and is protected.

Prerequisite Tasks

Before proceeding, ensure that the following prerequisite tasks are complete:

- Ensure that the Tape Engine can detect at least one device in your environment. For more information, see "Managing Devices and Media."
- Ensure that the default Database Protection Job exists in the Job Queue. If the Database Protection Job does not exist in the Job Queue, you must recreate it. For more information, see [Recreate the CA ARCserve Backup Database Protection Job](#) (see page 573).

To modify or create a custom database protection job

1. Open the CA ARCserve Backup Manager Console.

From the Quick Start menu on the CA ARCserve Backup Home Page, click Job Status.

The Job Status Manager window opens.

2. Click the Job Queue tab.

Locate and select the Database Protection job.

Note: If the Database Protection Job does not exist, you must recreate it. For more information, see [Recreate the CA ARCserve Backup Database Protection Job](#) (see page 573).

Right-click the Database Protection Job and select Modify from the pop-up menu.

The Backup Manager window opens displaying the Staging, Destination, and Schedule tab.

Note: When you modify the Database Protection Job, CA ARCserve Backup detects the type of database that is running in your environment (SQL Express 2005 or SQL Server) and specifies the database objects that are required to protect the database.

3. Do one of the following:

- Click the Staging tab and specify where you want to stage the backup data. For more information about using staging, see [How to Manage Backup Data Using the Disk to Disk to Tape Option](#) (see page 223).
- Click the Destination tab and specify a location, media, or both where you want to store the backup data. For more information, see [Options You Can Specify on the Backup Manager Destination Tab](#) (see page 136).

4. Click the Schedule tab and specify a schedule for the job. For more information, see [Rotation Schemes](#) (see page 287).

5. Click Options on the toolbar.

The Global Options dialog opens.

6. Click the Operation tab.

Specify Append Backup of CA ARCserve Backup data at the end of job options required for your CA ARCserve Backup database:

SQL Server 2005 Express Edition--Required Options

For SQL Server 2005 Express databases, the following options are required and preselected for you:

- **CA ARCserve Backup database**--This option ensures that the CA ARCserve Backup database is backed up after jobs are complete.
- **Job scripts**--This option ensures that new and updated job scripts are backed up after jobs are complete.
- **SQL Server Disaster Recovery Elements for CA ARCserve Backup database**--This option ensures that the elements required to recover a SQL Server database from a disaster are backed up after jobs are complete.

SQL Server 2005 Express Edition--Optional Options

For SQL Server 2005 Express databases, the following options are optional:

- **Catalog files**--This option ensures that the Catalog files are backed after backup jobs are complete.

SQL Server--Required Options

For SQL Server databases, the following options are required and preselected for you:

- **CA ARCserve Backup database**--This option ensures that the CA ARCserve Backup database is backed up after jobs are complete.
- **Job scripts**--This option ensures that new and updated job scripts are backed up after jobs are complete.

SQL Server--Optional Options

For SQL Server databases, the following options are optional:

- **SQL Server Disaster Recovery Elements for CA ARCserve Backup database**--This option ensures that the elements required to recover a SQL Server database from a disaster are backed up after jobs are complete.
- **Catalog files**--This option ensures that the Catalog files are backed after backup jobs are complete.

Click OK.

The Global Options dialog closes and the Operation options are applied.

7. Click Start on the toolbar.
The Submit Job dialog opens.
8. From the Submit Job dialog, enter a description for your job and click OK.
The Database Protection Job is submitted.

Specify Microsoft SQL Server 2005 Express Backup Options

CA ARCserve Backup can use full and differential backup methods when backing up Microsoft SQL Server 2005 Express databases. This capability lets you use a rotation scheme or a schedule when backing up the CA ARCserve Backup database. Additionally, CA ARCserve Backup lets you check the consistency of the database before the backup job starts or after the backup job is complete.

To specify Microsoft SQL Server 2005 Express backup options

1. Open the Backup Manager windows, select the Source tab, and expand the Windows System object to locate the CA ARCserve Backup primary server.
2. Expand the Primary server, right-click the CA ARCserve Backup Database object, and select Agent Option from the pop-up menu.

The Agent Backup Option dialog opens.

3. From the Agent Backup Option dialog, specify the options that you require to protect the database.

Backup Method

Specify one of the following backup methods:

- **Use Global or Rotation Options**--Select this option to perform a full or differential backup based on the global job method or rotation phase. The Incremental job method or rotation phase results in a Differential backup.

This is the default backup option.

- **Full**--Select this option to perform a full backup every time the job is run.

When you perform a full backup, CA ARCserve Backup performs a full backup of the three system databases, the 24 ARCserve databases, and records a synchronization checkpoint. CA ARCserve Backup creates two backup sessions. One session will contain the disaster recovery elements. The other session will contain all of the data that is required to restore the CA ARCserve Backup database.

- **Differential**--Select this option to perform a differential backup every time the job is run.

When you perform a differential backup, CA ARCserve Backup performs a differential backup of the 24 ARCserve databases and records a synchronization checkpoint. CA ARCserve Backup creates one backup session containing all of the data that is required to restore the CA ARCserve Backup database.

Database Consistency Check

The following options let you check the allocation and structural integrity of all of the objects in the specified databases. Specify the options that you require.

- **Before backup**--Select this option to check the consistency of the database before the backup starts.
- **After backup**--Select this option to check the consistency of the database after the backup completes.
- **Continue with Backup, if DBCC fails**--Select this option to continue the backup even if the check before backup operation fails.
- **Do not check indexes**--Select this option to check only the system tables.
- **Check the physical consistency of the database**--Select this option to detect torn pages and common hardware failures. In addition, it checks the integrity of the physical structure of the page and record headers, and the consistency between the page's object ID and index ID.

Override Global Options

Causes the Agent to ignore all checkbox-based options from the Global Agent Options tab for only the specified database.

Note: Backup Method and Transaction Log Truncation options are not affected by this option because they can be overridden separately. This option is available only on a per-database basis.

4. Click OK.

Specify Microsoft SQL Server Backup Options

CA ARCserve Backup can use full and differential backup methods when backing up Microsoft SQL Server databases. This capability lets you use a rotation scheme or a schedule when backing up the CA ARCserve Backup database. Additionally, CA ARCserve Backup lets you back up only the transaction log and check the consistency of the database before a backup job starts or after the backup job is complete.

Note: To specify SQL Server backup options, you must authenticate using Windows or SQL Server credentials.

To specify Microsoft SQL Server backup options

1. Open the Backup Manager windows, select the Source tab, and expand the Windows System object and locate the server that is hosting the CA ARCserve Backup database.
2. The server hosting the ARCserve database can be a primary server, a member server, or a remote system. If the server hosting the Microsoft SQL Server database does not appear in the Backup Manager system tree, you must first add the system to the directory tree under the Windows Systems object before continuing. For more information, see [Back Up Remote Servers](#) (see page 189).
3. Expand the server, right-click the CA ARCserve Backup database object, and select Agent Option from the pop-up menu.

The Agent Backup Option dialog opens.

4. From the Agent Backup Option dialog, specify the options that you require to protect the database.

The following backup methods are provided:

Use Global or Rotation Options

Backs up the database selected using the job's Global or Rotation Phase Backup Method. The Global or Rotation Options provides the following options:

- The Full job method will result in a Full backup of the database.
- The Differential job method will result in a Differential backup of the database, unless this database has not yet had a Full backup.
- The Incremental job method will result in a Transaction Log backup With Truncation for databases using the Full and Bulk-Logged Recovery Models, and a Differential backup of databases using the Simple Recovery Model, unless this database has not yet had a Full backup.
- The three main System databases are exempt from the Global or Rotation job method; selecting this option for databases [master], [model], or [msdb] will always result in a Full backup.

Full

A Full backup is performed. The files included in the Database Subset will be backed up in their entirety.

Differential

Backs up data that has changed since the last Full backup. For example, if you ran a complete backup of your database on Sunday night, you can run a differential backup on Monday night to back up only the data that changed on Monday. This option is not available for the [master] database.

Transaction Log

Backs up only the Transaction log. This option is only available for databases using the Full and Bulk-Logged Recovery Models.

The following Database Subset options are provided:

The database subset backs up selected files in a database. Use this option to back up a file or FileGroup when the database size and performance requirements do not allow you to perform a full database backup.

Note: The Database Subset options are disabled if the selected Backup Method is Transaction Log Only.

Entire Database

Backs up the entire database.

Files and FileGroups

Backs up selected files in a database. Use this option to back up a file or FileGroup when the database size and performance requirements make it impractical to perform a full database backup. This option is available only for databases using the Full and Bulk-Logged Recovery Models.

Partial Database

Backs up the Primary FileGroup, and any other Read-Write FileGroups. For a Read-Only database, only the Primary FileGroup will be backed up. This option requires SQL Server 2005 or later.

Back up Transaction Log After Database

Backs up the transaction log after the database is backed up. This allows you to perform a Full or Differential backup and a Transaction Log backup in the same job. This option is available only for databases using the Full and Bulk-Logged Recovery Models.

The following Log Truncation Options are provided:

Remove inactive entries from transaction log, after backup

Truncates the log files. This is the default option.

Do not remove inactive entries from transaction log, after backup

Retains inactive log entries after backup. These entries are included in the next Transaction log backup.

Backup only the log tail and leave the database in unrecovered mode

Backs up the log and leaves the database in a restoring state. This option is available for Microsoft SQL Server 2000 or later. Use this option to capture activity since the last backup and take the database offline to restore it.

Important! Do not use the "Backup only the log tail and leave the database in unrecovered mode" log truncation option to back up the ARCserve Database. Performing a backup with this option causes the database to be placed in an offline status, and you can lose the ability to find the backups of the ARCserve Database in order to perform a restore and bring the database online. If you perform a backup of the ARCserve Database using this option, you can use the `ca_recoverdb` command line utility to restore the ARCserve Database and bring it back online.

The following database consistency options are provided:

A DBCC tests the physical and logical consistency of a database. DBCC provides the following options:

Before Backup

Checks consistency before the backup of the database.

After Backup

Checks consistency after the backup of the database.

Continue with backup, if DBCC fails

Performs a database backup even if the consistency check fails.

After restore

Performs DBCC after the restore of the database.

Do not check indexes

Checks the database for consistency without checking indexes for user-defined tables.

Note: The system table indexes are checked regardless of whether you select this option.

Check the physical consistency of the database

Detects torn pages and common hardware failures. In addition, it checks the integrity of the physical structure of the page and record headers, and the consistency between the page's object ID and index ID.

Include Checksums generated by SQL Server

Includes error checking information from Microsoft SQL Server, which can be used to validate the integrity of the backed-up data during restore. This option requires SQL Server 2005 or later.

All error messages that are generated during the DBCC are recorded in the Agent for Microsoft SQL Server log file called sqlpag.log. The log is located in the Backup Agent directory.

Override Global Options

Enabling this option will override the Global option setting pertaining to the selected database.

Note: Backup Method and Transaction Log Truncation options are not affected by this option because they can be overridden separately. This option is available only on a per-database basis.

5. Click OK.

The Agent Backup Options are applied.

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](#) (see page 573).

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.

Delete the CA ARCserve Backup Database Protection Job

Use the following procedure to delete the default CA ARCserve Backup Database Protection Job.

Important! You should always back up the CA ARCserve Backup database. Failure to do so can result in unrecoverable backup data.

To delete 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 opens.
2. Select the Job Queue tab and locate the Database Protection Job.
Right-click the Database Protection Job and select Delete from the pop-up menu.
A warning message appears.
3. If you are sure that you want to delete the Database Protection Job, click OK.
The Database Protection Job is deleted.

Note: Form information about how to recreate the CA ARCserve Backup Database Protection Job, see [Recreate the CA ARCserve Backup Database Protection Job](#) (see page 573).

Recreate the CA ARCserve Backup Database Protection Job

The following procedure describes how to recreate the Database Protection Job. Use this procedure when you want to recreate the Database Protection Job because the original job was deleted or you want to reset the Database Protection Job to its original settings.

To recreate 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 Server Admin.
The Server Admin window opens.
2. Click the Configuration toolbar button.
The Configuration - <Server name> dialog opens.

3. Select the Database Engine tab and do the following:
 - a. Check the Submit ARCserve DB protection job check box.
 - b. In the Server field, specify the name of the CA ARCserve Backup server where you want the Database Protection Job to run. You can specify an ARCserve primary server or an ARCserve member server from the domain where you want to recreate the Database Protection job.
 - c. In the Group field, specify the name of the device group where you want to store the Database Protection Job data.

Click OK.

CA ARCserve Backup recreates the Database Protection Job.

4. Start the CA ARCserve Backup Database Protection Job.

Note: For more information, see [Start the CA ARCserve Backup Database Protection Job](#) (see page 571).

How to Restore the CA ARCserve Backup Database

There are several methods that you can use to restore the CA ARCserve Backup database. The following list describes these methods and includes a description of any special considerations or limitations associated with the method.

Important! Microsoft SQL Server database architecture and CA ARCserve Backup sessions are quite different from that of Microsoft SQL Server 2005 Express. If you attempt to restore Microsoft SQL Server data with Microsoft SQL Server 2005 Express backup sessions, or, conversely, restore Microsoft SQL Server 2005 Express with Microsoft SQL Server backup sessions, the recovery process can corrupt your data.

- **ca_recoverdb Utility**--ca_recoverdb is a command line based utility that lets you recover the CA ARCserve Backup database when it is in an unusable state. It lets you recover the CA ARCserve Backup database if it was backed up in the same CA ARCserve Backup domain that is using it.

Note: For more information, see the *Command Line Reference Guide*.

- **Standard Restore - Backed up in the CA ARCserve Backup domain that is using the database**--This restore method can be used in the following scenarios:

- The CA ARCserve Backup database was backed up in the CA ARCserve Backup domain that is using the database.
- The CA ARCserve Backup database is on line and functioning properly.
- You want to restore the CA ARCserve Backup database to a particular point in time.

Note: You can restore the CA ARCserve Backup database to its original location or a different location.

- **Standard Restore - Backed up in a different CA ARCserve Backup domain**--This restore method can be used in the following scenarios:

- The database was backed up in a CA ARCserve Backup domain that is different from the CA ARCserve Backup domain that is using the database.
- The CA ARCserve Backup database is on line and functioning properly.
- You want to restore the CA ARCserve Backup database to a particular point in time.

Note: For SQL Server 2005 Express installations, you must restore the CA ARCserve Backup database to its original location. For SQL Server installations, you can restore the CA ARCserve Backup database to its original or a different location.

Open the Agent Restore Options Dialog

The Agents Restore Options dialog lets you specify how you want to restore Microsoft SQL Server 2005 Express Edition and Microsoft SQL Server database instances.

To open the Agent Restore Options dialog

1. From the Quick Start menu in the Navigation Bar on the home page, click Restore.

The Restore Manager window opens.

2. From the restore method drop-down list, select Restore by Tree.

From the server tree, locate and expand the system hosting the ARCserve database instance.

Right-click the CA ARCserve Backup Database object and select Agent Option from the pop-up menu.

The Agent Restore Options dialog opens.

3. Complete the required fields for the ARCserve database instance.

More information:

[Agent Restore Options - Restore Options](#) (see page 576)

[Agent Restore Options - Restore DB Files As](#) (see page 578)

[Agent Restore Options - SQL Instance Restore](#) (see page 578)

[Agent Restore Options - SQL Instance DB Files As](#) (see page 586)

Agent Restore Options - Restore Options

The Agent Restore Options dialog lets you specify database restore options and the location to restore them.

The Restore Options tab lets you choose how your database is recovered. This tab contains the following selections:

CA ARCserve Backup Automatic Selection

Lets you automatically select all required sessions and options. This option is enabled by default for every restore job and applies selected options appropriately to the automatically selected sessions.

Miscellaneous

Force restore over existing files or database

Enable this option to let Microsoft SQL Server overwrite files it does not recognize as part of the database it is restoring. Use this option only if you receive a message from Microsoft SQL Server prompting you to use the With Replace option. This option is equivalent to using the With Replace parameter of the restore command.

Use current ASDB as original location

Enable this option if you wish to use current CA ARCserve Backup database as original location.

Recovery Completion State

The following switches determine the condition of the database at the end of the restore job.

Leave database operational

Instructs the restore operation to roll back any uncommitted transactions. After the recovery process, the database is ready for use.

Note: If you use Automatic Selection, you do not have to choose any of the Recovery Completion State selections manually, because CA ARCserve Backup performs the selection of sessions and the necessary options automatically. If you do not choose Automatic Selection, you must follow Microsoft SQL Server rules regarding the restore flow. For more information, see Microsoft SQL Server documentation.

Leave database offline and able to restore differential

Instructs the restore operation not to roll back any uncommitted transactions and to leave the database in a state where it can accept additional Files-and-FileGroups, Differential, or Transaction Log restores. This is usually selected when performing manual restores.

Database Consistency Check

After restore

Enable this option to check the consistency of the database after the backup completes. To select this option, you must also choose Leave Database Operational. Selecting this option enables the following options.

Do not check indexes

Enable this option to check for consistency without checking indexes for user-defined tables.

Check only the physical consistency of the database

Enable this option to check the database for torn pages and common hardware failures. Additionally, it checks the integrity of the physical structure of the page and record headers, and the consistency between the page's object ID and index ID. This option bypasses the data validity tests normally performed in a standard database consistency check and examines only those related to physical integrity. Index checking is part of the physical integrity tests unless you specifically disable it by selecting Do not check indexes.

Agent Restore Options - Restore DB Files As

The Restore DB Files As tab lets you specify the location to which the database is recovered. This tab contains the following selections:

Restore to Original Location

Lets you restore the database to its original location, overwriting the current version.

Database Move Rules

Lets you recover the database to a new drive or directory.

Agent Restore Options - SQL Instance Restore

The Agent Restore Options dialog lets you specify database restore options and the location to restore them.

The Restore Options tab lets you choose how your database is recovered. This tab contains the following selections:

CA ARCserve Backup Automatic Selection

Lets you automatically select all required sessions and options. This option is enabled by default for every restore job and applies selected options appropriately to the automatically selected sessions.

Restore

Database

Lets you back up the entire database.

Files and FileGroups

Lets you backup a file or file group when the database size and performance requirements make it impractical to perform a full database backup.

Partial restore

Note: This option is for Microsoft SQL Server 2000 and Microsoft SQL Server 2005 only.

Lets you restore part of the database to another location so that damaged or missing data can be copied back to the original database. The granularity of the partial restore operation is the database file group. The primary file and file group are always restored, along with the files that you specify and their corresponding file groups. The result is a subset of the database. File groups that are not restored are marked as offline and are not accessible.

Torn Page Repair - Online

Repairs databases in place without the need to perform a restore of the entire database. This operation is recommended when only a few pages are damaged and an immediate recovery is critical.

The database should first be taken offline by performing a Transaction Log backup with the Log Tail option. A Database Consistency Check Before Backup with the Continue if DBCC Fails option is recommended to identify damaged pages that are not recognized, and forestall the possible need of repeating the process. This option is available for all editions of Microsoft SQL Server 2005. The Torn Page Repair restore can then be performed from the latest Full or Differential backup session of that database. If the Automatic Selection option is selected, all of the successive Transaction Log sessions are located, as they would for a Files-and-FileGroups restore. If a Differential session is selected, then the corresponding Full backup session will also be automatically selected. The database remains offline until the restore is complete.

Note: Microsoft recommends this only as an emergency measure. A Torn Page Repair can be used to return a damaged database to service when time is critical, but it is strongly recommended that you migrate the database to a new disk at the earliest opportunity to forestall the risk of further errors.

Torn Page Repair - Offline

This option requires the Enterprise Edition of Microsoft SQL Server 2005. A Transaction Log backup with the Do Not Truncate option is used to obtain the latest transaction information which might need to be applied to the damaged pages. A Database Consistency Check Before Backup with the Continue If DBCC Fails option is recommended to identify any damaged pages which have not yet been encountered, and forestall the possible need to repeat the process. You can then perform the Torn Page Repair restore from the latest Full or Differential backup session of that database. If the Automatic Selection option is selected, Automatic Selection will locate all of the successive Transaction Log sessions, as they would for a Files-and-FileGroups restore. If a Differential session is selected, then the corresponding Full backup session will also be automatically selected. The database remains online during the entire process and any tables which are not affected by the damaged pages will remain accessible.

Note: In some cases, you may need to perform an additional Transaction Log Backup with the Do Not Truncate option, and restore that backup without the Automatic Selection option, to fully reactivate the repaired tables. This usually occurs if such a backup was not taken at the start of the process.

For Torn Page Repair restores, the Recovery Completion State option is restricted to the Leave Database Online option. The Database Consistency Check Before Restore option is only enabled when using the Torn Page Repair – Online option, as this is the only time the database will be online during a restore. If a Database Consistency Check was not performed before the last Transaction Log backup, this option can be used to ensure that Microsoft SQL Server identifies any additional torn pages.

Note: Microsoft recommends this only as an emergency measure. A Torn Page Repair can be used to return a damaged database to service when time is critical, but it is strongly recommended that you migrate the database to a new disk at the earliest opportunity to forestall the risk of further errors.

Miscellaneous

Force restore over existing files or database

Enable this option to let Microsoft SQL Server overwrite files it does not recognize as part of the database it is restoring. Use this option only if you receive a message from Microsoft SQL Server prompting you to use the With Replace option. This option is equivalent to using the With Replace parameter of the restore command.

Restricted user access after restore

If this option is selected, then a restore to Original Location will overwrite the current ARCserve Database, rather than the database that was backed up to this session. This option is generally used to migrate the session and log information from one ARCserve Domain to another.

Keep replication settings

Instructs the restore operation to preserve replication settings when restoring a published database to a server other than the one on which it was created. This prevents Microsoft SQL Server from resetting the replication settings when it restores a database or log backup on a warm standby server and recovers the database. Use the Keep Replication Settings option when setting up replication to work with log shipping.

You cannot select this option when restoring a backup with the Leave database non-operational, but able to restore additional transaction logs option. Use this option only with the Leave database operational, no additional transaction logs can be restored option.

Use current ARCserve Database as original location

If this option is selected, then a restore to Original Location will overwrite the current ARCserve Database, rather than the database which was backed up to this session. This option is generally used to migrate the session and log information from one ARCserve Domain to another.

Preserve current ARCserve Domain Memberships

If this option is selected, then the current information about ARCserve Domains, such as the ARCserve Domain name, Primary Server identity and Member Server identities, will be retrieved from the destination database before the restore begins, and written back after the restore completes, preserving this information even after the restore. This option is enabled when the “Automatic Selection”, “Leave Database Operational” and “Use current ARCserve Database as original location” options are all selected, and is selected by default when it is enabled.

In this release, CA ARCserve Backup retains encryption information in the CA ARCserve Backup database. The encrypted information can include session passwords and user profile information, all of which is tied to a CA ARCserve Backup domain. When using this option, the agent determines if it can associate this information with a preserved CA ARCserve Backup domain from the overwritten database. If the restored database and the overwritten database contain the same domains, the associations will be re-established accordingly. If the restored database and the preserved domain list do not have domains in common, the agent will behave according to the table that follows. For any restored domains that the agent cannot map to one of the preserved domains, you will need to export the keys using the DumpDB utility on one of the CA ARCserve Backup primary servers or stand-alone servers that is using the database.

Restored ARCserve Database	Overwritten ARCserve Database	Agent Action	Manual Follow-up
One CA ARCserve Backup domain	One CA ARCserve Backup domain	<ul style="list-style-type: none"> ■ The CA ARCserve Backup domain key is transferred, and session passwords and user profiles are re-associated. ■ The server information from the restored CA ARCserve Backup database is not retained. 	You will be asked to provide the caroot password from the restored domain the first time you open the Manager Console after you restore the database. This finalizes the transfer of the CA ARCserve Backup domain key.
One CA ARCserve Backup domain	Two or more CA ARCserve Backup domains	<ul style="list-style-type: none"> ■ The CA ARCserve Backup domain key is propagated. ■ The session 	<ul style="list-style-type: none"> ■ You will be asked to provide the caroot password from the restored domain the first time you open the Manager Console, for

Restored ARCserve Database	Overwritten ARCserve Database	Agent Action	Manual Follow-up
		<p>passwords and user profiles are not re-associated.</p> <ul style="list-style-type: none"> ■ The server information from the restored CA ARCserve Backup database is retained. ■ A dollar sign ('\$') is appended to the domain name, the primary server name, and the individual server names of the servers listed in the restored data. 	<p>each CA ARCserve Backup domain, after you restore the database. This finalizes the migration of the CA ARCserve Backup domain key.</p> <ul style="list-style-type: none"> ■ You must manually export and import the session passwords using the DumpDB utility on the CA ARCserve Backup primary or stand-alone server that is to receive the keys. <p>Note: You must execute cstop and cstart on the primary server of each CA ARCserve Backup domain and finalize the key migration, before importing session passwords using the DumpDB utility.</p>
<p>Two or more CA ARCserve Backup domains</p>	<p>Any number of CA ARCserve Backup databases</p>	<ul style="list-style-type: none"> ■ The CA ARCserve Backup domain keys are not propagated. ■ The session keys and user profiles are not re-associated. ■ The server information from the restored CA ARCserve Backup database is retained. ■ A dollar sign ('\$') is appended to the domain name, the primary server 	<ul style="list-style-type: none"> ■ New domain keys will be created for the retained CA ARCserve Backup domains when the CA ARCserve Backup services are restarted on that domain's primary or stand-alone server. ■ You must manually export and import the session passwords using the DumpDB utility on the CA ARCserve Backup primary or stand-alone server that is to receive the keys. <p>Note: You must execute</p>

Restored ARCserve Database	Overwritten ARCserve Database	Agent Action	Manual Follow-up
		name, and the individual server names of the servers listed in the restored data.	cstop and cstart on the primary server of each CA ARCserve Backup domain before importing session passwords using the DumpDB utility.

Note: Before you run the DumpDB utility, you must execute cstop and cstart on all servers in each domain that uses the overwritten CA ARCserve Backup database.

For information about using the DumpDB utility, see the *Command Line Reference Guide*.

Log point in time restore

Stop before job mark

This option includes date and time fields in which you can set a specific date and time mark. The option recovers the database to the specified mark but does not include the transaction that contains the mark. If you do not check the After datetime check box, recovery stops at the first mark with the specified name. If you check the After datetime check box, recovery stops at the first mark with the specified name exactly at or after datetime.

Note: This option is available in Microsoft SQL Server 2000 and Microsoft SQL Server 2005 only.

Stop at log mark

This option includes date and time fields in which you can set a specific date and time mark. The option recovers the database to the specified mark, including the transaction that contains the mark. If you do not check the After datetime check box, recovery stops at the first mark with the specified name. If you check the After datetime check box, recovery stops at the first mark with the specified name exactly at or after datetime.

Note: This option is available in Microsoft SQL Server 2000 and Microsoft SQL Server 2005 only.

Stop at time

This option includes date and time fields in which you can enter a specific date and time. The option recovers the database to the specified date and time. This is the default option

Recovery Completion State

The following switches determine the condition of the database at the end of the restore job.

Leave database operational

Instructs the restore operation to roll back any uncommitted transactions. After the recovery process, the database is ready for use.

Note: If you use Automatic Selection, you do not have to choose any of the Recovery Completion State selections manually, because CA ARCserve Backup performs the selection of sessions and the necessary options automatically. If you do not choose Automatic Selection, you must follow Microsoft SQL Server rules regarding the restore flow. For more information, see Microsoft SQL Server documentation.

Leave database offline and able to restore differential

Instructs the restore operation not to roll back any uncommitted transactions and to leave the database in a state where it can accept additional Files-and-FileGroups, Differential, or Transaction Log restores. This is usually selected when performing manual restores.

Database Consistency Check

After restore

Enable this option to check the consistency of the database after the backup completes. To select this option, you must also choose Leave Database Operational. Selecting this option enables the following options.

Do not check indexes

Enable this option to check for consistency without checking indexes for user-defined tables.

Check only the physical consistency of the database

Enable this option to check the database for torn pages and common hardware failures. Additionally, it checks the integrity of the physical structure of the page and record headers, and the consistency between the page's object ID and index ID. This option bypasses the data validity tests normally performed in a standard database consistency check and examines only those related to physical integrity. Index checking is part of the physical integrity tests unless you specifically disable it by selecting Do not check indexes.

Continue Restore after Checksum Failure

Performs the restore even if consistency checking fails.

Agent Restore Options - SQL Instance DB Files As

The Database Files Options tab contains options and selections that control where you can restore your database.

Files or FileGroups

Choose the File or File Groups you wish to restore from the tree.

Restore Database Files As

Restore to Original Location

Lets you restore the database to its original location. Available at the Database level. Clears any changes to the drive letters, paths, and file names. You must click the Apply button after selecting this option for the change to take effect.

Restore to Original Location Except

Available at the Database, FileGroup and Transaction Log, and File levels. Applies the requested changes to the drive letter, paths and file names based on the location of the file when the backup was performed.

Move To Drive

Select the Move To Drive check box and enter a different drive letter in the field beside.

Move to Directory

Select the Move To Directory check box and enter a different directory path in the field beside.

Filename Pattern Change

Select the Filename Pattern Change check box, to change the filenames for the entire database, FileGroup, or Transaction Log. Enter a wildcard pattern that matches the names of the files you want to rename in the field below and enter the wildcard pattern that you want it to be renamed to in the to field.

For example, if you want to rename all the files that begin with Group as Members, enter Group* in the field and Member* in the to field.

Note: If you are using a wildcard pattern to rename files, and the pattern for the original filenames does not match with one or more of the files to which it would be applied, a yellow indicator will appear at the bottom of the dialog, and in the tree next to both the affected files and the object where the rule was applied.

Select the Rename File check box and enter a different file name, to rename a single file.

Click Apply for the changes to take effect.

Restore the CA ARCserve Backup Database (Different Domain)

This section describes how to restore the CA ARCserve Backup database and the database was backed up using an ARCserve server that resides in a different CA ARCserve Backup domain. You can restore the ARCserve database in the following scenarios:

- The ARCserve database is functional
- The ARCserve database is not functional and the instance hosting the ARCserve database is functional

In these scenarios you can restore the ARCserve database using the Backup Manager on the system that backed up the ARCserve database.

Important! You cannot restore the ARCserve database while there are jobs in progress. If a job tries to access the ARCserve database while the restore is in progress, the job will fail.

To restore the CA ARCserve Backup database that was backed up in a different CA ARCserve Backup domain

1. Stop all CA ARCserve Backup services running on the primary and the member servers in the domain using the cstop batch file.

Note: For more information, see [Stop and Start All CA ARCserve Backup Services](#) (see page 436).

2. Log in to the ARCserve domain containing the backup data for the database that you want to restore.

Open the Restore Manager window, click the Source tab, select the Restore by Tree method, expand the Windows Systems object, and browse to the primary server associated with the database that you want to restore.

Expand the server that you want to restore.

Based on the type of database that is running in your environment, select the following database objects:

Microsoft SQL Server 2005 Express

Expand the server object and select the following objects:

- CA ARCserve Backup Database object
- Microsoft SQL Server Disaster Recovery Elements

Note: If CA ARCserve Backup is installed in a cluster-aware environment, you must status the Microsoft SQL Server 2005 Express service in maintenance mode before you submit the restore job.

Microsoft SQL Server

Expand the server object, expand the Microsoft SQL Server object, and submit individual restore jobs for the following objects:

- System databases: [master], [msdb], and [model]
- asdb database object

3. Click the Options toolbar button.

The Global Options dialog opens.

4. Select the Operation tab, click the Disable Database Recording option, and click OK.

The database restore options are applied.

5. Click the Destination tab and select the Restore files to their original location option.

Important! If the CA ARCserve Backup database is a Microsoft SQL Server 2005 Express instance and CA ARCserve Backup is installed in a cluster-aware environment, you must place the SQL Server service in cluster maintenance mode before submitting the restore job.

Click the Start toolbar button.

The Submit Job dialog opens.

Note: If there are jobs in progress, CA ARCserve Backup prompts you to restore the ARCserve database to a different location. If you cannot restore the ARCserve database to a different location, allow all jobs in progress to complete, and then restore the ARCserve database.

6. Complete the fields on the Submit Job dialog and click OK.

After the restore job is complete, complete the following tasks:

- a. Start all services on the primary and member servers in the domain using the cstart command.

Note: For more information, see [Stop and Start All CA ARCserve Backup Services](#) (see page 436).

- b. Using the Merge utility, merge all backup media.
- c. Perform a full backup of the ARCserve database.

Be aware of the following behaviors:

- After you restore the CA ARCserve Backup database, the job history for the Database Protection Job will indicate that the job is incomplete and the Activity Log will indicate that the job is in progress with an Unknown status. This behavior occurs because the data for the Activity Log and the Database Protection Job is stored in the CA ARCserve Backup database and the data was incomplete while backup was in progress.

In addition, the status of the Database Protection Job (Done) will be the same as it was before you submitted the restore job. This behavior occurs because the Job Queue will obtain the status of the Database Protection Job from the job scripts rather than from the CA ARCserve Backup database.

- The first job that you run after you recover the CA ARCserve Backup database appears in the Job Status Manager with the same Job ID as the restore job for the CA ARCserve Backup database. This behavior occurs because the Job ID assigned to the CA ARCserve Backup database restore job is lost after you restore the CA ARCserve Backup database.
- CA ARCserve Backup may attempt to purge data that had already been purged from the staging device when you restore the CA ARCserve Backup database in a disk staging environment. You will receive a warning message, however, the purge job will complete successfully.

Restore the CA ARCserve Backup Database (Same Domain)

This section describes how to restore the CA ARCserve Backup database and the database was backed up using an ARCserve server that resides in the CA ARCserve Backup domain that is using the database. You can restore the ARCserve database in the following scenarios:

- The ARCserve database is functional
- The ARCserve database is not functional and the instance hosting the ARCserve database is functional

In these scenarios you can restore the ARCserve database using the Backup Manager or the `ca_recoverdb` utility on the system that backed up the ARCserve database.

Note: For more information about using the `ca_recoverdb` utility, see the *Command Line Reference Guide*.

Important! You cannot restore the ARCserve database while there are jobs in progress. If a job tries to access the ARCserve database while the restore is in progress, the job will fail.

To restore the CA ARCserve Backup database that was backed up in the domain that is using the database

1. Open the Restore Manager window, click the Source tab, select the Restore by Tree method, expand the Windows Systems object, and browse to the primary server associated with the database that you want to restore.

Based on the type of database that is running in your environment, select the following database objects:

Microsoft SQL Server 2005 Express

Expand the server object and select the CA ARCserve Backup Database object.

Note: If CA ARCserve Backup is installed in a cluster-aware environment, you must status the Microsoft SQL Server 2005 Express service in maintenance mode before you submit the restore job.

Microsoft SQL Server

Expand the server object, expand the Microsoft SQL Server object, and submit individual restore jobs for the following objects:

- System databases: [master], [msdb], and [model]
- asdb database object

Note: CA ARCserve Backup does not support using the Restore by Tree and Restore by Session methods to restore Disaster Recovery Elements when the Disaster Recovery Elements and the CA ARCserve Backup database are stored in the same SQL Server instance. In this scenario, you must use the ca_recoverdb Command Line utility to restore CA ARCserve Backup database. In the Restore by Session view, the Disaster Recovery Elements will have a volume name of "sqldr@" followed by the instance name. For a default instance of Microsoft SQL Server, the instance name will appear as "MSSQLSERVER", regardless of the version Microsoft SQL Server.

2. Click the Options toolbar button.
The Global Options dialog opens.
3. Select the Operation tab, click the Disable Database Recording option, and click OK.

The database restore options are applied.

4. Click the Destination tab and select the Restore files to their original location option.

Important! If the CA ARCserve Backup database is a Microsoft SQL Server 2005 Express instance and CA ARCserve Backup is installed in a cluster-aware environment, you must place the SQL Server service in cluster maintenance mode before submitting the restore job.

Click the Start toolbar button.

The Submit Job dialog opens.

Note: If there are jobs in progress, CA ARCserve Backup prompts you to restore the ARCserve database to a different location. If you cannot restore the ARCserve database to a different location, allow all jobs in progress to complete, and then submit the restore job.

5. Complete the fields on the Submit Job dialog and click OK.
6. After the restore job is complete, complete the following tasks:
 - a. Close and open the Manager Console.
 - b. Using the Merge utility, merge all backup media.
 - c. Perform a full backup of the CA ARCserve Backup database.

Be aware of the following behaviors:

- After you restore the CA ARCserve Backup database, the job history for the Database Protection Job will indicate that the job is incomplete and the Activity Log will indicate that the job is in progress with an Unknown status. This behavior occurs because the data for the Activity Log and the Database Protection Job is stored in the CA ARCserve Backup database and the data was incomplete while backup was in progress.

In addition, the status of the Database Protection Job (Done) will be the same as it was before you submitted the restore job. This behavior occurs because the Job Queue will obtain the status of the Database Protection Job from the job scripts rather than from the CA ARCserve Backup database.

- The first job that you run after you recover the CA ARCserve Backup database appears in the Job Status Manager with the same Job ID as the restore job for the CA ARCserve Backup database. This behavior occurs because the Job ID assigned to the CA ARCserve Backup database restore job is lost after you restore the CA ARCserve Backup database.
- CA ARCserve Backup may attempt to purge data that had already been purged from the staging device when you restore the CA ARCserve Backup database in a disk staging environment. You will receive a warning message, however, the purge job will complete successfully.

How to Recover the ARCserve Database When the SQL Server Instance Hosting the ARCserve Database is Not Functional

A typical disaster recovery scenario consists of the following steps:

1. Reinstall Windows, if necessary.
2. Reinstall CA ARCserve Backup, if necessary.
3. Reinstall the Agent for Microsoft SQL Server and the Client Agent for Windows, if necessary. (The Client Agent is needed to restore Microsoft SQL Server Disaster Recovery Elements.)
4. Perform one of the following steps as appropriate:
 - If you have a Microsoft SQL Server Disaster Recovery Elements session, restore it.
 - If an offline backup exists, restore it.
 - If you do not have an offline backup or a Disaster Recovery Elements session, and you have the Microsoft SQL rebuildm.exe utility, use the utility to recreate the master and model database. For more information, see the Microsoft documentation.
 - If an offline backup or Disaster Recovery Elements backup do not exist and you do not have the Microsoft SQL rebuildm.exe utility, reinstall the Microsoft SQL Server or MSDE-based application.
5. Restore the [master] database.
6. Restart Microsoft SQL Server in normal, multi-user mode.
7. Restore the [msdb] database.
8. Restore all other databases and transaction logs, except the replication database.
9. If replication is being used, restore the replication database.

Restore the CA ARCserve Backup Database Using the ca_recoverdb Command

Each time you run a backup job, CA ARCserve Backup records information in its databases about the machines, directories, and files that have been backed up, and the media that was used. This allows you to locate files whenever you need to restore them. The database recovery command (ca_recoverdb) is a self-protection feature that allows you to recover a CA ARCserve Backup database if it is lost and was backed up by the CA ARCserve Backup domain that is using the database.

The `ca_recoverdb` utility invokes the `ca_restore` commands to implement the database recovery function. The `ca_recoverdb` utility automatically determines if the CA ARCserve Backup database is a SQL Server database or SQL Server 2005 Express Edition instance and provides the appropriate parameters for the `ca_restore` command.

When a CA ARCserve Backup server is configured as cluster-aware, all critical ARCserve base-related services (not agent-related services) will be monitored by the applicable cluster service (MSCS or NEC CLUSTERPRO). If an ARCserve base-related service fails or needs to be shut down, the cluster service automatically tries to restart it or trigger a failover if the restart attempt fails. To run this task, you must stop ARCserve services. However, in a cluster-aware environment, you must first manually stop the cluster service from continuing to monitor the service and attempting an automatic restart or failover. For information about how to stop HA service monitoring by the Cluster Service, see the appendix Cluster Support Using CA ARCserve Backup.

Be aware of the following behaviors:

- The first job that you run after you recover the CA ARCserve Backup database appears in the Job Status Manager with the same Job ID as the restore job for the CA ARCserve Backup database. CA ARCserve Backup demonstrates this behavior because the Job ID assigned to the CA ARCserve Backup database restore job is lost after you restore the CA ARCserve Backup database.
- When restoring the CA ARCserve Backup database in a disk staging environment, CA ARCserve Backup may attempt to purge data that had already been purged from the staging device. You will receive a warning message, but note that the purge job will complete successfully.

Syntax

The `ca_recoverdb` command line syntax is formatted as follows:

```
ca_recoverdb [ -cahost <hostname> ]  
  
    [-i [n]]  
    -username <username> [-password <password>]  
    [-dbusername <database username> [-dbpassword <database password> ] ] [-  
    sessionpassword [session password] -session password [session password]...]  
    [-waitForjobstatus <polling interval>]
```

Options

The `ca_recoverdb` provides various options for recovering a lost CA ARCserve Backup database.

The `ca_recoverdb` command includes the following options:

cahost <hostname>

Redirects default host from the backup log to the host specified by `cahost`.

For example:

HostA - The default host that existed in backup log, which will be used in `ca_restore`.

HostB - The host that you specify.

In these examples, if you do not specify the `cahost` switch, then the `ca_restore` command invoked by the `ca_recoverdb` utility will look as follows:

```
ca_restore -cahost HostA
```

If you do specify the `cahost` switch with the parameter HostB, then the `ca_restore` command invoked by the `ca_recoverdb` utility will look as follows:

```
ca_restore -cahost HostB
```

-i [n]

Specifies to use the interactive mode. If you include this switch, it allows you to specify a point in time from which to perform the CA ARCserve Backup database recovery by selecting which backup to use as a baseline. When the interactive mode is invoked, the `ca_recoverdb` displays the list of CA ARCserve Backup sequences for which it has log files. Each of the log files start with a Full database backup, and contains all of the other backups which are dependent on that Full backup to be restored (the Full backup is root of the "dependency chain" for those sessions).

The parameter *n* is used to specify the number of latest backup log sets (dependency chains) that you want to select from. The range of values for *n* is 1 to 99, and the default value is 10.

When you select a Full backup sequence, you will then be prompted to select which session to use as the restore point. After you select a session, the `ca_recoverdb` utility will determine the dependency chain for that sequence, and use `ca_restore` to submit a restore job for each session.

If you do not include the `-i` switch, the `ca_recoverdb` utility automatically uses the most recent backup as the specified selection, and builds the dependency chain for that session. This is helpful if you just want to recover to the latest point in time backup. However, if the most recent backup is lost or damaged, you can use the interactive mode to restore from an older session, and then merge tapes to re-integrate the latest information.

-username <username> [-password <password>]

Specifies the authenticating information for the database agent that will perform the actual recovery job. If you do not include the password option, it will default to no password required.

-dbusername <database username> [-dbpassword <database password>]

Specifies the authenticating information for the database. If you do not include the database username and corresponding database password, it will default to "dbusername" and "dbpassword" for authenticating purposes.

[-sessionpassword [session password] -sessionpassword [session password] ...]

Specifies the authenticating information for the sessions being set authenticating password.

[-waitForJobStatus <polling interval>]

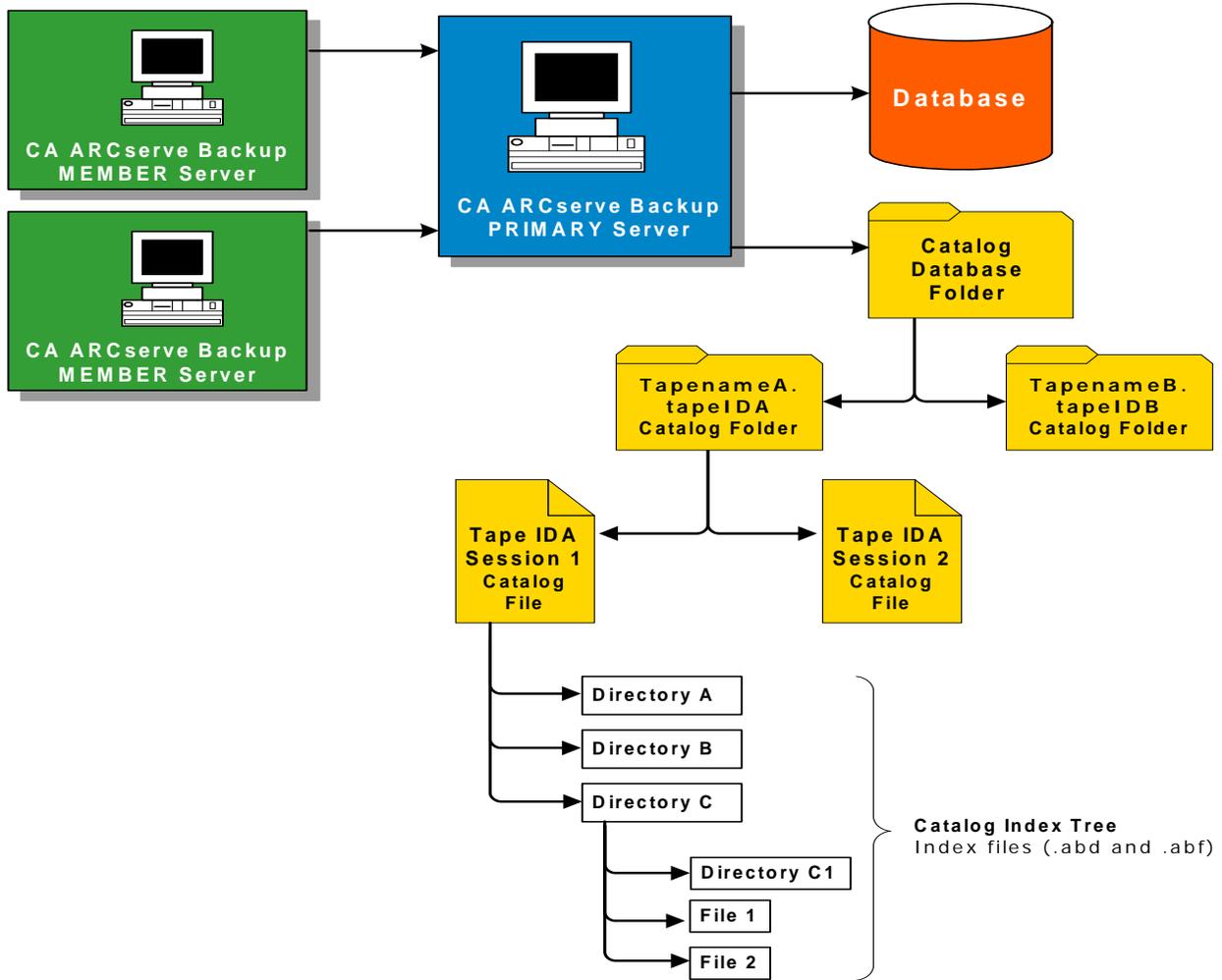
Specifies the time interval (in seconds) that ca_recoverdb will wait until the job is completed and then exit with a return code that indicates the success or fail outcome of the job.

The <polling interval> value defines how often (in seconds) that the ca_recoverdb utility checks the job status with the Queue services. The default polling interval is 60 seconds.

How the Catalog Database Works

As the amount of information and data that you create grows larger, the backup jobs that are used to ensure their security also grows larger. As a result, the amount of time needed to parse or analyze this information could become very time-consuming and have a negative impact on the performance and scalability of your system.

To resolve this problem, whenever CA ARCserve Backup performs a backup, all the job, session, and media information is loaded into a database, while a separate catalog file is also created under the catalog database folder with just the pertinent description information about each session. In addition, two corresponding catalog index files (.abd and .abf) are also generated displaying the index tree structure of the directories and files within the catalog file. These catalog index files are retained on the disk and can be used to quickly browse the content of the session in the catalog file to locate the information when needed.



More information:

[Configure the Catalog Database](#) (see page 600)

Catalog Browsing

Whenever you need to check for a directory or file to be restored, or to get the version history, or to just perform a search, instead of querying the content of the entire database, CA ARCserve Backup performs the query on just the catalog files with the help of the catalog index. If this catalog browsing finds the details in the catalog database folder for a specific session, it will not look in the CA ARCserve Backup database. However, if it does not find it, it will then attempt to look in the CA ARCserve Backup database again. If it still does not find the details of the session in both the catalog database folder and the CA ARCserve Backup database, it will then prompt you to select whether or not you want to merge the session again so that the merge process can recreate the catalog file into the catalog database folder or can regenerate the details from the tape session contents into the CA ARCserve Backup database.

Note: All application agent sessions except for Microsoft Exchange, such as SQL Server, Informix, Oracle, Microsoft SharePoint, Lotus Notes etc, do not support catalog browsing and the details from those sessions will be inserted into the CA ARCserve Backup database.

Catalog Database Pruning

Whenever you use CA ARCserve Backup to back up information and data, the amount of description information (catalog files and index files) stored in the catalog database folder increases. Without any controls, in time the size of the catalog database folder would increase, eventually occupying the entire backup disk, and resulting in backup errors due to insufficient free disk space.

To resolve this problem, CA ARCserve Backup allows you to specify a catalog database pruning threshold. The pruning threshold (or Minimum disk free space threshold) setting is accessible from the Configuration dialog of the Server Admin Manager. The selectable range of this threshold is from 1% to 99%, with the default value set to 10%, and is based on the percentage value of the detected free disk space.

Note: CA ARCserve Backup periodically checks the free disk space percentage on the volume where the catalog database folder is located. If the detected free space is lower than the specified percentage, a warning message will be sent to the activity log and it would automatically begin to delete catalog database files (minimum of 7 days old and starting with the oldest first) from the disk until the detected free space percentage is greater than the threshold setting.

How a Centralized Catalog Database Works

When operating in a centralized management environment (a primary server and one or more member server), CA ARCserve Backup centralizes all catalog files into the primary server. As a result, the catalog database files created on a member server during a backup job will be transferred (when the backup is complete) to the catalog database folder located on the associated primary server. In this way, the performance of merging and browsing catalog files that are always local to the primary server will be significantly improved and the maintenance of catalog database, such as pruning and backing up tasks will be simplified and be done only from the primary server.

The CA ARCserve Backup centralized catalog database helps you manage enterprise-level, multi-server environments. You can browse media information or generate reports for multiple servers at the same time. The members servers in your network update the central CA ARCserve Backup catalog database with media session information and details from their own database. The central catalog database is set up locally on a machine that manages the centralized catalog database. Media session information for all of the CA ARCserve Backup machines in your enterprise is contained there.

Configure the Catalog Database

You can configure the catalog database options to customize the location and performance of the database and the associated centralized catalog.

To configure the catalog database

1. Open the Server Admin Manager and click the Configuration toolbar button.

The Configuration dialog appears.

2. Select the Database Engine tab.

The Database Engine dialog appears displaying the catalog database options at the bottom of the dialog.

3. Complete the following fields:

- **Catalog database folder--**Lets you define the where you will store the catalog database. The catalog database folder will contain all the associated catalog files and catalog index files. You can click the ... (ellipsis) button to browse and select a different location for the catalog database folder.

By default, the catalog database folder will be stored in on the primary of stand-alone server in the following directory:

C:\Program Files\CA\ARCserve Backup\CATALOG.DB\

Note: You can only modify the catalog database folder from the Primary Server.

- **Compress catalog transfer on the following member servers--** Lets CA ARCserve Backup compress catalog information when the data is transferred from a member server to the primary server.

If the primary server has any associated member servers, the Compress catalog transfer on the following member servers field will be enabled, displaying the names of the member servers.

By default, this option is disabled. With this option disabled, CA ARCserve Backup will not compress the catalog information when it is transferred from the member server to the primary server.

- **Minimum disk free space threshold--**Lets you specify the minimum percentage of free disk space when CA ARCserve Backup deletes catalog files.

Default value: 10 %

Range: 1% to 99%

Note: CA ARCserve Backup periodically checks the free disk space percentage on the volume where the catalog database folder is located. If the detected free space is lower than the specified percentage, a warning message will be sent to the activity log and it would automatically begin to delete catalog database files (minimum of 7 days old and starting with the oldest first) from the disk until the detected free space percentage is greater than the threshold setting.

Example: If the detected free space is lower than the 10%, a warning message is sent to the activity log and it would automatically begin to delete catalog database files (minimum of 7 days old and starting with the oldest first) from the disk until the detected free space percentage is greater than 10%.

4. Click OK.

The Catalog Database options are applied.

Move the CA ARCserve Backup Catalog Database to a Different Location

This topic describes how to move the CA ARCserve Backup catalog database to a different new location. You may wish to move the catalog database to a different location when you experience any of the conditions that follow:

- The overall size of the catalog database increases significantly. For example, the size of the catalog database increased from one GB (gigabyte) to 30 GBs.
- There is a noticeable time lag when you retrieve restore data.
- More than eight hours are required to complete the Database Protection Job.
- More than four hours are required to complete the Database Pruning Job.
- The catalog database is consuming a significant amount of disk space on the C:\ drive, which affects the amount disk space required for the Windows pagefile.sys file.
- Microsoft SQL Server performance has deteriorated due to increased CA ARCserve Backup transactions and overhead, and you do not have a dedicated SQL Server system.
- You cannot export the CA ARCserve Backup database to a flat file using Microsoft SQL Server utilities due to the overall size of the database.
- You wish to modify your current CA ARCserve Backup database configuration such that summary information is recorded in the CA ARCserve Backup database and detail information is recorded in the catalog database.

Best Practices

Before you move the CA ARCserve Backup catalog database to a different location, consider the following best practices:

- By default, the catalog database is installed in the directory that follows:

C:\Program Files or Program Files(x86)\CA\ARCserve Backup\CATALOG.DB

If you must move the catalog database, the best practice is to move the catalog database to a location resides or communicates locally with the CA ARCserve Backup server.

Note: You should not move the catalog database to a remote disk that resides on a Network Attached Storage (NAS) device or a mapped network drive. These locations may require authentication to access the devices.

- The application used for the CA ARCserve Backup is not relevant to the location of the catalog database. However, consideration should be given for the protocols used for communication:
 - **ODBC/RPC**--The communication protocol used between member servers and the catalog database on the primary server and the communication protocol used between the catalog database on the primary server and Microsoft SQL Server.
- For configurations where the catalog database resides on a SAN device, you should consider installing an additional SCSI controller or HBA card on the CA ARCserve Backup server to accommodate communication between the CA ARCserve Backup server and the storage device.

Note: The steps that follow apply to CA ARCserve Backup servers using Microsoft SQL Server or Microsoft SQL Server 2005 Express Edition to host the CA ARCserve Backup database.

To move the CA ARCserve Backup catalog database to a different location

1. Complete the following tasks:
 - Ensure that all jobs, including the Database Protection Job and the Database Pruning Job, are in a Hold state.
 - Ensure that the CA ARCserve Backup Manager Console is closed on all servers in the CA ARCserve Backup domain, with the exception of the primary or stand-alone server.

2. If there are member servers in the CA ARCserve Backup domain, execute Cstop on all member servers to stop all CA ARCserve Backup services.

Note: For information about using Cstop, see [Stop and Start All CA ARCserve Backup Services Using Batch Files](#) (see page 436).

3. Execute Cstop on the CA ARCserve Backup primary or stand-alone server to stop all CA ARCserve Backup services.

4. After all services stop, bring the new location for the catalog database online.

5. In the new location for the catalog database, create the the path.

For example:

F:\ARCserve\catalog.db

6. Copy all folders from the original location to the new location.

For example:

Original location

C:\Program Files\CA\ARCserve Backup\CATALOG.DB

New location

F:\ARCserve\catalog.db

7. After you copy the Catalog files to the new location, open the Server Admin and click the CA ARCserve Backup primary server or stand-alone server.

Click Configuration on the toolbar.

The Configuration dialog opens.

8. Click the Database Engine tab.

In the Catalog database folder field, specify the new path to the catalog database.

For example:

F:\ARCserve\catalog.db

Optionally, you can click the ellipsis to browse to the new location for the catalog database.

Click OK.

The Configuration dialog closes.

9. Execute Cstart on the primary or stand-alone CA ARCserve Backup server to restart all CA ARCserve Backup services.

Note: For information about using Cstart, see [Stop and Start All CA ARCserve Backup Services Using Batch Files](#) (see page 436).

Allow several minutes to elapse to ensure that all CA ARCserve Backup services start.

10. Submit a simple backup job from the primary or stand-alone server.

11. After the simple backup job is complete, submit a simple restore job from the primary or stand-alone server.

12. After the simple backup and restore jobs on the primary or stand-alone server are complete, ensure that CA ARCserve Backup is writing job summary and detail information to the new location for the catalog database.
13. If there are members servers in the CA ARCserve Backup domain, execute Cstart on one of the member servers. Allow several minutes to elapse to ensure that all CA ARCserve Backup services start.
14. Submit a simple backup job from a member server.
15. After the simple backup job is complete, submit a simple restore job from the member server.
16. After the simple backup and restore jobs on the member server are complete, ensure that CA ARCserve Backup is writing job summary and detail information to the new location for the catalog database on the primary server.
17. Execute Cstart on the remaining member servers in the CA ARCserve Backup domain. You should allow five minutes to elapse between Cstart executions to minimize SAN, LAN, and CA ARCserve Backup RPC updates.

Note: After you move the catalog database to a different location, restore job and summary and detail data from the same backup job may not reflect in the catalog database. To remedy this problem, run Repair Database Connection using the Server Configuration Wizard. For more information, see [Repair the ARCserve Database Connection on a Primary Server](#) (see page 525).

Using Microsoft SQL Server as the CA ARCserve Backup Database

The following section describe how to plan, configure, and deploy Microsoft SQL Server as the CA ARCserve Backup database.

Microsoft SQL Server Database Considerations

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

- If you are upgrading to this release and currently running Microsoft SQL Server for the CA ARCserve Backup database, you must continue using Microsoft SQL Server for the CA ARCserve Backup database.
- CA ARCserve Backup does not support using Microsoft SQL Server 7.0 for the CA ARCserve Backup database.

- By default, CA ARCserve Backup creates the CA ARCserve Backup database (ASDB) using a simple recovery model. You should retain this model for proper operation.
- Microsoft SQL Server supports local and remote communication. This capability lets you configure the CA ARCserve Backup database to run locally or remotely to your CA ARCserve Backup server.

Note: For more information, see [Remote Database Considerations](#) (see page 607).

- By default, CA ARCserve Backup stores information about the backed up files and directories in the Catalog Database. This behavior causes the Catalog Database to grow in size at a faster rate than the CA ARCserve Backup database. Given this behavior and the needs of your organization, you should plan to have a sufficient amount of free disk space to support the growth of the Catalog Database.
- If you are backing up operating systems that support case-sensitive naming conventions, you should create the SQL instance that will contain the CA ARCserve Backup 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 when prompted for the CA ARCserve Backup Database (SQL) System Account during installation of CA ARCserve Backup with Microsoft SQL support.

- Set the database security mode to SQL security in the SQL Enterprise Manager. This applies when using SQL security as the authentication mode and the systems that you want to back up reside inside or outside the CA ARCserve Backup domain.
- If you specify Microsoft SQL 2000 or Microsoft SQL 2005 as the CA ARCserve Backup database during setup, you can use Windows authentication or SQL authentication to communicate with the Microsoft SQL database.
- If the Microsoft SQL Server account is changed, you must make the corresponding changes using the Server Admin.
- The CA ARCserve Backup Database Engine periodically polls the status of the Microsoft SQL Server database. If Microsoft SQL Server does not respond in a timely fashion, the Database Engine assumes that the Microsoft SQL Server is unavailable and shuts down (red light). To avoid this situation, you can set the registry key to an appropriately longer value to increase the wait time for CA ARCserve Backup Database Engine, as follows:

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

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

Remote Database Considerations

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

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

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

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

Note: For more information, see [How to Enable TCP/IP Communication on Microsoft SQL Server Databases](#) (see page 609).

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

Specify ODBC Communication for Remote Database Configurations

If you have another CA ARCserve Backup server running that uses Microsoft SQL as its database, you can redirect the local database to the remote machine. CA ARCserve Backup can use ODBC to connect to the Microsoft SQL server. You can direct the ODBC data source to another server if the server has SQL installed and the CA ARCserve Backup SQL database is properly set up. You also need to make sure the local server user is authenticated in the remote server.

To specify ODBC communication for remote database configurations

1. Open the Windows Control Panel, select Administrative Tools, Data Sources (ODBC), and System DSN.
2. Add a System Data Source labeled as follows:
Name: ASNT
Server: MachineName\InstanceName
3. Follow the on-screen instructions to test and complete the configuration.

How to Calculate the Number of Required SQL Connections

For each job that you run, you need two SQL connections. Be sure that you have set enough connections (or licenses) in your SQL server. To determine your default SQL connections, select Server and SQL server from the SQL ARCserve Manager. When you browse from the Configuration tab, you can see the user connections. Set these values to the appropriate user setting. If an error message appears, for example, "Cannot Update Record" or "Failed to Login," you may have run out of connections. You should increase the open object to 2000.

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

If you are hosting the ARCserve database instance using Microsoft SQL Server 2000, Microsoft SQL Server 2005, or Microsoft SQL Server 2008, and the CA ARCserve Backup database will reside on a remote system, the installation wizard may not be able to communicate with the database on the remote system.

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

- **Microsoft SQL Server 2000**--To enable TCP/IP communication on Microsoft SQL Server 2000 systems, run the SQL Server Network utility and ensure that TCP/IP appears in the Enabled Protocols. If TCP/IP does not appear in the Enabled Protocols list, add TCP/IP to the list and click OK. To apply TCP/IP communication, restart all Microsoft SQL Server services.
- **Microsoft SQL Server 2005 and Microsoft SQL Server 2008**--To enable TCP/IP communication on Microsoft SQL Server 2005 and Microsoft SQL Server 2008 systems, run the SQL Server Configuration Manager and enable TCP/IP communication for the SQL Server instance. To apply TCP/IP communication, restart all Microsoft SQL Server services.

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

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 a CA ARCserve Backup Database Application

The following sections describe how to configure Microsoft SQL Server and Microsoft SQL Server 2005 Express as the CA ARCserve Backup underlying database.

Configure Microsoft SQL Server as the CA ARCserve Backup Database

Using the Server Configuration Wizard, you can configure Microsoft SQL Server as the CA ARCserve Backup database.

Before you configure Microsoft SQL Server as the CA ARCserve Backup database, the following considerations apply:

- Microsoft SQL Server must be installed on the system hosting the CA ARCserve Backup database before you start this task.
- After you configure CA ARCserve Backup to use Microsoft SQL Server as the ARCserve database, the Server Configuration Wizard opens a command utility labeled `exptosql.exe` that migrates the core and detail tables from the Microsoft SQL Server 2005 Express database to the newly configured Microsoft SQL Server database.
- You can use this procedure to move the CA ARCserve Backup Microsoft SQL Server database to a different server.

Note: For more information about using Microsoft SQL Server as the CA ARCserve Backup database, see [Using Microsoft SQL Server as the CA ARCserve Backup Database](#) (see page 605).

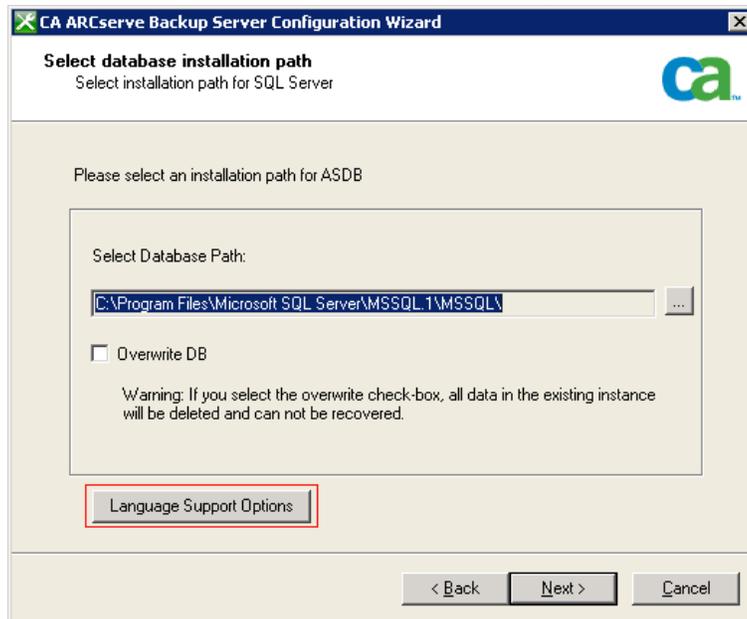
To configure Microsoft SQL Server as the CA ARCserve Backup database

1. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

2. Click the Select database option and click Next.
3. Follow the on-screen instructions to complete the configuration.

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



4. After the configuration is complete, the Server Configuration Wizard opens a command line window, starts `exptosql.exe`, and migrates the SQL Server 2005 Express core and detail tables to the new SQL Server database.

If `exptosql.exe` does not start, open a command line window and start `exptosql.exe`.

Note: By default, `exptosql.exe` is installed in the following directory:

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

Execute the following commands:

- a. **exptosql.exe core**

This is a required step. The `core` argument lets you migrate the core tables from the SQL Server 2005 Express database to the SQL Server database.

Important! You must execute this command immediately after the SQL Server configuration is complete.

- b. **exptosql.exe detail**

This is an optional step. The `detail` argument lets you migrate the detail tables from the SQL Server 2005 Express database to the SQL Server database. You can execute this command, at any time, after the core migration process is complete.

Note: Depending on the size of the SQL Server 2005 Express database, the detail table migration process can require a significant amount of time to complete.

Move the CA ARCserve Backup Database to a Different System or Instance

Use the Server Configuration Wizard to move the CA ARCserve Backup database to a different system or instance.

Note: This option only applies to Microsoft SQL Server installations.

Before you move the CA ARCserve Backup database to a different system or instance, be aware of the following considerations:

- The Server Configuration Wizard lets you change your current Microsoft SQL Server configuration to the following types of configurations:
 - Cluster-aware
 - Remote
 - Local
- To access the new SQL Server installation, you must specify a method of authentication. You can use one of the following authentication methods:
 - Windows security
 - SQL Server security
- For remote SQL Server installations that use SQL Server authentication, you must provide the Login ID and Password for the Remote Server Administrator Account.

To move the CA ARCserve Backup database to a different system or instance

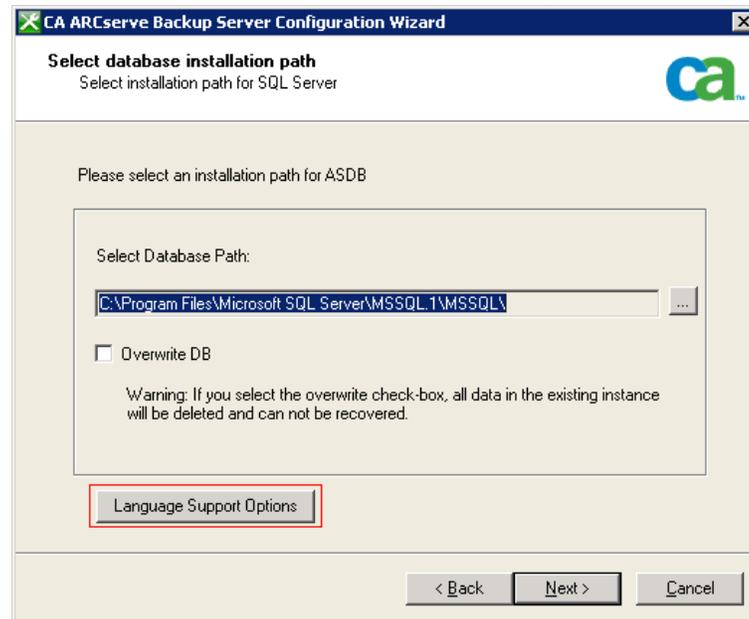
1. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

2. Select the Select Database option and click Next.

Follow the on-screen instructions to complete the configuration.

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



After the configuration is complete, you must install the CA ARCserve Backup database protection agent on the system hosting the SQL Server database.

3. To install the ARCserve database protection agent, do **one** of the following:
 - If the SQL Server database is installed on the CA ARCserve Backup primary server, open Windows Explorer and browse to the following directory:
C:\Program Files\CA\ARCserve Backup\Packages\ASDBSQLAgent
 - If the SQL server database is not installed on the CA ARCserve Backup primary server, open Windows Explorer and browse to the following directory:
C:\Program Files\CA\ARCserve Backup\Packages\ASDBSQLAgent
Copy the contents of the ASDBSQLAgent directory to any location on the system hosting the SQL Server database.
4. In the ASDBSQLAgent directory, double-click the following file:
SQLAgentRmtInst.exe
The ARCserve Backup Agent for SQL Setup dialog appears.
5. Complete the following fields, as required, for your installation:
 - SQL Instance Name
Specify the name of the SQL instance that you want to protect.
 - Auth Mode
Specify the authentication mode that CA ARCserve Backup will use to communicate with and protect the database.
If you specify SQL Authentication as the authentication mode, complete the following fields:
 - SQL SA Name
Specify the SQL system account name.
 - SQL SA Password
Specify the SQL system account password.
6. Click Install and follow the on-screen instructions to complete the installation.

Configure Microsoft SQL Server 2005 Express as the CA ARCserve Backup Database

Using the Server Configuration Wizard, you can configure Microsoft SQL Server 2005 Express as the CA ARCserve Backup database.

Before you configure Microsoft SQL Server 2005 Express as the CA ARCserve Backup database, be aware of the following considerations and limitations:

- To deploy Microsoft SQL Server 2005 Express in your environment, Microsoft .NET Framework 2.0 and Microsoft Data Access Components (MDAC) 2.8 Service Pack 2 must be installed on the primary server. If the Server Configuration Wizard does not detect either of these applications, the wizard installs them for you.
- Microsoft SQL Server 2005 Express does not support remote installations. You must install the ARCserve database on the CA ARCserve Backup primary server.
- You cannot migrate database information from a Microsoft SQL Server database installation to a Microsoft SQL Server 2005 Express database installation.
- Microsoft SQL Server 2005 Express Edition is not supported on Windows IA (Intel Itanium) 64-bit operating systems.

To configure Microsoft SQL Server 2005 Express as the CA ARCserve Backup database

1. From the Windows Start menu, click Start, select All Programs, CA, ARCserve Backup, and click Server Configuration Wizard.

The Server Configuration Wizard opens.

2. Click the **Select Database** option and then click **Next**.
3. Follow the on-screen instructions to complete the configuration.

Note: If you protect data that contains Unicode-based characters from East Asian languages (for example, JIS2004) you must enable SQL collation to ensure that you can search and sort the data. To do this, click Language Support Options on the SQL Server Express Instance dialog and follow the on-screen instructions to complete the configuration.

CA ARCserve Backup Logs and Reports

CA ARCserve Backup provides the following options for displaying logs and reports:

- Activity Log--Logs all CA ARCserve Backup activity.
- Tape Log--Logs all media activity (for debugging purposes only)
- Job Logs--Logs activity related to a specific job.
- Reports Manager--Generates reports from the CA ARCserve Backup database for viewing or printing.
- [The Unicenter Monitoring Agent](#) (see page 631)--Starts and stops services, monitors the status of the CA ARCserve Backup processes and tape, and reports on the failure of backup jobs.

Activity Log Data

The Activity Log contains comprehensive information about the operations performed by CA ARCserve Backup. It provides an audit trail of all CA ARCserve Backup activity (including group activities) for every job that is run. You can scan this log every day to see if any errors have occurred. You can also use it to find out a session number in case you need to restore a specific session. The log is located on the upper right corner of the Job Status Manager.

The Activity Log has an organize feature which allows you to sort the log using filters, message grouping, or message post date. For further information on the Activity Log, see the chapter "Customizing Jobs."

Tape Log

The Tape Log contains messages sent by the tape drives to CA ARCserve Backup. This log is not generated during normal operation. It is designed for debugging purposes only. To enable the Tape Log, use the Server Admin Configuration menu.

Note: In a cross-platform environment, the Tape Log does not display information for non-Windows servers. Only Windows server Tape Engine information is available for viewing in the GUI.

Job Log

A Job Log is generated for each job that is run by CA ARCserve Backup. You can specify the level of detail in the log by choosing the log options before you submit the job. See the online help for how to configure and view the log report for a job. For further information on the job log, see the chapter "Customizing Jobs."

Report Manager

The Report Manager provides you with a variety of reports based on the backup activity stored in the CA ARCserve Backup database. You can preview a report, print to a printer or file, as well as schedule when to generate a report.

Generate Reports Using Report Manager

The Report Manager lets you generate reports about CA ARCserve Backup activities.

You can generate reports that Run Now from primary servers, stand-alone servers, and member servers. You can schedule reports to run at a specific time on primary servers and stand-alone servers. If you schedule a report from a member server, the report will run from the primary server, display in the Manager Console on the primary server, and will be stored in the <ARCSERVE_HOME>/Reports directory.

Report Manager Considerations

- You can view all Create now-based reports in the Report Manager window or a browser application, such as Internet Explorer.
- You must view all Schedule-based reports in the Report Manager window.
- You must save all reports that you generate in the default storage location.

To generate reports using Report Manager

1. From the Monitor & Reports menu in the Navigation Bar on the home page, click Report.

The Report Manager opens and a collapsible tree that provides an expandable view of reports in various categories appears.

2. On the Report Categories view, select a report template from the list.

The Report template list appears on the right pane.

- Select and right-click the report that you want to generate. From the pop-up menu, specify one of the following options:

Schedule

Lets you schedule a report to run at a specific time.

When you specify this option, the Schedule Report dialog opens. On the Schedule Report dialog, follow the prompts and complete the required fields to schedule the report.

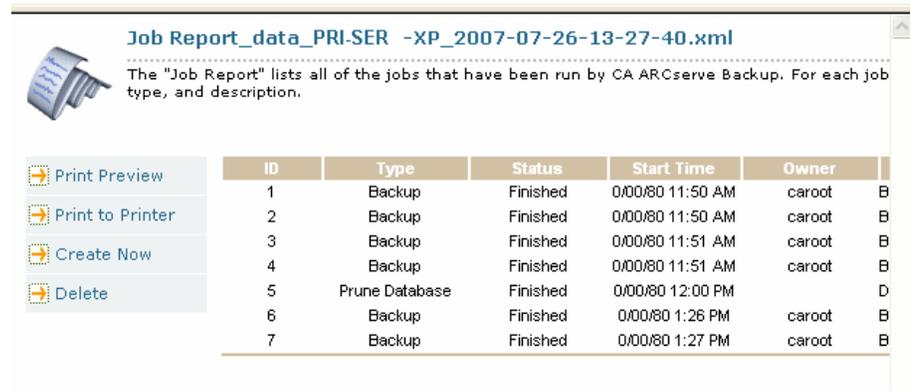
Create now

Lets you generate a report that runs now.

When you specify this option, the Create Report dialog opens. On the Create Report dialog, follow the prompts and complete the required fields to create the report now.

After CA ARCserve Backup creates the report, you can view the report results on the Report Content view pane as illustrated by the following graphic.

Job Report_data_PRI-SER-XP_2007-07-26-11-48-22.xml
 Job Report_data_PRI-SER-XP_2007-07-26-13-27-40.xml



Job Report_data_PRI-SER -XP_2007-07-26-13-27-40.xml

The "Job Report" lists all of the jobs that have been run by CA ARCserve Backup. For each job type, and description.

ID	Type	Status	Start Time	Owner	
1	Backup	Finished	0/00/80 11:50 AM	caroot	B
2	Backup	Finished	0/00/80 11:50 AM	caroot	B
3	Backup	Finished	0/00/80 11:51 AM	caroot	B
4	Backup	Finished	0/00/80 11:51 AM	caroot	B
5	Prune Database	Finished	0/00/80 12:00 PM		D
6	Backup	Finished	0/00/80 1:26 PM	caroot	B
7	Backup	Finished	0/00/80 1:27 PM	caroot	B

Print Preview
 Print to Printer
 Create Now
 Delete

Note: The Report Manager also allows you to remove reports using the delete option to delete the entire report files or delete reports based on date.

Report Manager Reports

Using Report Manager, you can generate three types of reports:

- Standard
- Custom
- Advanced

These reports are described in further detail in this section. For a summary listing of each report and type, see [Report Categories](#) (see page 621).

Standard Reports

CA ARCserve Backup provides several standard reports that display general backup and restore activity. The reports cover activity for job runs, media backups, and backup device errors. You can use a report filter to select the backup media you want to include in the report. Standard reports cannot be customized or scheduled to print at a specific time interval (not including the Preflight Check Report and GFS Media Prediction Report).

Custom Reports

Custom reports can be modified to meet your specific needs. Although the layout is similar to standard reports, custom reports are created using templates and saved in .XML format.

Note: You can adjust the layout of a custom report by modifying the width of the report columns. Open Windows Notepad and search for the report you want to adjust. Add or change the WIDTH attribute of the FIELD tag in the report template.

Custom reports can be scheduled to run immediately, at a specified time or repeat interval, and can be scheduled from the Primary server or a Member server. You can also specify to have the generated custom report sent to you by email.

There are two types of custom reports:

- **Predefined**--Available in seven categorical types when you install CA ARCserve Backup. Predefined reports contain basic report data headings that you can modify to suit your specific needs using Report Writer.
- **User-created**--Using Report Writer, you can create a report without using a template as a guide. If you save your user-created report in the CA ARCserve Backup reports directory, the title of the report displays in the My Reports folder in Report Manager.

Note: Although you can schedule reports from a Primary server and a Member server, CA ARCserve Backup generates the reports from the Primary server. To ensure that user-created, custom reports run as scheduled from the Primary server, you must copy the user-created report template to the reports directory on the primary server. The default reports template directory on the Primary server is as follows:

```
C:\Program Files\CA\ARCserve Backup\templates\reports
```

Advanced Reports

Advanced reports provide you with an overview of the current data protection status in your ARCserve environment. Advanced reports are predefined, available in different types when you install CA ARCserve Backup, and contain report data headings that you can modify to suit your specific needs.

To run a report, you must specify the report type and the path of the file where the generated report will be saved.

Advanced reports are similar to custom reports in that they can be scheduled to run immediately or at a specified time or repeat interval. You can also elect to have the generated advanced report sent to you by email.

Report Categories

The report categories that display in Report Manager originate from an external XML schema file (categories.xml) in the CA ARCserve Backup home directory. You can change the display order of the report categories by editing the categories.xml file.

The following table describes the categories, and types available for standard and custom reports.

Daily Status Reports

This report category provides the status of all jobs executed within the last 24 hours, including reports that display all clients which failed backup and media written in the last 24 hours.

The following reports are available:

- Daily Job Status Report (custom)
- Daily Backup Status Report (custom)
- Daily Failed Backups Report (custom)
- Recently Written Media Report (custom)

Note: The Daily Backup Status Report contains a field called Compression Ratio. The compression ratio shows the amount of data actually written to disk after deduplication. The field is available only for sessions backed up to deduplication device groups. This field is present through the Report Manager and also through Report Writer, File, Open, CA ARCserve Backup Home Directory, Templates, Reports.

Job Reports

This report category shows the status information for report jobs executed on a weekly basis. It provides reports showing all failed backups and a preflight check report that displays the status of report jobs scheduled to run at a future date.

The following reports are available:

- Job Report (standard)
- Enterprise Job Status Report (standard)
- 7 Days Job Status Report (custom)
- 7 Days Backup Status Report (custom)
- Failed Backups Report (custom)
- Preflight Check Report (standard)

Media Reports

This report category shows detailed media information about sessions backed up, including a list of media errors generated. Forecasted media schedules for GFS jobs are also available.

The following reports are available:

- Backup Media Error Report (standard)
- Session Detail Report (standard)
- Session Report (standard)
- ARCserve Backup for Laptops & Desktops Session Details Report (standard)
- GFS Media Prediction Report (standard)
- Media Usage Comparison Report (custom)
- Media Utilization Report (custom)
- Media Required for Data Recovery Report (custom)
- 7 Days Media Usage History Report (custom)
- Scratch Set Media in Device Report (standard)

Note: The Media Utilization, Session Detail and Session Reports now contain a field called Compression Ratio for Deduplication. This ratio shows the amount of data actually written to disk after deduplication. The field is only available for sessions backed up to deduplication device groups. This field is present through the Report Manager and also through Report Writer, File, Open, CA ARCserve Backup Home Directory, Templates, Reports.

Media Pool Reports

This report category shows detailed media pool related information including the status of media in scratch sets and GFS rotation profiles.

The following reports are available:

- Media Pool Report (standard)
- Media Pool Location Report (standard)
- GFS Rotation Profile Report (standard)
- Detailed Media Pool Report (custom)
- Media in Scratch Sets Report (custom)

Device Reports

This report category shows information about backup devices used with CA ARCserve Backup including the number of errors incurred during a backup on a device.

The following report is available:

- Backup Device Report (standard)

Backup Clients Reports

This report category shows backup client information including database and client agent data sizes.

The following reports are available:

- Backup Client Data Size Report (custom)
- Backup Clients and Job Associations Report (custom)
- Detailed Media Usage by Backup Clients Report (custom)

Note: The Backup Client Data Size Report now contains a field called Compression Ratio. This ratio shows the amount of data actually written to disk after deduplication. The field is only available for sessions backed up to deduplication device groups. This field is present through the Report Manager and also through Report Writer, File, Open, CA ARCserve Backup Home Directory, Templates, Reports.

Resource Usage History Reports

This report category shows forecasted usage information based on historical data.

The following reports are available:

- 7 Days Media Usage History Report (custom)
- Media Utilization Report (custom)
- Media Usage Comparison Report (custom)
- Backup Window and Throughput Comparison Report (custom)

Staging Reports

This report category provides you with information that you can use to analyze and manage data that was backed up to a file system device using the Disk to Disk to Tape Option.

With Staging Reports you can view status information about migration sessions, SnapLock sessions, and sessions that did not purge from staging devices. The Summary report lets you view information about a specific job or a group of jobs based upon a user-specified range of dates.

The following reports are available:

- Staging Migration Report
- Staging Purge Failed Report
- Staging SnapLock Report
- Staging Summary Report

Audit Log Reports

This report category adds audit fields to existing activity log information such as service starts and stops, or password changes. You can now identify who executed an action, from what machine, and using what application.

The following report is available:

- Audit Log

Statistics Reports

This report category provides an overview of the current data protection status. The reports include information about the backup and restore status. However, the output is based on the filter combinations you specify.

The following reports are available:

- Backup Attempt Success Rate: Summary Report (advanced)
- Backup Attempt Success Rate: Individual Client Report (advanced)
- Restore Attempt Success Rate Report (advanced)
- Drive Throughput Report (advanced)
- Backup Error Report (advanced)
- Failed Backup Attempt (advanced)
- Consecutive Failed Backup Attempt (advanced)
- Partial Backup (advanced)
- Full Backup Duration (advanced)
- Last Backup Status Report (advanced)
- Vaulting Report (advanced)

My Reports

This report category shows user-created reports that are saved in the following directory:

CA\ARCserve Backup\Templates\Reports

Statistics Reports

The statistics reports can accept and parse a variety of report filters; however, not all filters are required for all the reports. Based on the type of report that is being generated, only the filters required and supported by that specified report will be used.

To run any advanced report, you must specify at least the report type and the path to where the generated report will be saved.

The following report types, along with the corresponding supported filters can be generated using the statistic report category:

Backup Attempt Success Rate: Summary

This report provides information on what percentage of backup attempts that are successful and also shows percentage of incomplete and failed backup attempts.

Supported Filters:

- Start Date
- End Date
- Job Comment

Backup Attempt Success Rate: Individual Client

This report provides information on what percentage of backup attempts that are successful on a per node basis.

Supported Filters:

- Start Date
- End Date
- Job Comment

Restore Attempt Success Rate

This report provides information on what percentage of all restore attempts that are successful.

Supported Filters:

- Start Date
- End Date

Drive Throughput

This report provides information about the average throughput that is being seen on the tape drives in the system. Throughput obtained from this report can be compared against the native throughput of the drive. The output of this report can be filtered to specific drives by specifying the drive serial number.

Backup Error

This report shows the number of errors and warnings generated for the backup job for each of the backup paths during the reporting period. This helps in determining the clients with most number of errors.

Supported Filters:

- Start Date
- End Date
- Job Comment

Failed Backup Attempt

This report shows the clients with the most failed backup attempts during the reporting period.

Supported Filters

- Start Date
- End Date
- Job Comment
- Top Count (Limit output to the top 'n' clients only)

Consecutive Failed Backup Attempt

This report shows the clients with the consecutive failed backup attempts during the reporting period.

Supported Filters

- Start Date
- End Date
- Top Count (Limit output to the top 'n' clients only)

Partial Backups

This report shows the clients with the most number of partial backups. This reports help identify and restore critical file.

Supported Filters

- Start Date
- End Date
- Top Count (Limit output to the top 'n' clients only)

Full Backup Duration

This report shows the average backup time, average backup data, and average throughput for full backups of all backup paths during the reporting period.

Supported Filters

- Start Date
- End Date

Last Backup Status Report

This report shows the status of last execution of all the backup jobs in the queue. If a job is still active, it shows the current status of the running job. This report only shows the status of the job in the queue at the time the report is generated.

Supported Filters

- None

Vaulting Report

This report shows the list of tapes that will move in or out of the vault on the day of reporting.

Supported Filters

- None

Custom Report Job Scheduling

There are two ways you can schedule a custom report to run—Report Manager or Job Schedule Wizard. From Report Manager, you can schedule two of the standard reports (Preflight Check Report and GFS Media Prediction Report) and custom reports that represent Predefined or User-Created which display in the report categories.

Schedule a Custom Report Using the Report Manager

To schedule a custom report from Report Manager

1. Locate the report you want to schedule from the report list tree.
2. Click Schedule in the left panel pane next to the report description.
3. Specify the name and format type (.xml or .csv) for the report.
4. (Optional) Check the alert option box if you want to be alerted when report is sent by email and click Next.

5. Choose schedule options to run the report immediately or at a specific time and click Next.
6. Review your selection in the Job Summary page and enter a job description, if necessary.
7. Click Submit to execute the report job run.

Schedule a Custom Report Using the Job Scheduler Wizard

To schedule a custom report from the Job Scheduler wizard

1. Create a report template using the CA ARCserve Backup Report Writer and save it to a file.
2. Locate the Job Scheduler Wizard executable in the CA ARCserve Backup home directory and double click to launch it.
3. Select CAReports in the Run this program combo box and enter the report template name, the output file name where the report data will be stored, and silent mode (-s) mode as the parameters.

Note: For a full command line supported by the Report Writer, see the *Command Line Reference Guide* or the online help.

Create Custom Reports Using the Report Writer Utility

Report Writer is a CA ARCserve Backup utility that you can use to create custom reports. You can access Report Writer from the Utilities menu (or the Utilities section) in the CA ARCserve Backup home page.

Note: Reports created using Report Writer can be previewed, printed, or scheduled in Report Manager.

To create and generate a custom report

1. Open the Report Writer utility by selecting the Utilities menu and then choosing Report Writer.
2. Select the File menu and click Open to locate the report you want if you are generating a Predefined report. Otherwise, if you are generating a User-defined report, go to Step 3.
3. Enter a name for your report in the Report Title text box. Optionally, you can enter a description of your report in the Description text box.

4. In the Available Queries table, highlight the source from which you want to gather information for your report. When you highlight a source (such as Tape or Media Pool), the Available Columns table is populated with the types of data you can collect from the selected source. For example, if you select Job in the Available Queries table, you can choose to collect information about the Job Type, the Job Owner, the Job's Start Time, and several other items.

To select an item to include in your report, highlight the item in the Available Columns table and click Add. The item will be moved to the Report Columns table.

Note: You can create reports made up of information collected from multiple sources. For example, you could create a report that reports on Job Type, Tape Name, and Source Host.

5. Click Next to go to the Report Criteria screen. From this screen, you can customize your report in the following ways:
 - Set the order of the records—The records (or rows) in the columns of your report can be sorted in either ascending or descending order. By default, the records are ordered in ascending order.
 - Set the order of the columns—The column at the top of the Report Columns list will be the first (left-most) column in your report. To change the position of a column, highlight it in the Report Columns table and click the up or down arrow.
 - Set filters—The records for your report can be filtered for specific criteria that you define. Use the Enter Value field, along with the Operators and Condition drop-down menus, to specify the criteria for each type of record (each listing in the Report Columns table) in your report. After specifying a filter, click Add Criteria to add it to the Query Criteria table.

For example, to report only on jobs with a Job ID between 150 and 250, follow these steps:

- a. Click Job, Job ID in the Report Columns table.
 - b. Set the Operators drop-down menu to ">=", type 150 in the Enter Value field, and set the Condition drop-down menu to "and." Then click Add Criteria.
 - c. Set the Operators drop-down menu to "<=" and type 250 in the Enter Value field. Click Add Criteria. The Query Criteria table will reflect your criteria.
6. To run your report, click Generate Report.

Note: If you are using Report Writer to generate predefined Disk Staging Reports, the Add and Remove buttons are not accessible.

Report Generation for Multiple CA ARCserve Backup Servers

You can generate reports for a CA ARCserve Backup server at any time using the -m switch with the CARports command line utility. If you want to generate reports for more than one CA ARCserve Backup server, it is recommended that you create and store report templates on one server, and use remote servers as data sources. The customized report templates do not have to be updated for each CA ARCserve Backup server. Use the -m switch for each server so that all template updates are batched as a generic job.

Note: You can use the -a switch with the CARports command line utility to enable auto-file naming to generate daily reports.

Run a Session Details Report for ARCserve Backup for Laptops & Desktops

The ARCserve Backup for Laptops & Desktops Session Details Report identifies which (physical) tapes contain ARCserve Backup for Laptops & Desktops data. The report also identifies ARCserve Backup for Laptops & Desktops files that are expired. You can then make media management decisions based on this information. For example, if you find a tape that only contains expired ARCserve Backup for Laptops & Desktops files, you may choose to reuse that tape for other purposes.

To run a Session Details Report for ARCserve Backup for Laptops & Desktops

1. From the Monitor & Reports menu in the Navigation Bar on the Home Page, click Report.

The Report Manager opens.

2. Expand Reports, expand Media Reports, and select ARCserve Backup for Laptops & Desktops Session Details Report.

Select one of the viewing options to view the report: Print Preview, Print to File, or Print to Printer.

The report identifies all ARCserve Backup for Laptops & Desktops files and their locations. If the value in the Name Space column is "Unknown," then the file is expired.

Monitor Activity Using the Unicenter Monitoring Agent

If Unicenter was installed before you installed CA ARCserve Backup, you can use the Unicenter Monitoring Agent to monitor CA ARCserve Backup. This agent can be used to start and stop services, monitor the status of the CA ARCserve Backup processes and media, and report on the failure of backup jobs.

To use the Unicenter Monitoring Agent, you must install the manager with Unicenter and the agent with the CA ARCserve Backup server.

The agent part starts automatically when you start the SNMP agent on the agent machine.

To start the Unicenter manager component

1. Open Programs/Unicenter TND (or TNG)/WorldView/2-D Map.
2. Run Unicenter AutoDiscovery to find the machine that has the ARCserve Backup Unicenter Monitoring Agent installed.
3. Click the machine in the 2-D map.
The icon of the CA ARCserve Backup Unicenter Monitoring Agent displays.
4. Right-click the icon to open a pop-up menu.
5. Click Object View, View Note, or View Agent to monitor the status of CA ARCserve Backup processes, tapes, and jobs. (The information comes from the CA ARCserve Backup database.)
6. Click View Agent to start or stop CA ARCserve Backup services.

CA ARCserve Backup Diagnostic Utility

The CA ARCserve Backup Diagnostic Wizard utility is a convenient tool for gathering and packaging various CA ARCserve Backup and system logs, which may be necessary for troubleshooting.

Note: This utility is installed by default.

Diagnostic Utility Components

The Diagnostic Utility contains two components:

- Diagnostic Wizard
- Diagnostic Report Manager

You can launch the Diagnostic Wizard from the CA ARCserve Backup program group. It allows you to configure what kind of report and log you want to generate.

You can run one of the two following report generation modes:

- **Express Mode**--Collects information about the local machine. Does not include advanced debugging information.
- **Advanced Mode**--Collects information about the local machine or a remote machine and generates reports with greater debugging information enabled. If you select this mode, you are prompted to rerun the relevant job so that the newly selected debug flags can be processed during the job and entered into the report.

The Diagnostic Wizard also lets you select where to place the log on your hard disk. After you complete the Diagnostic Wizard, a file is created. You can view this file from the Diagnostic Report Manager, which is also accessible from the CA ARCserve Backup program group.

The following sections describe the process of running and reviewing an Express mode report.

Note: To run the Diagnostic Wizard in the Advanced mode, choose the Advanced option on the Select Diagnostic Type screen, and then follow the on-screen instructions.

Create a Report Using the Express Mode Diagnostic Utility

Using the ARCserve Diagnostic Wizard you can generate reports that collect diagnostic information about the local server.

Note: The Express Mode does not collect advanced debugging information about the local server.

To create a report using the Express Mode Diagnostic Utility

1. Open the Diagnostic Wizard by selecting Start, Programs, CA, ARCserve Backup, and then Diagnostic Wizard.

The ARCserve Diagnostic Wizard opens.

2. Click Next.

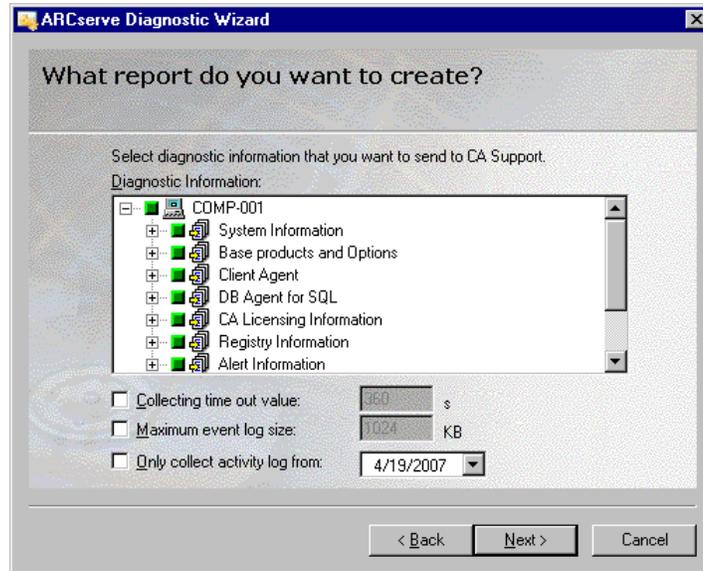
The Select Diagnostic Type window opens.

From here, you can choose to collect diagnostic logs from either the local server or a remote server, as well as whether or not you want to include advanced debugging information in the report.

Choose the Express type to gather local logs without including debugging information.

3. Click Next.

Select the attributes of the machine you want to gather logs from.



4. Click Next.

Specify the location where you want to save the diagnostic information file in the Diagnostic Information File Name field and click Next.

A summary of the logs to be collected displays.

5. Click Start.

This process can be lengthy, depending on the system and the amount of information that you requested.

6. When the process is complete, click OK, and then click Finish.

After the file has been created, you may be prompted to send it to CA Technical Support.

Create a Report Using the Advanced Mode Diagnostic Utility

To create a report using the Advanced Mode Diagnostic Utility

1. Open the Diagnostic Wizard by selecting Start, Programs, CA, ARCserve Backup, and then Diagnostic Wizard.

The ARCserve Diagnostic Wizard opens.

2. Click Next.

The Select Diagnostic Type window opens.

From here, you can choose to collect diagnostic logs from either the local server or a remote server, as well as advanced debugging information in the report.

Choose the Advanced type to gather local logs without including debugging information.

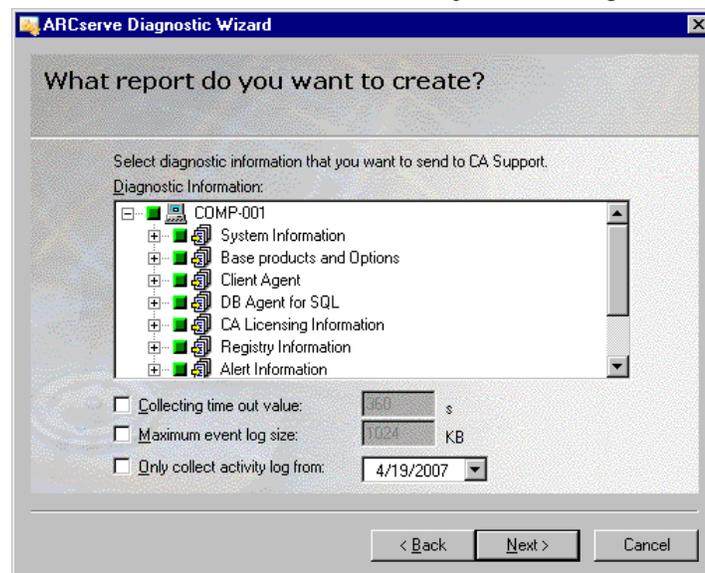
3. Click Next.

The Select an ARCserve Backup Job window opens.

Choose an ARCserve job.

4. Click Next.

Select the attributes of the machine you want to gather logs from.



5. Click Next.
Select the debug mode.
6. Click Next.
Specify the location where you want to save the diagnostic information file in the **Diagnostic Information File Name** field and click Next.
A summary of the logs to be collected displays.
7. Click Start.
This process can be lengthy, depending on the system and the amount of information that you requested.
8. When the process is complete, click OK, and then click Finish.
After the file has been created, you may be prompted to send it to CA Technical Support.

View a Report Using the Diagnostic Report Manager

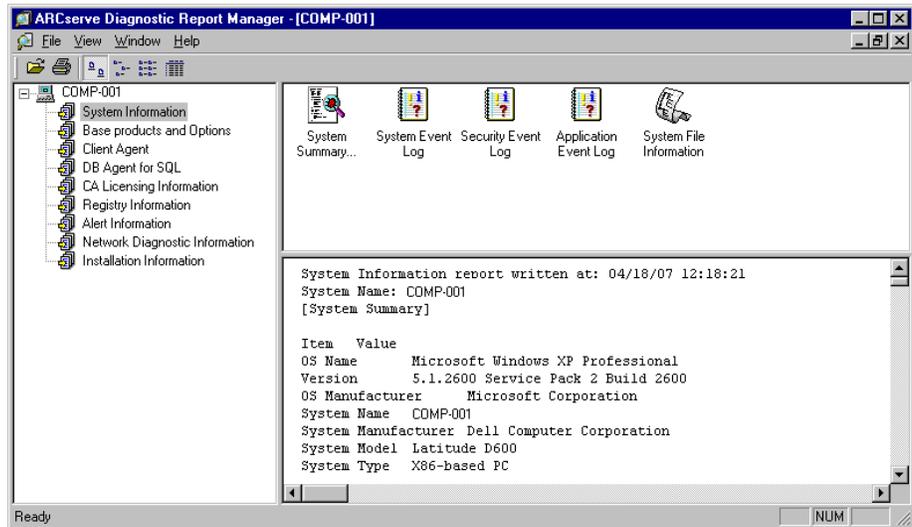
After the information you requested is collected, you can use the Diagnostic Report Manager to view it.

To view a diagnostic report

1. Start the Diagnostic Report Manager by selecting Start, Programs, CA, ARCserve Backup, and then select Diagnostic Report Manager from the ARCserve Backup program group.
The **Diagnostic Report Manager** opens.
2. From the File menu, choose Open.

3. Locate your saved log file and click **Open**.

A console opens that shows a list of your logs on the left-hand side. Detailed information appears in the bottom-right pane as you select items in the left-hand pane.



From the File menu on the Diagnostic Report Manager you can export, save, and print the selected log file.

Chapter 9: Using the Alert Manager

This section contains the following topics:

[How the Alert Manager Works](#) (see page 639)

[Alert Manager Components](#) (see page 641)

[Set Up Alerts](#) (see page 641)

[Alert Manager Configuration](#) (see page 643)

How the Alert Manager Works

Alert is a notification system that sends messages to people in your organization using various methods of communication. For example, you can send alerts to the system administrator, or a hardware technician in or out of the office. You can also send alerts to groups of people in different segments of the network.

The Alert Manager does not generate its own messages. You must configure the manager with the information you want to communicate and where you want to send it. Use the Alert options in the Backup Manager or Alert configuration in Server Admin to tell Alert what information you want to communicate. Use the Alert Manager or the Alert options in the Backup Manager to tell Alert how to send information and who to send it to. For more information on how you can select methods and specify recipients from within the Backup Manager, see the chapter “Backing Up Data.”

The information you communicate through Alert is called an Event. Events are words or phrases that appear in the Activity Log. You can select predefined job-related events, such as “Job Completed Successfully” and “Job Incomplete.” You can also customize job-related events, such as error, warning, or notification codes. In addition, you can specify non-job related events, such as starting or stopping the Tape Engine.

You can setup alerts from the following CA ARCserve Backup managers and utilities:

- Backup Manager
- Restore Manager
- Media Assure & Scan Utility
- Compare Utility
- Purge Utility
- Copy Utility
- Merge Utility
- Count Utility

To select job-related events, open these managers or utilities, click the Options toolbar button, and then select the Alert tab on the Options dialog.

Job-related events can also be accessed by selecting the Utilities menu and choosing any of the Utilities menu options. To select non-job related events, in Server Admin click Config, and then the Alert tab.

After you select events and they appear in the Activity Log, Alert generates notification messages and sends them to the appropriate recipients. For more information on selecting the information you want to communicate using Alert, see the chapter "Backing Up Data" for job-related events, and the chapter "Administering the Backup Server" for non-job related events.

Alerts can be sent in the following ways:

- **Broadcasts**--Sends pop-up messages to specific computers.
- **CA Unicenter TNG Option**--Sends messages to the TNG console and WorldView repository.
- **Lotus Notes**--Sends email messages using Lotus Notes.
- **Microsoft Exchange**--Sends email messages using Microsoft Exchange.
- **Windows Event Log**--Places event information in the Event logs of local and remote machines.
- **Pager**--Sends alphanumeric pager messages.

Note: Pager options are not supported on Japanese versions of CA ARCserve Backup.

- **SMTP (Simple Mail Transfer Protocol)**--Sends email messages using the standard email protocol on the Internet.
- **SNMP (Simple Network Management Protocol)**--Sends messages to SNMP managers, such as NetWare Management System (NMS), HP OpenView, and CA Unicenter TNG.
- **Trouble Tickets**--Sends printed documents to any print queue on your network.

Alert Manager Components

Alert is comprised of the following components:

- **Alert Manager**--The Alert Manager is used to configure how Alert sends its messages and to whom to send them.
- **Alert Service ([Alert Notification Server] Service)**--This service is responsible for the reception, processing, and distribution of Alert messages.
- **ALBUILD.DLL**--This .DLL acts as the channel between Alert and other applications. This file should be located in the Alert home directory.
- ***.CFG**--The application profile file is provided by an application. This *.CFG file must be present in the Windows directory so that Alert can handle messages generated by an application.

Set Up Alerts

CA ARCserve Backup provides event-based notification through email, pager, SNMP, broadcast, event log, or through Unicenter Network and Systems Management views. If you have Unicenter installed, you can use its Monitoring Agent to monitor the status of the CA ARCserve Backup processes and media, and report on the failure of backup jobs.

Example: Alert Notification

You can configure Alert to broadcast a message when a backup job finishes successfully.

To set up Alerts

1. From the Backup Manager window, click the **Options** toolbar button.
The Options dialog opens.
2. Click the **Alert** tab.
The Alert options display.

3. Click the **Configure** button to specify the transmission method.
The **Methods & Recipients Configuration** dialog appears.
4. In the Methods & Recipients Configuration dialog, click **New**.
The Configuration Name dialog opens.
5. Enter a name for the configuration in the **Configuration Name** field and then click **OK**.
Select the **Broadcast** method, and click the **Add** button.
The **Add Broadcast Recipient** dialog opens.
6. In the **Group/Machine** field, select your machine from the network, and click **Add** to add it to the Recipients field.
Or, if you know the machine name, enter the machine name into the recipient field.
Click **OK** and click **OK** again to save the configuration.
7. From the **Methods & Recipients** drop-down menu, select the saved configuration.
8. Select an Event from the **Event** drop-down menu, and click the **Add** button.
Now that you have set up Alert, you can proceed with your backup.
Click **OK** and click **Start** to submit your job.
The Security and Agent Information dialog appears.
9. From the **Security and Agent Information** dialog, select the job you want to run.
If the user name and password do not appear, click the Security button and enter the appropriate user name and password.
Review the security information and click **OK**.
The **Submit Job** dialog screen opens.
10. Enter a description for your backup job (optional), and click **OK** to submit the job.
Your job, which is now active, appears on the Job Queue tab in the Job Status window. If the job is active, you can view its status by double-clicking it on the Job Queue tab to invoke the Job Properties dialog.
When the job finishes, Alert notifies you, using the specified method.

Alert Manager Configuration

Before you use the Alert notification system, you must first establish a service account. To do this, open the Alert Manager, go to the Service menu, and select Set Service Account.

Note: If the Alert Manager was previously installed with another CA product, it is not reinstalled to the CA ARCserve Backup directory; it remains in the directory where it was previously installed.

You can send alerts using many communication mechanisms or applications. Any application that calls Alert specifies one of three event priorities—Critical, Warning, or Informational.

To view a list of the applications that call Alert, open the Alert Manager, and, in the left pane, expand Configuration and then expand Default or CA ARCserve Backup. You can either use the Alert default settings, which will be used by all applications that use the Alert Service, or you can enter configuration information specifically for each application. If you choose the latter, these configurations override the default Alert configurations.

The following sections describe how to configure each of the available communication mechanisms. To begin, expand Configuration, and then expand CA ARCserve Backup to view options discussed in the following sections.

Ports Option

The Ports option contains communication port profiles. Pagers and functions that use serial port access use these profiles. To configure, right-click Ports and select New Item. Enter the following information:

- **Port**--The name of the communications port you want the pager message to be broadcast from.
- **Data Bits**--The number of data bits, 7 or 8, which your modem uses.
- **Baud Rate**--The baud rate used by your modem.
- **Parity**--The parity setting, none, odd, or even, of your modem.
- **Stop Bits**--The number of stop bits, 1 or 2, which your modem uses.

If you want these settings to apply to any function that uses serial port access, place a check mark in the Use As Default box. When you are finished configuring port information, click OK.

Note: Pager options are not supported on Japanese versions of CA ARCserve Backup.

Broadcast Alerts

You can use Alert broadcasts to communicate information to specific network users or groups.

To use Broadcast Alerts, you must enable Windows Messenger services on Windows XP and Windows Server 2003 systems. The Messenger service is disabled by default on Windows XP and Windows Server 2003 systems.

Note: Windows Vista and Windows Server 2008 do not support Messenger services. As a result, Broadcast Alerts is not supported either of these platforms.

To configure broadcast options, right-click Broadcast and select New Item.

When the Broadcast Recipients page appears, enter or select all machine names in your network that you want to receive alert messages, and then click Add. For more information about adding broadcast recipients, see the online help.

CA Unicenter TNG

You can use CA Unicenter TNG to send messages to the Unicenter TNG console and World View repository when an alert is generated.

Note: Alert must be running on both the Event Management machine and the WorldView machine.

To configure CA Unicenter TNG settings, right-click CA Unicenter TNG and select Unicenter TNG Settings. When the Unicenter TNG Settings dialog appears, enter the following information:

- **Event Management Machine**--Enter the name of the machine that is running the Unicenter Event Management console.
- **TNG World View Machine**--Enter the name of the machine that contains the WorldView repository. If the WorldView machine is the same machine you are running Alert on, enter the user name and password for access to the Unicenter TNG repository.

You can also configure the TNG Event Map to set the criteria for Alert specifications in the Unicenter TNG environment. To do this, expand CA Unicenter TNG, right-click Critical, Warning, or Informational, and select Edit Item. When the Unicenter TNG Event Map screen appears, enter the following information:

- **Application Event Priority**--This displays the Application Event priority that is passed to Alert from the application. The categories can be Informational, Warning, or Critical. This field is automatically populated depending on which category you selected (under the CA Unicenter TNG object) in order to configure the TNG Event Map.
- **Severity**--Use this option to tailor the severity of the message that is passed from Alert to TNG. Select the type of alert message that you want to broadcast, Error, Fatal, Informational, Success, or Warning.
- **Color**--Select the color you want the message to display.
- **Attribute**--Set the message to blink or reverse. The default option sets the message to the TNG default.
- **Flags**--Select the appropriate check boxes to hold the message or highlight the message in the console.
- **Sent to Console**--Select the check box to send the alert message to the console.
- **Update object status in WorldView Repository**--Select this option in the TNG WorldView group to store the status of the current object in the WorldView Repository.

For more information about sending alerts using the CA Unicenter TNG Console and WorldView repository, see the online help.

Sample TNG Alert Scenarios

If you want to send informational alerts to the Unicenter TNG Console using blue text, configure a recipient as follows:

Event Priority	Description
Informational	Application Event Priority
Blue	Color
4	Send to Console
4	Send to World View

If you want to send error alerts to the Unicenter TNG Console using red text, and have the object status in the World View repository updated, configure another recipient as follows:

Event Priority	Description
Critical	Application Event Priority
Red	Color
4	Send to Console
4	Send to World View

Email Notification

You can use Lotus Notes, Microsoft Exchange, or SMTP to send email notification messages to specific users.

Important! You must install Lotus Notes or Microsoft Exchange Client to set up configuration data and to send messages. See your Windows manual for instructions on how to set up your email account.

Lotus Notes

To configure Lotus Notes settings, right-click Lotus Notes and select Lotus Notes Settings. When the Lotus Notes Settings page appears, enter the following information:

- **Lotus Notes Install Path**--Enter the appropriate install path.
- **Password**--Enter your password.
- **Use Specific Account**--If you want Alert to switch to another user ID, place a check mark in this box and enter information in the following fields:
 - **ID File**--For example, joeuser.id
 - **Mail Server**--For example, NotesServer/NotesDomain
 - **Mail File**--For example, mail/joeuser.nsf

After you configure Lotus Notes Settings and right-click Lotus Notes, select New Item or Message Attributes.

If you select New Item, Alert contacts the Lotus Notes server to display the address book. Select the users to whom you want to send alerts.

If you select Message Attributes, you can attach files to the email alert. Enter a subject, click Add File to select the file you want to attach, and then click OK.

Microsoft Exchange

To configure Microsoft Exchange settings, right-click and select one of the following:

- **New Item**--Lets you select email recipients.
- **Message Attributes**--If you select this, you can attach files to the email alert. Enter a subject, click Add File to select the file you want to attach, and then click OK.
- **MS Exchange Settings**--If you select this, the Service Logon Settings dialog appears. This is the same dialog that appears when you set up a service account. Enter the domain, user name, and password you want to use with the Alert Service. Make sure the account and user you enter is an account with Login as Service rights and is also an account on the Microsoft Exchange Server. If you are running the Microsoft Exchange Client, you must also enter the name of the server and mailbox. The mailbox name is case-sensitive and should not be hidden in a folder.

Note: If you are using Microsoft Outlook, right-click your Microsoft Outlook icon and select Properties. Select Microsoft Exchange Server and click Properties to view the server and mailbox information you should enter.

Send Job Logs Via Email

In addition to sending email notification messages, you can also use Lotus Notes or Microsoft Exchange to email job logs. To do this, create a new item and select recipients. Then, in the Backup Manager, before you submit a job, click the Options icon or, from the Backup menu, select Options. When the Global Options dialog appears, click the Alert tab, place a check mark in the Attach Job Log box, and then click OK. After you submit the job, the job log is sent to the recipients you specified.

Windows Event Log Notification

You can configure the event log so that Alert puts an event for a selected server in that machine's event log.

To configure event log configurations, right-click Window Event Log and select New Item. When the Eventlog Recipients dialog appears, enter or select all machine names in your network to which you want to send Alert messages, and then click Add.

Alert Manager Pager Options

Note: Pager options are not supported on Japanese versions of CA ARCserve Backup.

You can use the Pager option to communicate information using alphanumeric pager messages. Before you can add pager recipients, you must configure the communication ports.

Note: For more information about configuring ports, see [Ports Option](#) (see page 643).

To set up pager configurations, right-click Pager and select New Item. When the Pager Configuration page appears, enter the following information:

- **Owner Name**--Enter the name of the pager recipient.
- **Pager Type**--Select alphanumeric pager. Numeric is not supported.
- **Pager Number**--Enter a maximum of 24 characters. If a digit, such as 9, is needed for a dial tone, you must include it in this field.

Enter a comma to indicate a one second pause. If you want a longer pause, enter a string of commas.

You can use a dash to separate digits, but it has no function. (Check your modem manual because this can vary by modem.)
- **Pager ID**--Enter up to eight digits to identify the pager that will receive the alerts.
- **Site ID**--Enter up to four digits to identify where the alert occurred. This ID is included in the message to the pager; therefore, if the number is less than four digits, use leading zeros.
- **Connection Delay**--Enter the number of seconds you want to wait before a connection is made with the pager company. This will vary with your pager company, location, time of day, telephone equipment, and telephone traffic. If the connection is not established immediately, adding a delay prevents the alert from being sent before the connection is established.
- **Message Delay**--Enter the number of seconds to wait between the time the connection is made and the time the alert message is sent.
- **Port Configuration**--Select the appropriate port configuration. See Ports Option in this chapter for information on how to create new port profiles.

Note: When sending an alphanumeric page, consult your paging service for proper modem settings. The Alert service requires the TAP protocol for alphanumeric pages.

Pager Message Options

You can send variations of the messages in the following list to an alphanumeric pager. Substitute the bracketed words with the actual information.

- Boot Virus Detected
- Manager Detected a Virus [*virusname*] in [*path*]
- Infected File [*servername/path*] Detected
- Infected File [*path*] Accessed by user name at workstation address

Note: Pager options are not supported on Japanese versions of CA ARCserve Backup.

SMTP Notification

You can use SMTP to send email notification messages to recipients on the Internet. To configure SMTP settings, right-click SMTP and select New Item. When the SMTP Recipients page appears, enter the following information:

- **Address**--Enter the Internet email address for the recipient. For example, johnsmith@bigcompany.com.
- **Display Name**--Enter the name of the recipient.

SNMP Notification

You can use SNMP to send an SNMP trap to an SNMP manager. Examples of SNMP managers include NetWare Management System (NMS), HP OpenView, IBM NetView, and CA Unicenter TNG.

To configure SNMP settings, right-click SNMP and select New Item. When the SNMP Recipient page appears, enter the following information:

- **Manager Name**--Enter the name of the SNMP Manager.
- **Send Via**--Select one of the following options:
 - IPX--If you select this, enter the 8-byte network address of the machine where the SNMP manager is located. Next, enter the 12-byte node address of the machine where the SNMP manager is located. Use this field for Novell networks.
 - IP--If you select this, enter the IP address of the machine where the SNMP manager is located. Use this field if you are running the TCP/IP stack.

Trouble Tickets

You can use Trouble Tickets to communicate information through printed documents.

To configure Trouble Ticket settings, right-click Trouble Ticket and select New Item. When the Trouble Ticket Recipients page appears, enter the following information:

- **Company**--Enter the name of your company.
- **Location**--Enter the appropriate location information.
- **Header**--Enter the information that will appear at the top of each Trouble Ticket.

To select recipients, highlight a printer and click Add. When prompted, enter a user name and password to connect to the printer device.

In addition to using Trouble Tickets to send printed notification messages, you can also Trouble Tickets to send job logs. To do this, create a new item and select recipients. Then, in the Backup Manager, before you submit a job, click the Options icon or, from the Backup menu, select Options. When the Global Options dialog appears, click the Alert tab, place a check mark in the Attach Job Log box, and then click OK. After you submit the job, the job log is sent to the recipients you specified.

Event Priorities

All applications calling Alert specify one of the following event priorities:

- Critical
- Warning
- Informational

Message Testing

To test any of the Alert messaging functions, from the toolbar, select Send Test Message. You should test each setting after you configure it.

To avoid unnecessary alarm, inform Alert recipients that you are performing a test.

Alert Activity Details

To review alert activity, expand the Activity group and select one of the following:

- **Alert Summary**--Displays the status of Alert.
- **Alert Event Log**--Stores every message that Alert generates. It displays the date and time a particular event occurred, the applications that sent the alert, and the application that generated the event.
- **Alert Activity Log**--Stores a historical listing of alerts.

You can view, print, or clear these logs.

Appendix A: Troubleshooting

This section provides troubleshooting information to help you identify and resolve problems that you may encounter when using CA ARCserve Backup.

This section contains the following topics:

- [Log in Problems](#) (see page 653)
- [Jobs Do Not Start on Schedule](#) (see page 661)
- [Hardware Does Not Function as Expected](#) (see page 661)
- [Authentication Problems](#) (see page 664)
- [Cannot Back Up Open Files](#) (see page 668)
- [Tape Errors Occur When Backing Up or Restoring Data](#) (see page 670)
- [Discovery Service Does Not Function Properly](#) (see page 671)
- [GUI Freezes in Active Directory Restore Mode](#) (see page 672)
- [Restore Job Fails on Citrix Server](#) (see page 672)
- [Local Restore Data Backed Up with Compression and/or Encryption Failed](#) (see page 673)

Log in Problems

This section provides troubleshooting information to help you identify and resolve problems that relate to logging in to CA ARCserve Backup.

Unable to Log In After Changing the caroot Password

Valid on Windows

Symptom:

I changed the password for the caroot account. Why is it saying invalid password when I try to log in to CA ARCserve Backup?

Solution:

Your password did not change at the time of setup. There are various reasons for this; your machine name may have extended characters or you may have a machine name in a language other than English. If so, run the following debugging authentication commands (replace AB_MACHINE with your machine name) so that you can send the logs to CA Customer Support for investigation:

1. ping the machine by name. For example:

```
ping.exe AB_MACHINE
```

where AB_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.

2. Enter the following command

```
ipconfig /all > ipconfig.log
```

3. Enter the following command to tell CA Customer Support if the portmapper is running on your machine:

```
netstat -na >netstat.log
```

4. Enter the following command to let CA Customer Support know which CA ARCserve Backup services have registered with the rpc server running on the client machine:

```
rpcinfo.exe -p AB_MACHINE >rpcinfo.log
```

where AB_MACHINE is your machine.

5. Enter the following command:

```
rpcinfo.exe -t AB_MACHINE 395648 1 > caauthd.txt
```

where AB_MACHINE is your machine.

Note: Using '>' to a file does not show the results on the screen.

6. Set up the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA  
ARCserve Backup\Base\LogARCserve\[DWORD]DebugLogs ==1.
```

This creates the rpc.log file in the CA ARCserve Backup home directory under \log.

Makeup Jobs Created When the Media is Full

Valid on Windows 64-bit operating systems.

Symptom:

While performing a backup to tape operation using the Client Agent for Windows, ARCserve detects a media full condition. You must replace the media within 20 minutes of the detection. If you replace the media after 20 minutes of the detection elapses, the following events occur:

- Error E3392 (Backup server TCP reconnection timeout) is recorded in the Activity Log.
- The job completes successfully with a completion status of Failed.
- ARCserve creates a Makeup Job.

Solution:

The remedies for this problem are as follows:

- Although the job completed successfully, Error E3392 caused the job to appear to fail. The Makeup Job was created because ARCserve detected a failed job. In conclusion, you can safely delete the Makeup Job.
- You can increase the time-out waiting period value by modifying the following registry keys:

HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA ARCserve
Backup\ClientAgent\Parameters\SendTimeOut

Default: 1200 (seconds)

HKEY_LOCAL_MACHINE\Software\ComputerAssociates\CA ARCserve
Backup\ClientAgent\Parameters\ReceiveTimeOut

Default: 1200 (seconds)

Example: To increase the waiting period to 60 minutes, modify the above DWORD values to 3600.

Unable to Log In to CA ARCserve Backup After Changing the Computer Name

Valid on Windows**Symptom:**

I changed the name of a machine that has CA ARCserve Backup installed and rebooted it. Why can't I log in to the CA ARCserve Backup Manager Console anymore?

Solution:

The computer name is a name that your computer uses to identify itself in a network or a domain. In a centralized management environment, an ARCserve domain can consist of a primary server and one or more member servers, or a stand-alone server. CA ARCserve Backup uses the computer names of the primary server and the member servers to establish communication between the servers.

For more information about how to process computer name changes in an ARCserve domain, see [How to Process Computer Name Changes in an ARCserve Domain](#) (see page 494).

CA ARCserve Backup Cannot Communicate after Changing the IP Address of a CA ARCserve Backup Server

Valid on Windows platforms.

Overview

There are several reasons why the IP address would be changed on a CA ARCserve Backup server. Some of the common reasons are as follows:

- The network interface card (NIC) was replaced in a CA ARCserve Backup server. When the computer rejoins the network, the IP address is different from that of the previous network card.
- The CA ARCserve Backup server communicates with a DHCP server to obtain an IP address and the CA ARCserve Backup server connects to a different DHCP server.

Symptoms

After you change the IP address on a primary server, a stand-alone server, and a system hosting the CA ARCserve Backup Manager Console, CA ARCserve Backup demonstrates the following behavior:

- On a member server and a system hosting the CA ARCserve Backup Manager Console, the value of the Domain is "None" in the Default Server and Security fields on the Manager Console.
- Error messages appear when you click the Backup link in the Navigation Bar on the member server. For example, a pop-up message appears "Connecting to primary server."
- Pinging the primary server from the Command Line on a member server, returns the message "Request timed out."
- Equivalence errors may occur when you execute a task using a CA ARCserve Backup command line utility on the primary server or a stand-alone server. For example, one of the following messages may appear:

```
Ntuser not validated in authentication server on Hostname.  
Do you want to create equivalence (default : y)?
```

After you change the IP address on a member server, CA ARCserve Backup demonstrates the following behavior:

- On a member server, the value of the Domain is "None" in the Default Server and Security section on the Manager Console.
- From the primary server or a system hosting the CA ARCserve Backup Manager Console, you cannot log in to the member server.

- Pinging a member server from the Command Line on the primary server, returns the message "Request timed out."
- Equivalence errors may occur when you execute a task using a CA ARCserve Backup command line utility on a member server. For example, one of the following messages may appear:

```
Ntuser not validated in authentication server on Hostname.  
Do you want to create equivalence (default : y)?
```

Solutions

To remedy the communication problems, use the procedure that corresponds with the type of CA ARCserve Backup server where the IP address was changed.

IP Address Changed on the Primary Server or Stand-alone Server

Important! After you change the IP address of a primary server or a stand-alone server, basic backup jobs and restore jobs from the server itself can complete successfully. Additionally, the host names of the member servers should display in the CA ARCserve Backup managers on the primary server. However, to ensure that you can successfully complete backup jobs and restore jobs on member servers, you must complete the modification described in Step 1 on the member server before completing any other task.

1. If the CA ARCserve Backup server is a primary server, stop and restart the CA ARCserve Backup services using the following commands:

- cstop
- cstart

2. If there are member servers in your CA ARCserve Backup domain, open the Windows Command Line the member server.

Execute the ipconfig command using the /flushdns switch. For example:

```
c:\documents and settings\windows user name>ipconfig /flushdns
```

Note: You must repeat this step on all member servers in your CA ARCserve Backup domain.

3. Create equivalence on the primary server or stand-alone server using the ca_auth command. The syntax for this task is as follows:

```
ca_auth [-cahost HOST-NAME] -equiv add ntuser HOST-NAME ARCserveBackupUser  
[caroot_username] [caroot_password]
```

Note: For more information about using the ca_auth command, see the *Command Line Reference Guide*.

IP Address Changed on a Member Server

1. Create equivalence on the member server using the `ca_auth` command. The syntax for this task is as follows:

```
ca_auth [-cahost HOST-NAME] -equiv add ntuser HOST-NAME ARCserveBackupUser  
[caroot_username] [caroot_password]
```

Note: For more information about using the `ca_auth` command, see the *Command Line Reference Guide*.

2. Open the Windows Command Line on the primary server. Execute the `ipconfig` command using the `/flushdns` switch. For example:

```
c:\documents and settings\windows user name>ipconfig /flushdns
```

IP Address Changed on a Server that is Hosting the ARCserve Manager Console

No action is required when the IP address is changed on a server that is hosting the CA ARCserve Backup Manager Console. You can continue to manage other CA ARCserve Backup servers without experiencing communication problems.

IP Address Changed on an Agent System

Select one of the following corrective actions:

- Open the Windows Command Line on the CA ARCserve Backup server that is backing up the agent system.

Execute the `ipconfig` command using the `/flushdns` switch. For example:

```
c:\documents and settings\windows user name>ipconfig /flushdns
```

- If you added the agent system to the primary server, a member server, or a stand-alone server by referencing the IP address rather than the agent system's host name, you can log in the CA ARCserve Backup server and manually change the IP address of the agent system. To do this, complete the following steps:

1. Log in to the CA ARCserve Backup server, open the Backup Manager, and expand the Windows system object.
2. Right-click the agent system and select **Modify Agent** from the pop-up menu.

The Agent Option dialog opens.

3. Specify the new IP address in the IP address field and click **OK**.

The new IP address is applied to the agent system.

IP Address Changed on a System Using a Static IP Address

Select one of the following corrective actions:

- When you use a static IP address, you can register the new static IP address on the DNS server. Based on the type of server (for example, a primary server, member server, and so on), use the ipconfig command task described in the previous sections to refresh their local DNS client.

This action lets you resolve the cache for establishing a new relationship between the host name and IP address.

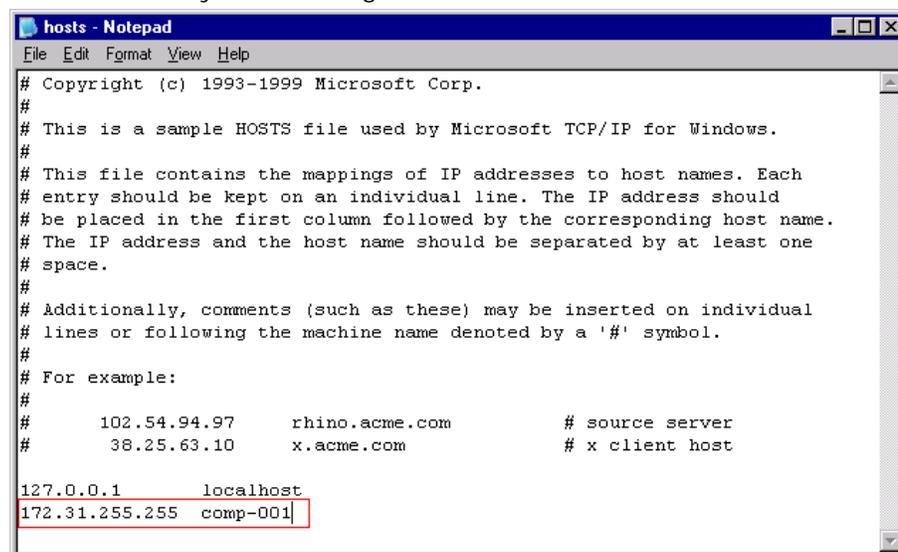
- If you do not register the new static IP address with the DNS server, you must modify the Hosts file on the servers to reflect this change.

To remedy this scenario, do the following:

1. From Windows Explorer, open the following file using a text editing application such as Notepad:

C:\WINDOWS\system32\drivers\etc\hosts

2. Specify the static IP address and host name of the system as illustrated by the following screen:



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com              # x client host
127.0.0.1        localhost
172.31.255.255  comp-001
```

3. Close the file and save the changes.

Note: When you use this solution, you must modify the Hosts file when you change the IP address, and delete the specified information when you revert to a dynamic IP address.

Authentication Errors Occur When Stopping and Starting the CAportmapper Service

Valid on Windows platforms.

Symptom:

Authentication errors occur that prevent you from opening the Manager Console after you stop and restart the CAportmapper service.

Solution:

This condition only occurs under the following sequence of events:

- All ARCserve services are running.
- You stop the CAportmapper service using either the Net Stop command or by stopping the service from the Windows Computer Management console.
- You restart the CAportmapper service.

Important! You must stop and start the CAportmapper Service using the `cstop` or `cstart` command. These commands let you stop and start all CA ARCserve Backup services sequentially, based on their dependencies with other CA ARCserve Backup services.

More information:

[Stop and Start All CA ARCserve Backup Services Using Batch Files](#) (see page 436)

Jobs Do Not Start on Schedule

Valid on Windows, UNIX, and Linux platforms.

Symptom:

Scheduled jobs do not start on schedule.

This problem is most likely to occur when you have multiple CA ARCserve Backup servers in a centralized management environment and the ARCserve primary server and ARCserve members reside in different time zones.

Solution:

To remedy this problem, synchronize the system time on the primary server with the system time on all ARCserve member services in the ARCserve domain.

Use the Windows Time Service to complete this task.

Note: For information about how to synchronize the time using the Windows Time Services, see the Windows Help and Support.

Hardware Does Not Function as Expected

The following sections provide guidance to help you address hardware-related issues when using CA ARCserve Backup.

Possible Problems

If you are having hardware-related issues with CA ARCserve Backup, you may experience the following symptoms:

- E6300 Windows NT SCSI Port Errors in the CA ARCserve Backup Activity Log.
- Slots not showing the proper status or not updating properly.
- Devices not listed properly in CA ARCserve Backup Device screen.
- Critical hardware errors in the CA ARCserve Backup Activity Log.
- Inability to properly configure your tape device.
- Hardware-related inconsistencies in day-to-day CA ARCserve Backup functions.

Possible Resolutions

The following list of resolutions can help you address hardware-related issues:

- Ensure that the operating system is properly recognizing your devices. If the operating system is having a problem seeing the devices, CA ARCserve Backup may not function properly.
- Ensure that the latest Device Patch is installed for CA ARCserve Backup.
- Check the CA ARCserve Backup Certified Device list to ensure compatibility with your device's firmware.
- Ensure that the proper SCSI drivers are loaded for your SCSI adapter.
- Try using different tapes to ensure that the errors are not media-related.
- Check physical connections and SCSI cabling. Errors can occur because of physical problems, such as a bent SCSI pin.
- If you are running CA ARCserve Backup on a Windows platform, run Device Configuration by selecting Device Configuration from the Configuration menu. Choose Enable/Disable Devices (For RSM). If you see your devices listed in the Available Devices window, ensure that the check box is selected. Doing so gives CA ARCserve Backup full control over your device, and does not allow the Windows 2000 Removable Storage Manager service to interfere.
- Check if third-party device monitoring or controlling services are running and, if necessary, disable these services, as they may be conflicting with the CA ARCserve Backup ability to control the device.
- If you are using Library Quick Initialization, ensure that you disable this option when you are troubleshooting hardware and devices. You can then apply the Library Quick Initialization option after troubleshooting has been completed.

Note: The Library Quick Initialization option can be found on the General tab on the Library Properties dialog.

CA ARCserve Backup Does Not Detect a Cleaning Tape

Valid on Windows platforms.

Symptom:

There is a cleaning tape in the library but CA ARCserve Backup does not detect a cleaning tape.

Solution:

To remedy this problem, CA ARCserve Backup must detect the location (slot) of the cleaning tape. There are two methods that you can use to let CA ARCserve Backup detect the location (slot) of the cleaning tape.

- Let CA ARCserve Backup discover the location (slot) of the cleaning tape. To do this, complete the following steps:

1. Insert a cleaning tape into any available slot in your library.
2. Open the Device Manager window, right-click the library and select Inventory from the pop-up menu.

CA ARCserve Backup inventories the media in the slots. After the inventory process is complete, CA ARCserve Backup detects the presence of a cleaning tape. The slot where the cleaning tape resides becomes the cleaning slot.

- Manually specify the location (slot) of the cleaning tape. To do this, complete the following steps:

1. Open the Device Manager window, right-click the library and select Properties from the pop-up menu.

The Library Properties dialog opens.

2. Click the Cleaning tab.

The Cleaning options appear.

3. From the Available Slots lists, click an available slot and then click the Add button.

The available slot moves to the Clean Slots list.

4. Click OK.

5. Insert the cleaning tape into the slot specified.

CA ARCserve Backup Cannot Detect RSM Controlled Devices on x64 Platforms

Valid on Windows Server 2003 x64 platforms.

Symptom:

CA ARCserve Backup is installed on a Windows Server 2003 x64 system. From the Device Manager, CA ARCserve Backup cannot detect devices controlled by the Removable Storage Manager (RSM), and you cannot enable and disable RSM controlled devices.

Solution:

The CA ARCserve Backup Manager Console is designed using x86 architecture. The Manager Console cannot detect RSM controlled devices on all Windows 64-bit platforms. To remedy this limitation, you can enable and disable RSM controlled devices using the RSM Computer Management utility.

Authentication Problems

The sections that follow describe how to troubleshoot and correct authentication related problems.

Authentication Security Settings

The following section provides guidance to help you address authentication and security-related issues when using CA ARCserve Backup. Because symptoms of security-related issues vary widely, this section includes possible resolutions only.

Possible Resolutions

The following list of resolutions can help you address security-related issues:

Ensure that CA ARCserve Backup has properly authenticated the caroot account. Use the Server Configuration Wizard to perform this authentication. Select the Password for Backup Server Logon and Administration option to set the caroot account and password.

- Ensure that the CA ARCserve Backup folder is shared with:
 - Administrator--Full Control
 - ARCserve Backup System Account--Full Control
 - Backup Operators--Change and Read

- If you are having general problems understanding what rights your backup account needs to perform storage functions in your environment, consider the following information.

If you are backing up only your local CA ARCserve Backup server, the CA ARCserve Backup System account configured at installation has sufficient rights (Administrator and Backup Operator).

If you are backing up remote data within your domain (through the Client Agent for Windows or through the network facility of CA ARCserve Backup), your backup account requires additional rights. The following is a general outline of common permissions necessary for a powerful backup account. You can tailor your backup account to match your needs, and some rights may not be required in your environment.

Note: Security requirements for storage-related functions are dependent upon the resources accessed. Windows security rules and requirements should be considered at all times.

The backup account should have the following Group Rights:

- Administrator
- Backup Operator

Note: A user in the Backup Operator Group does not have rights to access the CA ARCserve Backup database. As a result member servers are not visible, to the user, in the Backup Manager.

- Domain Administrator

The backup account should have the following Advanced Rights:

- Act as part of Operating System
- Log on Locally
- Log on as a service

- When prompted by CA ARCserve Backup to enter security within a domain, always use domain\username as the context.
- If you have established a connection between two computers with one login/password session, Session Credential Conflicts can occur if you attempt to establish a second connection with the same login/password session. Consider any existing sessions you may have and how these may affect CA ARCserve Backup ability to access a resource.
- The security entered in CA ARCserve Backup jobs is static and does not update dynamically if the Windows security account information changes at the operating system level. If you change the account information packaged in your CA ARCserve Backup jobs, you must modify the jobs and repackage them with the proper security information.
- You must back up remote Registry and System State information through the CA ARCserve Backup Client Agent for Windows.

- If you manually stopped and restarted the CA Remote Procedure Call service (CASportmap) without using the cstop and cstart command, the service cannot communicate with its port assignments properly. This can prevent a user account with caroot equivalence from logging in to the CA ARCserve Backup domain.

To remedy the inability to log in to the CA ARCserve Backup domain, run the cstop command and then run the cstart command. This enables the service to communicate properly and lets the user account with caroot equivalence log in to the CA ARCserve Backup domain.

Restricted Users Cannot Access the Activity Log and the Audit Log

Valid on Windows Server 2003, Windows Vista, and Windows Server 2008 systems.

Symptom:

When you log in to CA ARCserve Backup using Windows authentication and a Windows account with restricted privileges (for example, Backup Operator and Remote Desktop User), you cannot access the CA ARCserve Backup Activity Log and Audit Log.

Note: This behavior does not occur when you configure CA ARCserve Backup to authenticate with the CA ARCserve Backup database using SQL Server authentication.

Solution:

To remedy this behavior, you must grant all Windows accounts that require access to the Activity Log and the Audit Log the privilege to connect to SQL Server using Microsoft SQL Server authentication.

To grant privileges on Microsoft SQL Server 2000

1. Allow Microsoft SQL Server to communicate by adding the application to the Windows firewall exceptions list.
2. Allow the restricted Windows accounts to communicate as members of the SQL instance group or the sysadmin group.

To grant privileges on Microsoft SQL Server 2005, Microsoft SQL Server 2005 Express Edition, and Microsoft SQL Server 2008

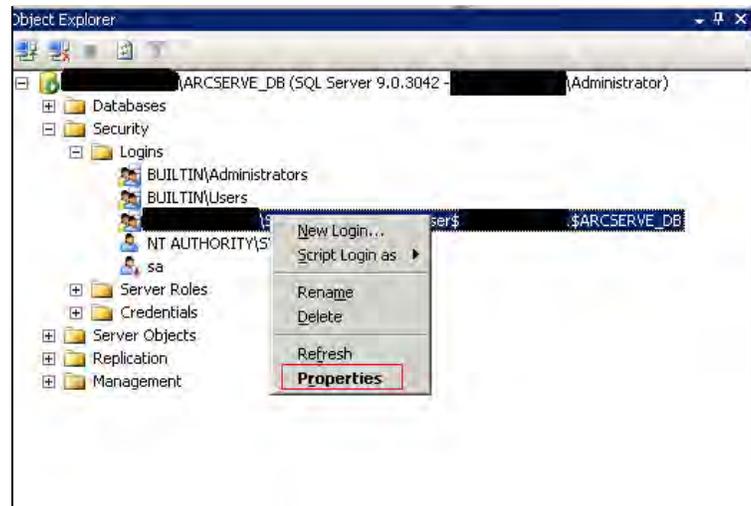
1. Allow Microsoft SQL Server to communicate by adding the application to the Windows firewall exceptions list.
2. Allow the restricted Windows accounts to communicate as members of the SQL instance group or the sysadmin group

3. Add the restricted Windows accounts into Microsoft SQL Server by doing the following:

- a. Open Microsoft SQL Server Management Tool.

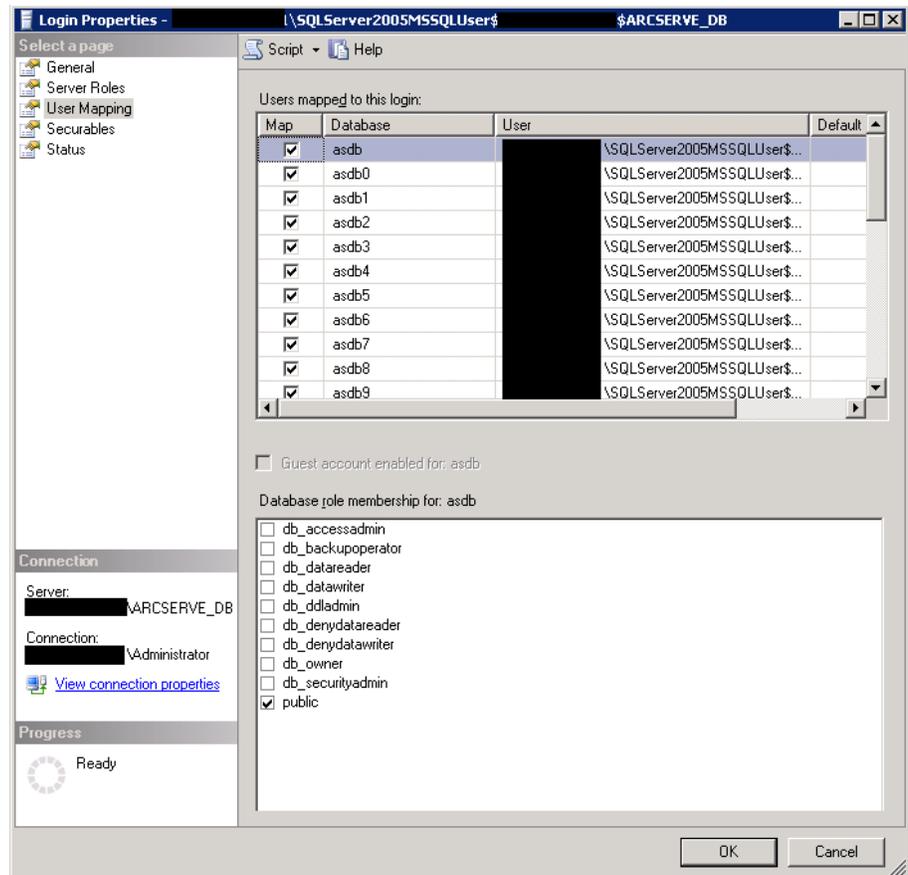
Open Object Explorer.

Expand the CA ARCserve Backup server, Security, and Logins as illustrated by the following screen:



- b. Right-click the CA ARCserve Backup instance and click Properties on the pop-up menu.

The Login Properties dialog opens as illustrated by the following screen.



- c. Click User Mapping.
- d. In the Users mapped to this logon field, select the databases that you want to map by click the Map check box.
- e. In the Database role membership for field, select the roles that you want to apply to this user for the selected database and click OK.

Cannot Back Up Open Files

The following section provides guidance to help you address issues related to open files when using CA ARCserve Backup.

Possible Problems and Resolutions

If a particular resource you are backing up is locked or in use by the operating system, you may receive the following errors. These errors may be preceded by error code W3404.

Note: The CA ARCserve Backup Agent for Open Files reconciles many common open file errors. If you are not using this Agent, you should consider doing so. We also recommend that you perform remote backups using the CA ARCserve Backup Client Agent for Windows.

MS Error Code	Cause and Resolution
SHARING VIOLATION	<p>Cause: File sharing violation error. Another process (such as an application service) was using a target file when CA ARCserve Backup ran a Backup Job.</p> <p>Resolution: Stop all services and applications using the target file and restart the Backup.</p>
ACCESS DENIED	<p>Cause: A target file for the backup job was not accessible, or another process (such as an application service) was using a target file when CA ARCserve Backup ran the backup job.</p> <p>Resolution: Ensure that your user account has sufficient rights to access the target file, and stop all services and applications using the target file before restarting the backup job.</p>
FILE NOT FOUND	<p>Cause: A target file has been deleted or moved between the submission and the execution of a Backup Job.</p> <p>Resolution: Modify and repackage Job and retry.</p>
PATH NOT FOUND	<p>Cause: A target file path has been deleted or changed between the submission and the execution of a Backup Job.</p> <p>Resolution: Modify and repackage Job and retry.</p>
BAD NET PATH	<p>Cause: A Backup Job is submitted to a Remote Machine and a target network path was not detected because of a missing path or network protocol delay.</p> <p>Resolution: Confirm your network environment and retry the Backup Job.</p>

Tape Errors Occur When Backing Up or Restoring Data

The following section provides guidance to help you address issues related to tape errors when using CA ARCserve Backup.

Possible Problems

If you receive an error that suggests that there is something wrong with one of your tapes, you should take corrective action as soon as possible to ensure the security of your data. Before replacing your tape, however, you should make certain that it is the tape that is causing the problem, and not another part of your system. Try these steps to rule out the possibility that the problem is being caused by something other than the tape:

- Check the history of the Activity Log for the task that caused the error. Although you may get a media error, it may only be the consequence of an earlier error.

For example, during a backup job, you may receive a SCSI port error. After receiving this error, you may get errors that indicate a problem with the tape, or even with the drive, but it is possible that these errors are only a consequence of the problems with the SCSI port. Therefore, you should check the Activity Log for all the messages and errors you received prior to receiving the error that indicated a problem with your tape. In this way, you can determine whether there is actually a problem with your tape, or if the tape error was the consequence of another problem.

- Monitor the library robot. If the robot is not functioning properly, you may get tape errors. Make sure that the robot can move tapes in and out of the drives.
- Rule out the possibility of a mechanical problem with the drive. To do so, try one of these options:
 - Clean the drive, then perform the same task again.
 - If the tape still causes errors after the drive has been cleaned, move the tape to a drive that you know is in good working order and try the same task again. If you get the same error, then it is likely that there is a problem with the tape.

Note: If your drives are inside a library, and you want to try your tape in a different drive, the problem drive must be offline. If CA ARCserve Backup did not automatically set the drive to an offline status when it detected the media error, right-click the library and select Offline from the pop-up menu.

- Try the same task on the same drive, but with a different tape. If you get the same error, then it is likely that the tape is fine, but that there is a problem with the drive or some other system component.

Possible Resolutions

After you have determined that there is a problem with the tape--part of the tape is unreadable, the tape is physically damaged in some way, and so on--you should replace the tape as soon as possible. Before you do that, you will need to back up the data on the bad tape to a reliable tape. You have two options at this point:

- Copy the data to a new tape
- Create a new backup tape

Copy the Data to a New Tape

If you can read data from the tape, follow the steps below. If no data can be read, see [Create a New Backup Tape](#) (see page 671) in this appendix for steps about creating a new backup tape.

1. Try moving the tape to a drive that you know is in good working order. You can also try cleaning the drive.
2. Use the Tapecopy utility to copy the data from the bad tape to the new tape.

Note: If the bad tape was part of a library, export the tape from the library so that it does not get used again.

Create a New Backup Tape

If you are unable to read any data from the bad tape, follow these steps to create a new backup tape.

1. Remove the bad tape. If the bad tape is part of a library, export it.
2. Insert a new tape and resubmit the backup job.

Discovery Service Does Not Function Properly

The following section provides guidance to help you address issues related to discovery service problems when using CA ARCserve Backup.

Possible Problems

You may experience a problem in discovering CA ARCserve Backup applications on a specific machine. It is possible that the machine to be discovered is not located on the same subnet as the machine the discovery service is running (the default setting for Discovery Service is the local subnet).

Possible Resolutions

Choose the Subnet sweep option in the Configuration window and restart the Discovery Service. Or, you can add the specific subnet or machine name (IP address) and restart the Discovery Service.

GUI Freezes in Active Directory Restore Mode

Valid on Windows platforms.

Symptom:

The CA ARCserve Backup manager freezes when Windows is started in the Active Directory Restore Mode and you are not able to restore the Active Directory if Windows is in the Active Directory Restore Mode. The cause is due to the fact that Microsoft SQL Server Express and Microsoft SQL Server will not function if you start Windows in the Active Directory Restore Mode.

Solution:

Submit the Active Directory restore job using Windows Normal Mode and execute the Active Directory restore job after restarting Windows using the Active Directory Restore Mode.

Restore Job Fails on Citrix Server

Valid on Windows platforms.

Symptom:

A restore job fails on a server running Citrix. The list that follows describes the environment on the Citrix server:

- Citrix 4.0
- Microsoft SQL Server (hosting the Citrix database instance)
- Client Agent for Windows
- Agent for Microsoft SQL Server

Solution:

When you restore a Citrix 4.0 server, the job may fail because the Microsoft SQL Server instance hosting the Citrix database instance will not start after the restore job is complete.

To remedy this problem, restart the Citrix database instance manually.

Local Restore Data Backed Up with Compression and/or Encryption Failed

Valid on windows platforms

Symptom:

During the backup, which is using compression and/or encryption, the file is increasing in size. When you perform a local restore, the job is incomplete with Error E3453 - Unable to write stream data.

Solution:

1. Create a DWORD value called RestoreDCENDataByWriteFile under the following registry key and set it to 1.
HKEY_LOCAL_MACHINE \SOFTWARE\ComputerAssociates\Base\Task\Restore
2. Select the files being restored that failed, set the destination, and submit a new restore job.

Appendix B: Using Deduplication

This section contains the following topics:

[How Data Deduplication Works](#) (see page 676)

[How to Plan a Deduplication Installation](#) (see page 678)

[Deduplication Considerations](#) (see page 679)

[How to Configure Your Implementation for Deduplication](#) (see page 681)

[Deduplication Device Group Configuration](#) (see page 683)

[Device Commands for Data Deduplication Devices](#) (see page 683)

[Backup Data with Deduplication](#) (see page 683)

[Recover Deduplicated Data](#) (see page 695)

[Deduplication Reports](#) (see page 700)

How Data Deduplication Works

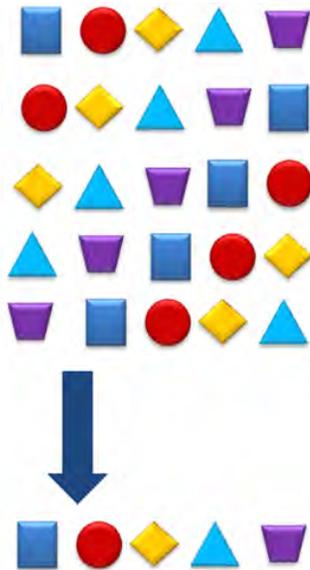
Data deduplication is technology that allows you to fit more backups on the same physical media, retain backups for longer periods of time, and speed up data recovery. Deduplication analyzes data streams sent to be backed up, looking for duplicate "chunks." It saves only unique chunks to disk. Duplicates are tracked in special index files.

In CA ARCserve Backup, deduplication is an in-line process that occurs at the backup server, within a single session. To identify redundancy between the backup jobs performed on the root directories of two different computers, use [global deduplication](#) (see page 694).

During the first backup:

- CA ARCserve Backup scans incoming data and segments it into chunks. This process occurs in the SIS layer of the Tape Engine.
- CA ARCserve Backup executes a hashing algorithm that assigns a unique value to each chunk of data and saves those values to a hash file.
- CA ARCserve Backup compares hash values. When duplicates are found, data is written to disk only once, and a reference is added to a reference file pointing back to the storage location of the first identified instance of that data chunk.

In the diagram below, the disk space needed to backup this data stream is smaller in a deduplication backup job than in a regular backup job.



With deduplication, three files are created for every backup session:

- **Index Files (Metadata files)**

- **Hash files**--store the markers assigned to each redundant chunk of data.
- **Reference files**--count hashes and store the address in the data files that correspond to each hash.

- **Data files**--store the unique instances of the data you backed up.

The two index files together consume a small percentage of the total data store so the size of the drive that stores these files is not as critical as its speed. Consider a solid state disk or similar device with excellent seek times for this purpose.

During subsequent backups:

- CA ARCserve Backup scans incoming data and breaks it into chunks.
- CA ARCserve Backup executes the hashing algorithm to assign hash values.
- CA ARCserve Backup compares new hash values to previous values, looking for duplicates. When duplicates are found, data is not written to disk. Instead, the reference file is updated with the storage location of the original instance of the data chunk.

Note: Use Optimization for better throughputs and decreased CPU usage. With Optimization enabled, CA ARCserve Backup scans file attributes, looking for changes at the file header level. If no changes were made, the hashing algorithm is not executed on those files and the files are not copied to disk. The hashing algorithm runs only on files changed since the last backup. To enable Optimization, select the Allow optimization in Deduplication Backups option located on the Deduplication Group Configuration screen. Optimization is supported on Windows volumes only. It is not supported for stream-based backups, such as SQL VDI, Exchange DB level, Oracle, and VMware Image level backups.

When you must restore deduplicated data, CA ARCserve Backup refers to the index files to first identify and then find each chunk of data needed to reassemble the original data stream.

How to Plan a Deduplication Installation

Data deduplication happens on the CA ARCserve Backup Server, so it works with all CA ARCserve Backup Agents running in your environment. However, you must upgrade any CA ARCserve Backup Windows and UNIX/Linux and Mac agents to r12.5. (Netware, AS400 and Open VMS agents prior to this release need not be upgraded.)

To deduplicate data during a backup job, set up the job as usual and select a properly configured deduplication device as the backup destination, or as the staging location in a disk to disk to tape backup job. To configure deduplication devices, refer to the topic, [Deduplication Device Management](#) (see page 341). To assist you as you determine where to add deduplication device groups, consider the following:

How often does the data you back up change?

Consider deduplicating data that remains relatively stable between backups. The less data changes between backups, the greater the incidence of identifying duplicates.

How long should backup images be retained?

Consider deduplicating data that must be retained for long time periods. Deduplication fits more backups onto the same physical media.

What type of data is suitable for deduplication?

There is no limitation on data type.

How large is your data size?

Huge backup data streams are good candidates for deduplication.

What is your backup window?

Deduplication happens on the backup server, which means data is transported over the network and then deduplicated.

What are the system requirements for backup servers when performing deduplication backup jobs?

The answer to this question depends on how much data you need to back up, with approximately 110MB of data per backup stream required. The following are suggested guidelines:

For less than 500 GB, 1 CPU

For 500 GB to 2 TB, 2 CPUs

For greater than 2TB, 2 dual core CPUs

Example

Suppose you backup 10 TB to a 25 TB disk, which means you can store a full backup for just one week. Using data deduplication, your first full backup might require only 8 TB of space. However, subsequent backups performed with data deduplication might require only as much as 800 GB (about 10% of its former space requirements). You would then be able to store about 20 full backups - about 5 months of backups - on the same disk.

Using this example, you could retain backup images:

- 2 weeks without deduplication
- 20 weeks with deduplication

Deduplication Considerations

Some data deduplication characteristics and considerations are as follows:

- You can specify a data deduplication device as the destination in a regular backup job.
- You can specify a data deduplication device as the staging device, the final destination device, or both. However, you cannot choose the same deduplication device for both staging and final destinations.
- You can specify different retention schedules for different jobs that all use the same deduplication device.
- You can Optimize data deduplication to improve throughput by deduplicating only the files that have changed since the last backup, except for stream-based files, such as SQL, SharePoint, Exchange, and Oracle data, which cannot be optimized. Optimization is enabled by default.
- You can create deduplication devices only on NTFS volumes.
- Deduplication groups are excluded from jobs that use * groups.
- You cannot use Encryption or Compression with deduplication devices.
- You can specify a purge policy for final destination when using a deduplication device. This is not possible using a normal FSD.
- You can specify a GFS rotation to a deduplication device where all full and incremental/differential backups are submitted to the same device, whereas GFS jobs to an FSD create daily, weekly, and monthly media.
- Due to the manner in which Oracle RMAN backup session header data is populated, the deduplication process cannot detect duplicate Oracle RMAN backup sessions and deduplicate the redundant sessions.

- Due to the manner in which AS400 backup session header data is populated, the deduplication process cannot detect duplicate AS400 backup sessions and deduplicate the redundant backup sessions.
- CA ARCserve Backup cannot deduplicate redundant NetWare backup sessions that contain a session path that is greater than eight characters.

Supported Functions Matrix

The following table shows what functions are supported with Data Deduplication.

Function	Supported	Not Supported
Compression ¹		X
Device Format	X	
Device Erase	X	
Deduplication in Windows, UNIX/Linux and Mac agents prior to r12.5		X
Deduplication in NetWare, AS400 and Open VMS agents prior to r12.5	X	
Deduplication in Windows, UNIX/Linux and Mac at r12.5 and later	X	
Encryption ²		X
Image Backup	X	
Migration (Copy Policy)	X	
Maximum Threshold	X	
Minimum Threshold		X
Multistreaming	X	
Multiple Concurrent Streams	X	
Multiplexing ³		X
Optimization in Deduplication	X	
Retention of Staging (Purge Policy)	X	
Scan Jobs	X	
SnapLock		X
Used by jobs using * groups		X
Used in media pools		X

Function	Supported	Not Supported
Used in GFS Rotations	X	
Used as Staging Location	X	
Used as Final Destination Location	X	

¹ Compression at agent or server is not supported

² Encryption at agent or server is not supported

³ You could use multiple concurrent streams instead of multiplexing

Licensing Requirements for Deduplication

No additional license is required to perform data deduplication because functionality is built into the CA ARCserve Backup base product. However, please consider the following:

- Deduplication devices can be used in disk to disk to tape or disk to tape to tape (disk staging) operations, but in order to use the disk staging feature, you must license the CA ARCserve Backup Enterprise Module.
- For deduplication, you should upgrade your Windows, UNIX/Linux and MAC client agents to this release. (Agents for NetWare, AS400 and Open VMS do not require upgrade.)
- To back up deduplication device files, you need the CA ARCserve Backup Agent for Open Files. On Windows 2003 and 2008 systems, only the license for the Agent for Open Files is required; the Agent does not need to be installed. On Windows 2000 systems, the Agent must actually be installed in order to back up deduplication device files.

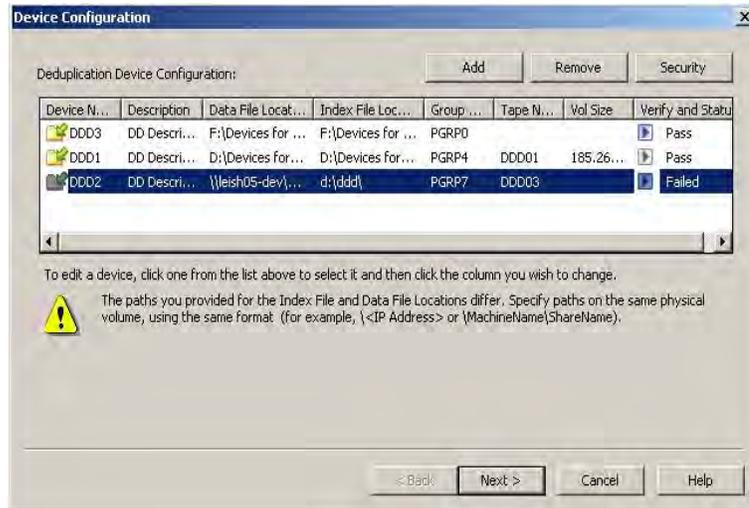
For more information on protecting the deduplication device itself, see [How to Back Up Deduplication Devices](#) (see page 689).

How to Configure Your Implementation for Deduplication

To use the CA ARCserve Backup deduplication feature, you must create and configure data deduplication device groups that contain a device set up for deduplication. The deduplication device configuration process is similar to creating a file system device (FSD). Once deduplication devices have been created and assigned to groups, you then choose a deduplication device group when you configure backup jobs.

You must specify the following information:

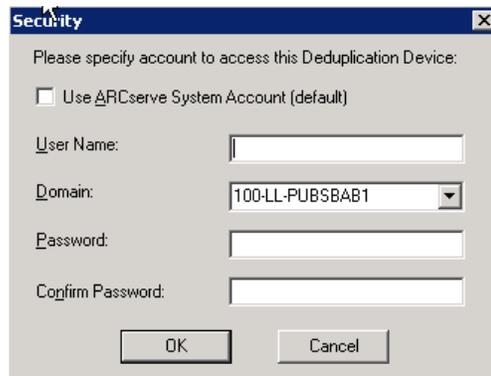
- The complete UNC path, if remote device.
- The path name to the directory that stores index files. Index files are the metadata files produced during deduplication.
- The path name to the directory that stores data files. We recommend a different path than what you specified for the index files directory.



Devices are verified as they are created. For more information on the status displayed in the Verify and Status column, see [Create Deduplication Devices](#) (see page 341).

Note: CA ARCserve Backup supports configuring an aggregate total of 255 FSDs and DDDs (only if the number of physical devices configured is 0).

Note: Deduplication devices may be created locally or remotely. If you are creating a remote deduplication device, click Security and enter login credentials.



You can also configure deduplication devices directly from the Device or Backup Manager screens by clicking Create Deduplication Device in the properties pane. For more information, see [Deduplication Device Management](#). (see page 341)

Deduplication Device Group Configuration

Data deduplication devices must be assigned to groups. If you do not specify your own group, a new default group is created and the deduplication device is automatically assigned to it at creation. You may not assign more than one deduplication device to the same group.

You may rename a deduplication group, remove a deduplication device from a group, or assign a deduplication device to an empty group.

You cannot convert a deduplication group to a staging group, nor can you convert a staging group to a deduplication group.

The following are some key distinctions between a staging group and a data deduplication device group:

- A staging group cannot be formatted or erased. A deduplication group can be formatted or erased.
- A staging group cannot be used as a backup destination. A deduplication group can be used as a backup destination.

Device Commands for Data Deduplication Devices

The device commands that are available for data deduplication devices are:

- **Format**--Deletes the sessions from that device and rewrites the header file with a new tape name
- **Erase**--Deletes the sessions and writes a blank header file on the device

Backup Data with Deduplication

You can back up and deduplicate data in two ways:

- **Regular backup job** -- Select a deduplication device group as the backup destination.
- **Staging backup job** -- Select a deduplication device group as the staging location, the final backup destination, or both provided you do not select the same deduplication device group.

How Regular Backup Jobs Work with Deduplication

Deduplicating data during a backup job operates much like a normal backup job, except you must select a deduplication device group as the backup destination.

- Specify local backup options as usual except for Compression and Encryption options. Deduplication does not support Compression and Encryption. If CA ARCserve Backup detects an encrypted session, deduplication is skipped and the job proceeds as a normal backup job. Refer to the section, [Compression and Encryption with Deduplication](#) (see page 687) for more information.
- Specify Global Options as usual:
 - Select a backup source.
 - Choose a deduplication device as the backup destination for a regular backup job. For more information, see [Deduplication Device Management](#). (see page 341)
 - Set up a schedule, including GFS rotation, if desired. For more information, see [GFS Rotation Jobs on Deduplication Devices](#) (see page 699).
 - Specify a purge policy. For more information, see [How to Specify Deduplication Device Copy and Purge Policies](#). (see page 687)

Refer to the section, [Submit a Backup Job](#) (see page 129), for the complete procedure on creating backup jobs.

How Staging Jobs Work with Deduplication

In a disk to disk to tape operation, you may specify a deduplication device group as the staging location, the final backup destination, or both, provided the *same* deduplication device group is not selected on both tabs.

- On the Staging tab, select the deduplication device group, enable staging and specify a staging policy.
- On the Destination tab, select a different deduplication device group and specify a purge policy. If you do not specify a purge policy, the default value of 4 weeks is inherited from deduplication device creation for full backups, and 2 weeks for incremental/differential backups.
- On the Schedule tab, set up the rotation or GFS schedule, if desired.

For more information, see [How to Submit a Disk Staging Backup Job](#) (see page 215).

Back up Data with Deduplication in a Staging Backup Job

You can select to deduplicate data during the staging phase, the migration phase, or both phases of a disk staging backup job by selecting deduplication device groups on the appropriate tabs.

To back up data with deduplication in a staging backup job

1. Open the Backup Manager, click the Source tab, browse to and select the source objects you wish to back up.
2. Click the Staging tab and expand the Staging Servers object.
 - a. Browse to and select the deduplication group you wish to choose as the staging group for this backup job.
 - b. Click Enable Staging.
 - c. Click Policy to open the Deduplication Staging Policy dialog.
 - d. Specify the staging policies for full, differential and incremental backups required for your job.
3. Click the Destination tab and expand the Servers object.
 - a. Browse to and select the group you wish to use as the final destination for this backup job.

Note: You may select a regular device group or another deduplication group, but you may not select the same deduplication group you specified as the staging destination.

- b. Click Deduplication Policy to open the Deduplication Purge Policies dialog.
- c. Click the Full Backup tab and specify the purge policy for full backups required for the job.
- d. Click the Differential/Incremental Backup tab and specify the purge policy for incremental and differential backups required for the job.
 - **Purge data after** -- Specify the number of weeks, days, hours and minutes to purge the job session after the operation ends.

Note: Make sure you view the deduplication staging policy because the default deletion policy is set to four weeks. If you wish to retain backups longer than four weeks, you must manually adjust the policy.

- e. Click the Miscellaneous tab and choose the desired miscellaneous options:
 - **Purge cancelled sessions from disk** --Removes any user-cancelled sessions from the deduplication device.
 - **Purge failed sessions from disk**--Removes any sessions that fail from the deduplication device.
- f. Click OK.

4. Click the Schedule tab and specify the schedule that you want to use for the backup job.

Note: If you choose Use Rotation Scheme and Enable GFS, the Media Pool fields are not available for deduplication device groups.

5. Click the Options button on the toolbar to open the Global Options dialog. Set up Global Options as usual.
6. Click Start to submit your job, as usual.

More information:

[Submit a Backup Job](#) (see page 129)

[Global Backup Options](#) (see page 140)

[Specify Copy and Purge Policies for Disk Staging Backups](#) (see page 205)

Configure Deduplication Groups to Use Staging

Regular FSD groups can be configured for staging using the Configure Staging Groups option in the device properties section of Backup Manager. This option does not apply to deduplication device groups.

Data deduplication devices can be configured for staging using only the following procedure.

To configure data deduplication device groups to use staging

1. From the Protection & Recovery menu in the Navigation Bar on the CA ARCserve Backup Manager Console, click Backup.
2. Click the Staging tab and choose a data deduplication device group to use as the staging destination.
3. Click Enable Staging.
4. Configure staging policies as usual.

More information:

[Backup Staging Methods](#) (see page 190)

How to Specify Deduplication Device Copy and Purge Policies

- If you use a deduplication device as the destination in a non-staging backup job, you may configure purge policies. Click Deduplication Policy. The policy is enabled by default.
 - On the Full Backup and Differential/Incremental Backup tabs, specify a purge policy, if desired. The default setting is 4 weeks for full backups and 2 weeks for incremental/differential backups.
 - On the Miscellaneous tab, choose the desired options.
 - **Purge cancelled sessions from disk** -- Use this option to delete sessions from the destination device after a backup to destination device is cancelled.
 - **Purge failed sessions from disk** -- Use this option to delete sessions from the destination device after a backup to destination device fails.

Both options help reclaim disk space as quickly as possible.

- If you use a deduplication device in a staging job as a staging device, you can specify both copy and purge policies by clicking Policy from the Staging tab. For more information, see Specify Copy and Purge Policies for Disk Staging Backups.
- In staging jobs where you use deduplication devices for both staging and destination locations, your jobs will have two purge policies.

Purge policy is always enabled. You cannot disable purge, but you can adjust the purge schedule.

Compression and Encryption with Deduplication

Compression and encryption are not supported when used with deduplication devices. However, in staging jobs, compression and encryption are not supported in the Staging phase, but are supported in the Migration Phase only when the final destination specified is a non-deduplication device. The following table lists the options available depending on the device specified.

Staging Destination	Final Destination	Compression/Encryption Options Available
Non-deduplication device	Non-deduplication device	All options are available.
Non-deduplication device	Deduplication device	Encrypt Data options not allowed Compress Data options not allowed
Deduplication device	Non-deduplication device	Encrypt Data options: "None", "At Backup Server During Migration" Compress Data options: "None", "At Backup

Staging Destination	Final Destination	Compression/Encryption Options Available
Deduplication device	Deduplication device	Server During Migration" Encrypt Data options are not allowed. Compress Data options are not allowed. You can still select them, but an error message will appear.

View Compression Results after Deduplication

You can view the compression ratios achieved after a backup job with deduplication is completed in the Activity Log. Compression is displayed as a ratio and as a percentage. This information is also stored in the CA ARCserve Backup database, so you may view it in Job History at the session level, job level and node level.

- From the Restore Manager, you can view session level compression ratio information.
- From the Backup, Restore or Device Managers, you can view the device/tape level compression ratios.
- From the Report Manager, you can view the session compression ratio from the Session Details and Session Reports. You can view device level or node level compression ratio from the Dashboard report.

The compression ratio is the result of the amount of actual data to be stored divided by the amount of data stored after deduplication expressed as a ratio or as a percentage.

How to Back Up Deduplication Devices

The index and data files produced during a deduplication backup job are critical to successfully restoring deduplicated data. If these files should become corrupt, CA ARCserve Backup will not be able to find and reassemble the data chunks needed to rebuild the original data stream, even if the deduplicated data is intact. You can back up deduplication device files, but there are some important considerations you should first understand.

- Deduplication device files are normally skipped in local backup jobs (deduplication device and CA ARCserve Backup are on the same machine). However, you can forcibly include them by opening Global Options and enabling "Back up deduplication device data" on the Operation tab.
- Deduplication device files are normally included in remote backup jobs (deduplication device and CA ARCserve Backup on different machines). However, there is a possibility that data and index files might be out of sync if other backup jobs to the deduplication device are running at the same time while the deduplication device is being backed up. We therefore recommend licensing the CA ARCserve Backup Agent for Open Files and using deduplication devices on machines that support VSS. For more information, see [Back up Deduplication Device Files](#) (see page 689).
- To back up deduplication device files, you need to license the Agent for Open Files. On Windows 2003 (and above) systems, there is no need to actually install the Agent for Open Files, but on Windows 2000 systems, you need to install the Agent for Open Files and apply the license so that deduplication device files can be backed up.

To restore deduplication devices, refer to the topic [Restore Deduplication Device Files](#) (see page 696).

Back up Deduplication Device Files

The procedure for including the deduplication device data and index files during a backup job is the same whether the device is locally or remotely connected to the CA ARCserve Backup server.

Note: If you are backing up data to a deduplication device, and CA ARCserve Backup is backing the deduplication device to another device, the data that is backed up on the deduplication device may not be complete on the other device. If you want to back up a deduplication device completely, you should back up the deduplication device while it is not in use by other jobs.

To back up deduplication device files

1. Ensure that you have licensed the CA ARCserve Backup Agent for Open Files so that files in use can still be backed up. If the deduplication device is connected locally to the backup server, you must issue the license on the backup server.
2. Ensure that the machine to which the deduplication device is connected supports VSS.
3. Configure backup job options as usual:
 - a. Select the deduplication data folder and index folder of the device you wish to back up. (If these folders reside on different volumes as recommended, they are backed up to two different sessions.)
 - b. From the Global Options Operation tab, enable Back up deduplication device data.
 - c. From the Global Options Volume Shadow Copy Service tab, enable Use VSS and disable Revert to traditional backup if VSS fails. If you do not perform this step, then the backup job automatically enables this option when the backup job runs.
4. Save and run the backup job as usual. For more information, see [Backing up Data](#) (see page 125).

Note: The ca_backup command line utility does not support the process of backing up data that belongs to deduplication devices.

How to Replicate Deduplication Devices with CA XOsoft

Deduplication devices can store data from numerous data sources, making protection of these devices especially critical. You can use CA XOsoft to replicate deduplication device data, adding another layer of protection to your CA ARCserve Backup environment.

Replicating deduplication devices using CA XOsoft requires you to install the CA XOsoft Engine on both the Master and Replica servers. See the *CA XOsoft Installation Guide* for more information.

- The local server hosting the deduplication device you wish to replicate should be designated as the Master server.
- The server running Windows Server 2003 or later should be designated as the Replica server.

Note: After you install the CA XOsoft Engine on both the Master and Replica servers, you must create and configure a CA XOsoft scenario for the deduplication device that you wish to protect. If a deduplication device fails, you can restore data using the VSS snapshot generated by CA XOsoft.

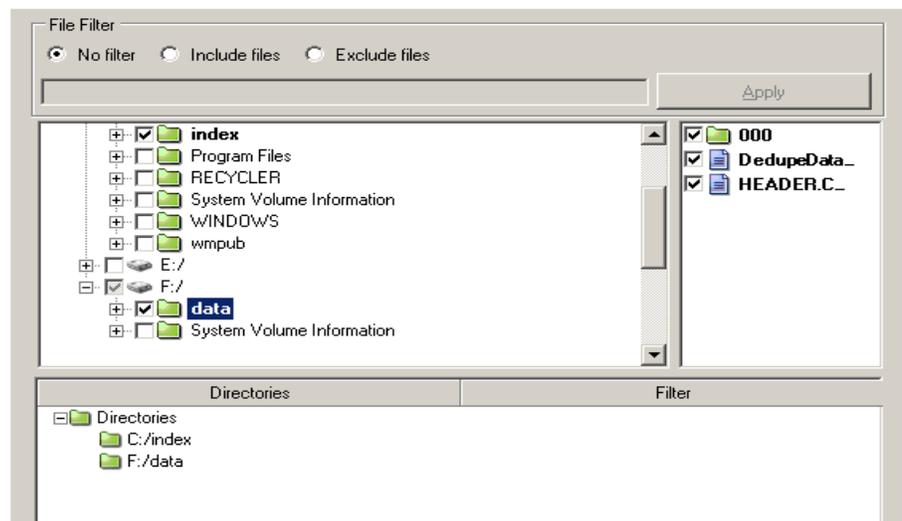
Create CA XOsft Scenarios for Deduplication Devices

The following procedure is presented to replicate deduplication devices using CA XOsft scenarios, specifically, a CA XOsft File Server scenario. For more information, see the CA XOsft User Guide.

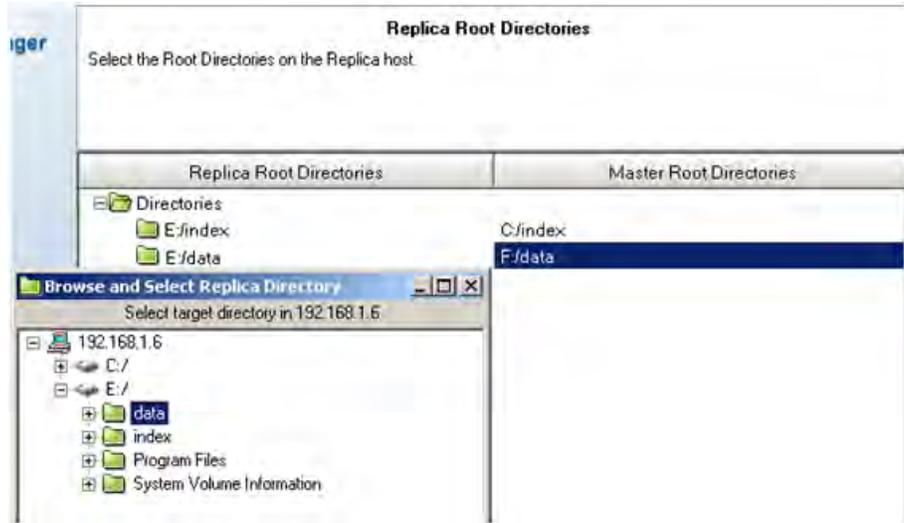
Important! The Master server is the local host for the deduplication device you wish to replicate.

To create CA XOsft scenarios for deduplication devices

1. From the CA XOsft Manager, choose Scenario, New, or click the New Scenario button from the toolbar to launch the Scenario Creation Wizard.
2. At the Welcome screen, select Create New Scenario, select an appropriate Group, and then click Next.
3. At the Select Server and Product Type screen, select File Server, Replication and Data Recovery Scenario (DR) and Integrity Testing for Assured Recovery (AR). You must choose the Integrity Testing for Assured Recovery (AR) option to generate the VSS Snapshots used for recovering failed deduplication devices. Click Next to continue.
4. At the Master and Replica Hosts screen, provide a Scenario Name. For example, DDD. Enter the Hostname or IP address and Port Number for both Master and Replica servers. Click Next to continue.
5. Wait for Engine Verification to complete. If needed, click Install to upgrade the Engine on one or both servers and then click Next to continue.
6. At the Master Root Directories screen, select the deduplication device data file folder and index file folder. Click Next to continue.



- At the Replica Root Directories screen, select the data file folder on the Replica server. Due to the size of the VSS snapshot, we recommend that you put the index and data files for the deduplication device being replicated on the same volume. Click Next to continue.



- At the Scenario Properties screen, accept the defaults and click Next to continue.
- At the Master and Replica Properties screen, accept the defaults and click Next to continue.
- Wait for Scenario Verification to complete. If errors or warnings are listed, resolve them before continuing. Click Next to continue.
- At the Scenario Run screen, do NOT click Run Now. Click Finish.

You must complete the Configure CA XOssoft Scenarios for Deduplication Devices procedure before you can run the scenario.

Configuration Considerations for CA XOssoft Deduplication Device Scenarios

To replicate deduplication devices using CA XOssoft, there are two configuration methods to consider:

- Online Replication Type** -- the deduplication device is replicated to the Replica server in real-time. This may impact device performance, which you can address by configuring the scenario spool on a separate hard disk. For more information on Spool size, see the CA XOssoft User Guide.
- Scheduled Replication Type** -- the deduplication device is replicated to the Replica server at the time you schedule. If you specify a time during which no jobs are running, the impact to the device is minimized.

Configure Online CA XOssoft Replication Scenario for Deduplication Devices

To configure scenarios for online replication

1. From the CA XOssoft Manager, select the scenario you created to replicate the deduplication device.
 - a. Click the Properties tab for this scenario.
 - b. Set the Replication, Mode property to Online.
2. From the CA XOssoft Manager, select the Master server to which the deduplication device is locally connected.
 - a. Click the Properties tab for this server.
 - b. Set the Spool, Spool Directory property to a folder on a different hard disk than the deduplication device. This improves performance.
3. From the CA XOssoft Manager, select the Replica server.
 - a. Click the Properties tab for this server.
 - b. Set the Scheduled Tasks, Replica Integrity Testing for Assured Recovery, Action on successful test, Create Shadow Copy (VSS) property to On.
 - c. Set its child properties as desired:
 - Number of Snapshots to keep -- 10 is used as an example. Raise or lower this value, as desired.
 - Shadow Storage Volume -- Default
 - Max Storage Size per Volume -- Unlimited
 - d. Set the Scheduled Tasks, Replica Integrity Testing for Assured Recovery, Scheduler property.
4. Save the changes.

Run the deduplication device replication scenario.

Configure Scheduled CA XOssoft Replication Scenarios for Deduplication Devices

When you use scheduled replication for your deduplication device replication scenario, you must manually generate VSS Snapshots in order to restore data in case of device failure.

To configure scenarios for scheduled replication

1. From the CA XOssoft Manager, select the scenario you created to replicate the deduplication device.
 - a. Click the Properties tab for this scenario.
 - b. Set the Replication, Mode property to Scheduling.
 - c. Schedule the replication time at 0:00 daily.

2. From the CA XOsoft Manager, select the Replica server.
 - a. Click the Properties tab for this server.
 - b. Set the Scheduled Tasks, Replica Integrity Testing for Assured Recovery, Action on successful test, Create Shadow Copy (VSS) property to On.
3. Save the changes.
4. Run the deduplication device replication scenario.
5. Manually generate VSS Snapshots:
 - a. Select the Replica server for the deduplication device replication scenario you created.
 - b. Click the Replica Integrity Testing button on the CA XOsoft Manager toolbar.
 - c. When the Replica Testing for Assured Recovery screen opens, click OK to start.

Global Deduplication

Global deduplication finds redundancies between C:\ drive backup sessions on different machines being backed up to the same deduplication device. Generally, the C:\ drive of a given machine holds operating system files, where high instances of redundancy are expected.

Global Deduplication happens every 6 hours but cannot happen while a backup or purge job is active, and will be interrupted if both jobs need to access the same session file.

To perform global deduplication, set up a backup job in the usual manner, ensure you have checked the Enable Global Deduplication option in Deduplication Device Group Configuration and you have select the C:\ drives of different machines specified as the backup source.

How Global Deduplication Works

Global deduplication finds redundant data between backup sessions of C:\ directories performed from different machines. Ensure Global Deduplication is enabled and then select the backup sessions previously performed as the source for the global deduplication job.

Perform Global Deduplication

To minimize data store requirements for operating system and other files on C:\ drives across different machines, perform Global deduplication.

To perform global deduplication

1. From Deduplication Device Group Configuration, ensure the Enable Global Deduplication option is set (default setting is enabled).
2. From the Backup Manager, set up a backup job in the usual manner.
3. From the Source tab, select the Windows C:\ volume directories of different machines.
4. (Optional) If using staging, click the Staging tab and select a deduplication device group.
5. From the Destination tab, select a deduplication device group.
6. Complete the job setup selections as usual.
7. Run the job.

More information:

[Submit a Backup Job](#) (see page 129)

[Configure Deduplication Groups](#) (see page 353)

Recover Deduplicated Data

Restoring data that has been deduplicated follows the same procedure as a normal restore job. Disaster Recovery supports deduplication and also follows the same procedure as a normal disaster recovery.

The CA ARCserve Backup Utilities also support deduplication devices.

Note: The Purge utility is assigned a lower priority than Backup, Restore, Merge and Scan. Purge is skipped when any active backup, restore, merge, or scan jobs are active on the same deduplication device. Backup, restore, merge, and scan jobs directed to a deduplication device where a purge session is already in progress take precedence and will halt the purge session.

Restore Deduplicated Data

The process of restoring data saved to deduplication devices is similar to that of normal FSDs. You must restore from a disk, even if you have migrated data to tape as part of a staging job.

More information:

[Restoring Data](#) (see page 239)

Restore by Sessions on Deduplication Devices

If a deduplication device contains a large number of sessions, you can use the Last number of days option to filter results. When you expand the device, a progress bar appears. You can cancel progress to display a shortcut menu and then select a target session from the expanded device to restore. You can also expand the remaining sessions using the Show More option from the shortcut menu.

Restore Deduplication Device Files

As long as you have also explicitly backed up the deduplication device data and index files, you can restore deduplicated data. To restore deduplication device files, do the following:

- Browse the node on which the backed up index files are stored
- Choose the correct sessions
- Choose the index or data files you wish to restore
- Restore to an alternate location
- Remove the original deduplication device to avoid conflicts
- Create a new deduplication device configured to use the restored index and data folders
- Stop and then restart the Tape Engine to ensure that any operations taking place when the back up was initiated are invalidated
- Merge the new deduplication device so that records match the physical device.

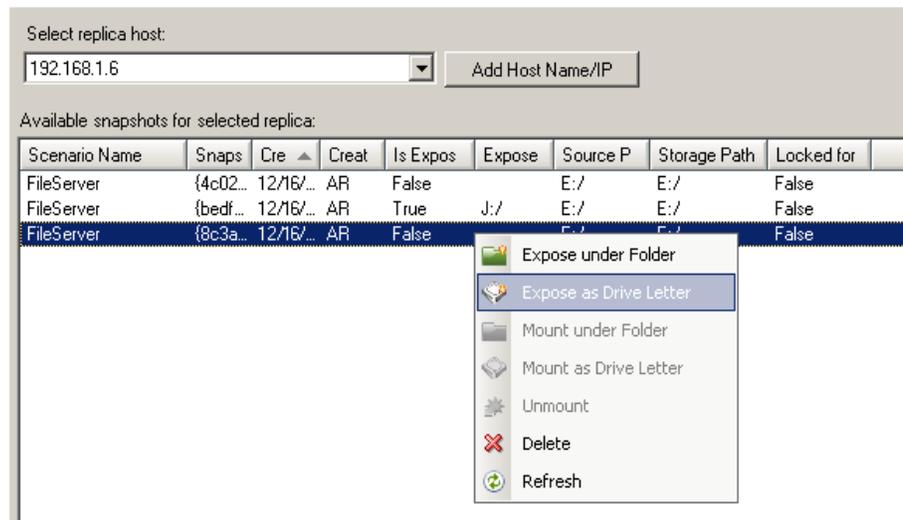
Note: The Merge operation may be incomplete or fail if there are active sessions on the backed up Deduplication device.

Restore Deduplication Devices Using CA XOssoft/VSS Snapshots

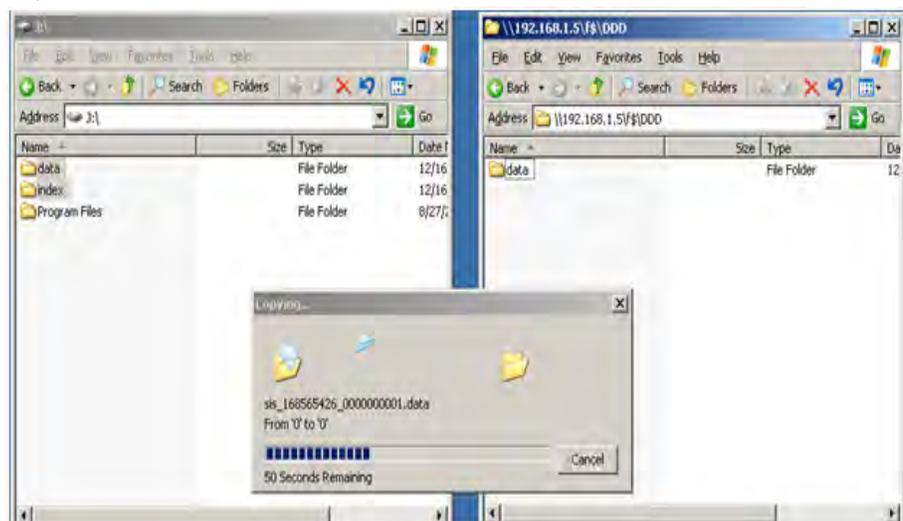
If a replicated deduplication device fails, you can recover the data stored on it using the VSS Snapshots.

To recover a failed deduplication device

1. From the CA XOssoft Manager, stop the replication scenario.
2. Expose the VSS Snapshot:
 - a. Click Snapshot View and select the snapshot from which you wish to restore.
 - b. Select Expose as Drive Letter to start the restore process.



3. Log on to the Replica server, open the exposed drive, and copy the exposed index and data files to an alternate location.



4. From the CA ARCserve Backup Device Manager, remove the failed deduplication device. This device must be removed to avoid conflicts in which two devices exist with the same tapeName, randomID, and sequenceNum.
5. From the CA ARCserve Backup Device Manager, create a new deduplication device using the index and data file paths just copied. For more information, see [Create Deduplication Devices](#) (see page 341).
6. Stop and restart the Tape Engine to ensure any operations taking place during backup initiation are invalidated.
7. Merge the new deduplication device so that the DB tape record is updated to match the physical deduplication tape. Use the Merge session header only option from Merge Global Option, Database menu to do so. The Merge operation may be incomplete or fail if there are active sessions on the backed up Deduplication device.

You may need to create a new CA XOssoft scenario to replicate the new deduplication paths. To use the existing scenario, you can restore the Snapshot to previous deduplication paths, but you will need to first delete or move any files presently stored there.

Scan Jobs with Deduplication

The process of running a Scan job with deduplication is the same as a regular Scan job. If desired, click the Media Assure button to access Media Assure options, then click the Enable Media Assure option to select it.

Media Assure works with all media types but for deduplication devices where hundreds of sessions are stored, it randomly samples the sessions that meet your criteria to ensure data can be recovered.

You can scan all data (default) or only session headers, as well as set filter options. You can specify one node or multiple nodes, separating names with commas in the field provided. You cannot specify * groups for deduplication Media Assure scan jobs, but you can specify a * tape in a specific group, or you can select a specific tape. The job scans the sessions that satisfy your selection criteria and repeats periodically until deleted.

Note: Media Assure supports scanning only one group and is suspended by other jobs targeting the same media. If suspended, an error is produced, "E3708 Unable to reserve group <group name> in <minutes> minutes."

More information:

[Media Assure & Scan Utility](#) (see page 32)

Merge Jobs with Deduplication

The process of performing a Merge job with deduplication is the same as a regular Merge job. For more information, refer to the topic, [Merge Utility](#) (see page 31).

GFS Rotation Jobs on Deduplication Devices

Deduplication devices cannot be assigned to media pools, so consider the following when setting up a GFS or Rotation scheme on these devices:

- When you select a deduplication device as the destination device in a staging operation on a GFS or Rotation job, you will not be permitted to specify a media pool name. You will be permitted to submit the GFS or Rotation scheme without media pool.
- When you select a deduplication device as the destination device in a GFS or Rotation job in a non-staging operation, media pool is not used and media will never be overwritten. Data is written to formatted media in the deduplication device group, if one exists. If one does not exist, blank media is formatted with the current data and time.
- When you select a deduplication device as the destination device in a GFS or Rotation job in a staging operation, the behavior of the staging phase is not changed, but the migration phase will never use a media pool and never overwrite media. Data is appended to formatted media in the deduplication device group if one exists. If not, blank media is formatted with the current date and time.
- With GFS or normal rotation, with Append Media or without Append Media, backup jobs saved to deduplication devices behave in the same way.

Refer to the topic, [Rotation Schemes](#) (see page 113), for more information on GFS rotation.

Deduplication Device Purge

Purging a deduplication device is different than purging a staging FSD. When a staging FSD is purged, CA ARCserve Backup immediately removes the session file. But for a deduplication session purge, CA ARCserve Backup renames the session hash file to `.hash_ToPurge` and updates the reference counter. In other words, the session is merely "marked" as purged, but not actually removed because there may be other sessions that still point to the original data.

The reference counter stored in the index files is decreased. When the reference counter reaches 0, no more hashes referencing the original data exist and the data chunk is now considered to be a "hole." When CA ARCserve Backup finds data files with holes greater than 25%, disk space is reclaimed by a purge thread that runs every 6 hours.

Disk Fragmentation

To reduce disk fragmentation, space is always allocated for the first backup of a given session in 1 GB increments, until the session ends. If four streams are writing, each stream uses a pre-allocated chunk of disk space. The last 1 GB chunk of data is rounded down to 512 MB as long as the size of that chunk is less than 512 MB. This process ensures the disk is fragmented in 1 GB chunks.

This is done only for backups to deduplication devices and only for the first backup of one root directory on one device.

For second backup and subsequent jobs, the amount of data physically written to disk is expected to be low.

Deduplication Reports

CA ARCserve Backup reports have been modified to include deduplication statistics. See [Report Categories](#) (see page 621) for more information.

Appendix C: Using CA ARCserve Backup in a Storage Area Network

The following topics provide an overview of Storage Area Network (SAN) support for CA ARCserve Backup.

This section contains the following topics:

[How to License the Storage Area Network \(SAN\) Option](#) (see page 701)

[The SAN Environment](#) (see page 702)

[Installing the SAN Option](#) (see page 705)

[Using the SAN Option](#) (see page 709)

[Troubleshooting SAN Configurations](#) (see page 714)

How to License the Storage Area Network (SAN) Option

To successfully license CA ARCserve Backup Storage Area Network (SAN) Option, you must fulfill the following installation requirements:

- You must install and license the option to perform backup operations to libraries that are shared on a SAN.
- You must install the option on the CA ARCserve Backup Primary server.
- You must issue all licenses on the primary server.
- Ensure that you have a sufficient number of Storage Area Network (SAN) Option licenses to support your environment.

The Central Management Option is a prerequisite component for the Storage Area Network (SAN) Option.

The Storage Area Network (SAN) Option is a count-based license. You must issue one license for all ARCserve servers that share a library with another ARCserve server.

Examples: How to License the Storage Area Network (SAN) Option

The following examples describe how count-based licensing works with the Storage Area Network (SAN) Option:

- Your environment consists of a primary server and three member servers. The primary server and the three member servers share a multiple drive library on a SAN. This configuration requires you to issue four Storage Area Network Option (SAN) licenses issued on the primary server. All servers in the ARCserve domain are sharing a library.
- Your environment consists of a primary server and three member servers. Two member servers share a multiple drive library and the third member server is configured with a locally attached, multiple drive library. This configuration requires you to issue four Tape Library Option licenses and three Storage Area Network (SAN) Option licenses on the primary server. All servers in the ARCserve domain have access to a multiple drive library; however, three ARCserve servers are sharing a library.

The SAN Environment

The servers within a SAN group include one primary SAN server and one or more SAN-attached member servers. The primary SAN server is the most important server because no tasks can occur until it initializes the tape libraries on the SAN.

The primary SAN server is responsible for the following actions:

- Initializes, governs, and maintains a shared device on the SAN
- Coordinates the use of shared library resources among the servers in the SAN, preventing conflict if two servers try to allocate a device or media at the same time

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

When a job is ready to run, the option reserves the device and media. Once reserved, that device and media are no longer available to any other jobs across all SAN servers.

The SAN Option enables CA ARCserve Backup servers to share one or more tape libraries by creating a virtual ring. Any backup or restore jobs on a server that has the option installed run as local jobs. As the backup progresses, CA ARCserve Backup sends data over the SAN hardware to the tape libraries for storage instead of over the LAN cabling. This provides greater speed, reduces network traffic, and maximizes backup and restore throughput.

Server Management

Using the SAN Option does not change the way you manage CA ARCserve Backup servers. You continue to connect to each SAN Option server through the Backup or Restore Manager to schedule backup and restore jobs and to manage your CA ARCserve Backup database.

Backup Plans

You should plan a backup strategy that is appropriate for your SAN configuration. You should consider the impact of multiple CA ARCserve Backup servers sharing a single device. For example, if your backup device contains two tape drives and there are five option servers sharing the media libraries, you should not schedule five backup jobs to begin simultaneously. This would force the option to determine which two of the five jobs to begin first. Instead, you should carefully consider and schedule the start times for jobs to meet your backup strategy and allow you to control the schedule sequence.

Note: Each scheduled backup job waits in the queue until a tape drive is available to perform the backup.

Benefits of Using the Option

The SAN Option provides the following benefits:

Decreased Costs

Allows servers to share one or more tape libraries.

Improved Backup and Restore Speed

Eliminates the need for remote backups through your Local Area Network (LAN).

Efficiency

Centralizes the backup of hardware and media.

Flexibility

Optimizes the flexibility by redirecting or reconfiguring in case of a device failure.

Terminology

The following terms are commonly used in a SAN environment:

Storage Area Network (SAN)

A high-speed network designed for sharing attached tape libraries.

SAN server group

A group of CA ARCserve Backup servers that can share a set of tape libraries on a Storage Area Network.

Primary SAN server

The CA ARCserve Backup server that initializes the shared tape libraries and is responsible for controlling usage and detecting any changes in status of these devices.

SAN-attached Member server

Servers in a SAN that are assigned to the primary server to use the shared tape libraries.

Shared device

A device on a SAN used by a SAN server group.

Installing the SAN Option

This section explains how to install and configure the SAN option on your primary and member-attached SAN servers from one central location.

Operating System Compatibility

This SAN option is compatible with the following Windows servers:

- Windows 2000
- Windows Server 2003
- Windows Server 2008

Installation Prerequisites

Before you install the SAN Option, verify the following prerequisites:

Note: CA ARCserve Backup supports libraries configured with one drive. If your library has more than one drive, you must license the CA ARCserve Backup Tape Library Option to enable multi-drive capabilities.

- Your system requirements meet the minimum requirements needed to install the option. For more information about installation requirements, see the *Implementation Guide*.
- Your system meets the minimum hardware and software requirements needed to install CA ARCserve Backup and the CA ARCserve Backup Tape Library Option (if necessary).

- You have installed all appropriate SAN hardware device drivers for adapters to access the devices attached to the Fibre Channel adapter.

Note: For information about the SAN hardware and drivers, see the CA ARCserve Backup for Windows Certified Device List. You can access the Certified Device List from the CA ARCserve Backup home page.

- You have CA ARCserve Backup and the Central Management Option installed on the computer on which you want to install the option. In addition, if you have a multi-drive library you must also have the Tape Library Option installed. This computer can be either a local computer or a remote computer.

Note: If these applications are not already installed, you must install them when you install the SAN Option.

- These options (Central Management Option, SAN Option, and Tape Library Option) are all installed on the Primary server only.
- There is license count for the Primary server and each SAN member server. There is one Central Management Option license for the entire SAN, and one SAN and Tape Library Option license for each server in the SAN (Primary server and all associated SAN member servers.)

- You have made a note of the default installation path.
- You have administrator privileges to install software on the computers on which you want to install the option.

Note: Contact your CA ARCserve Backup administrator to obtain the proper privileges and information if you do not have them.

- You know the user names, passwords and IP addresses for the primary SAN server and SAN-attached member servers.
- You have all SAN hardware and related device drivers installed.
- The Windows backup server identifies all of the appropriate SAN devices, including the medium changer and tape drives.
- All SAN servers in your storage area network can communicate with one another by pinging each server by name or by pinging their IP address with the display server name switch.

IP connectivity and name resolution among all servers participating in the SAN is essential. To ensure you have IP connectivity and name resolution, you may need to update the IP host file on each server so that the name and IP address of each server is present in the IP host file of all other servers. The IP host file on each server are in the following folders:

- For Windows 2000: \winnt\system32\drivers\etc
- For Windows Server 2003: \windows\system32\drivers\etc
- For Windows Server 2008: \windows\system32\drivers\etc

SAN Option Installation

The SAN Option follows the standard installation procedure for the system components, agents, and options of the CA ARCserve Backup. Start all installation sessions by running setup.exe.

- You can install the CA ARCserve Backup base product, agents, and options all in one session
- You can install the CA ARCserve Backup base product first, and then install the agents and options separately later.
- You can install the Storage Area Network (SAN) Option on the primary SAN server (only).

For more information on installation, see the *Implementation Guide*.

The installation process is very flexible and allows you to decide whether to install the different system components, agents, and options of CA ARCserve Backup in one installation session or in multiple installation sessions. The preferred method is to install all of the components in one installation session. You can, however, install each component sequentially in individual sessions or install selected components in one session and other components in individual sessions later.

Before starting the installation process, decide which system components, agents, and options of CA ARCserve Backup you want to install during this session. Then, gather the prerequisite information for each of the agents and options you want to install. You can find this information in each agent and option guide. Select the combination of installation sessions that best meets your needs.

For example, to install the CA ARCserve Backup server, the Tape Library Option, and the Agent for SQL Server, you can use any of the following combinations of installation sessions:

- Install the server, the option, and the agent in the same installation session.
- Use three separate installation sessions; one session to install the server, a second session to install the option, and a third session to install the agent.
- Use two separate installation sessions. When using two separate sessions, you can group the components in the following ways: Install the server in one session and the option and agent in a separate session; install the server and option in one session and the agent in a separate session; or install the server and agent in one session and the option in a separate session.

Using the SAN Option

This section provides the information you need to use the SAN Option. Specifically, it explains how you can use the option to perform the following tasks:

- Create shared device groups
- Backup and restore data
- Manage devices
- Manage media
- Monitor job status
- Control when jobs run
- Create reports and logs
- Use virtual libraries

Create Shared Device Groups

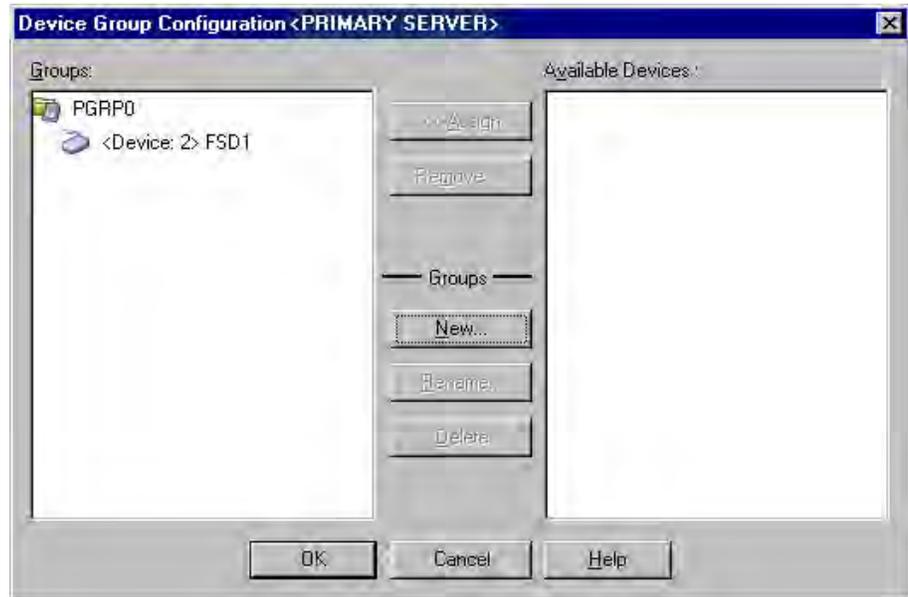
Creating shared device groups is the key to the flexibility and efficiency of CA ARCserve Backup.

Note: Shared device groups can only be modified, created, or deleted from the Primary server.

To create shared device groups

1. From the Device Manager window, select Configure Groups from the properties pane.

The Device Group Configuration dialog opens.



2. Click New.

The New Group dialog opens.



3. Select the type of device group in the Type field, and enter a name for the device group in the Name field. Click OK.

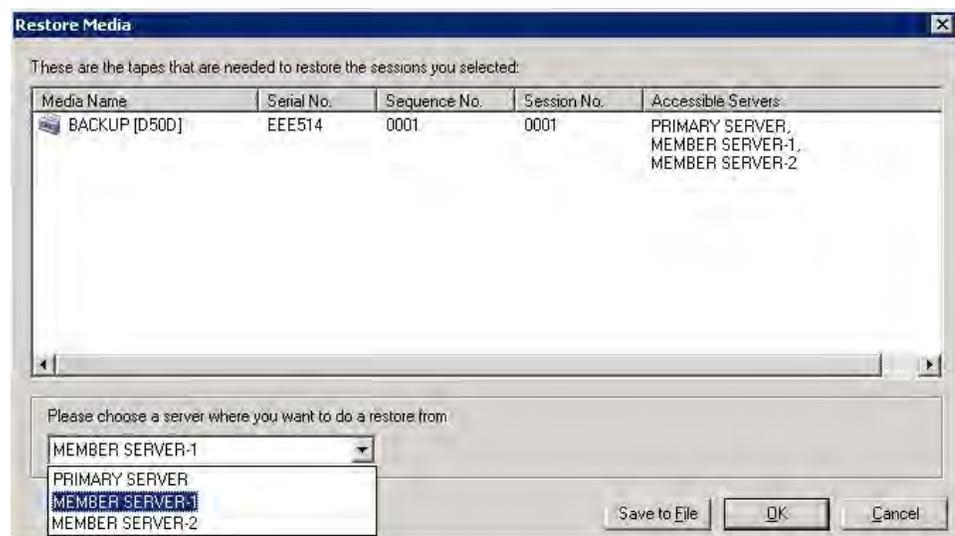
The new device group is displayed in the Device Group Configuration dialog.

Data Backup and Restore in a SAN Environment

You must use the Backup Manager or Restore Manager to configure and submit backup or restore jobs in your SAN environment. These backup and restore jobs run locally on the server where the SAN Option is installed. The data is transferred over the SAN hardware to the library instead of over the LAN cabling. This speeds up the job processing and reduces Ethernet traffic. If you use the Media view, information on backups performed by all SAN servers is available from the database.

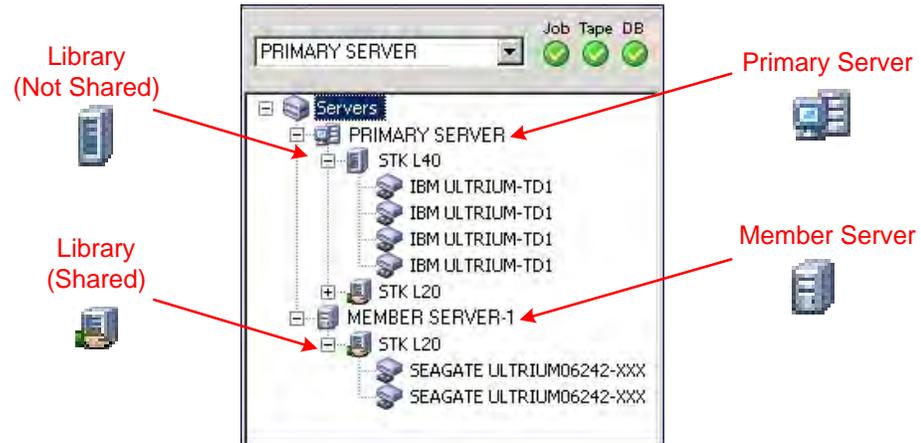
The option also provides a large number of backup and restore options, filters, and scheduling features for your jobs. For more information, see "Backing Up Data" and "Restoring Data."

When submitting a restore job of data found on a tape inside a SAN-attached Library you can use the drop down menu in the Restore Media pop up which lists all the SAN servers that the tape is accessible from. The server you select here will be the server on which the Restore operation will run and it does NOT have to be the server that actually did the Backup.



Device Management

Use the Device Manager to display information about the storage devices connected to your SAN server group, the media in these devices, and the status of these devices. Through the Device Manager, you can view all of the shared devices connected to your SAN server group.



Consider the following when managing devices:

- Each CA ARCserve Backup SAN Option installed server in the SAN server group displays the same view of the SAN attached devices.
- If you change the device configuration on the primary server (reconfiguring a library as a RAID, or add more drives to the library for example), you must stop the tape engine service on all SAN servers (primary and all member), then start the primary server Tape Engine first. After the primary server Tape Engine is running, you can then start each of the SAN attached member servers to see the new configuration correctly.

For more information about managing devices, see [Device Manager](#) (see page 355).

Media Management

Consider the following when managing media:

- Because SAN servers share media, be careful when selecting media from a scratch set. Scheduled jobs can be affected if the media is unavailable.
- Only one administrator of media pools should supervise the SAN server group.

- A tape in a save set cannot be destroyed, formatted, or erased, unless it is moved to a scratch set.

For more information about media pool management, see [Media Pool Manager](#) (see page 411).

Media Pools

A media pool is a collection of media that is managed as a set and shared in the SAN. Each media pool is assigned a name, and the media is organized by serial numbers. Manage media pools from the CA ARCserve Backup Media Pool Manager window, which you access by clicking the Media Pool Manager icon.

For more information about media pools, see [How Media Pools Work](#) (see page 401).

Control of Job Runtime

CA ARCserve Backup can determine if a device is being used by a job, even if it is on another SAN-attached server. It can then wait until the device is free before starting another job.

When there are many jobs waiting in the queue for the same device, there is no way to determine which job will run next. If priority is important, configure the start times based on how long you think the previous job will take. By carefully arranging the start times, you should have no more than one job ready to begin at a time.

For more information about scheduling, managing jobs, and the Job Status Manager, see [How You Can Use the Job Status Manager to Manage Jobs](#) (see page 298).

Reports and Logs

CA ARCserve Backup provides the following options for displaying logs and reports:

Activity Log

Contains comprehensive information about the operations performed by CA ARCserve Backup. It provides an audit trail of all backup activity, including every job that is run, and also displays the session number if you need to restore a session..

The activity log can be viewed from the Job Status Manager.

Tape Log (TAPE.LOG)

Contains all Tape Engine-related messages.

Job Log

Tracks activity related to a specific job.

Report Manager

Generates reports from the CA ARCserve Backup database for viewing or printing. You can open the Report Manager from the Quick Access menu and view reports such as the Job report, Backup Media Error report, Session report, Backup Device report, and the Media Pool report.

For more information about reporting, see [CA ARCserve Backup Logs and Reports](#) (see page 617).

ARCserve Virtual Libraries

The Tape Library Option is used in conjunction with the ARCserve virtual libraries to provide you with a versatile tool for addressing a wide range of storage requirements. The ARCserve virtual libraries work seamlessly over the Tape Library Option, allowing you to configure physical libraries into smaller virtual (logical) libraries. These virtualized libraries can share the same robotics and import/export slots, which in turn allows drives and storage slots to be grouped together.

When you use ARCserve virtual libraries, be aware of the following restrictions:

- You can configure ARCserve virtual libraries for shared Tape Libraries on the primary server only.
- If the device configuration on the primary server changes (for example, you reconfigure a library into multiple ARCserve virtual libraries), you must stop the tape engine service on all SAN servers (primary and all member), then start the primary server Tape Engine first. After the primary server Tape Engine is running, you can then start each of the SAN attached member servers to see the new configuration correctly

For more information about ARCserve virtual libraries, see [Virtual Library Configuration Option](#) (see page 335).

Troubleshooting SAN Configurations

This section provides the information you need to troubleshoot CA ARCserve Backup for Windows SAN installations.

Devices are Not Shared

Valid on Windows platforms.

Symptom:

Devices attached to the ARCserve (SAN) Primary server are NOT marked as "shared" in the ARCserve GUI.

The mechanism that is used to determine whether a device is "shared" is now dynamic. The CA ARCserve Backup Member server is responsible for detecting "shared" devices and reporting these "shared" devices to the CA ARCserve Backup (SAN) Primary server. Therefore, if the CA ARCserve Backup Tape Engine service is not running on any of the SAN-attached Member servers, then no "sharing" is occurring and the devices will not show as being "shared".

Solution:

Make sure the CA ARCserve Backup Tape Engine service has been started on at least one of the SAN-attached Member servers. If necessary, start the Tape Engine service on one or all of the SAN-attached Member servers.

Devices are Not Shared and the Tape Engine is Running

Valid on Windows platforms.

Symptom:

The Tape Engine service is up and running on all SAN-attached servers in the CA ARCserve Backup Domain, but the devices are NOT marked as "shared" in the CA ARCserve Backup GUI. The SAN-attached devices are not detected by all the SAN attached servers correctly.

Solution:

Analysis of your SAN zoning maybe necessary to make sure that all servers participating in the SAN can see all devices that are "shared" through the SAN. To do this you need to check the following:

- Check on each server that the "shared" devices can be seen by the Operating System, by checking the Windows Device Manager.
 - If the "shared" devices cannot be seen by Windows, then double check your SAN zoning to make sure this server is included. If it is included, reboot the server to get Windows to discover the devices. When you get Windows to see the devices, then you can restart the Tape Engine on that machine.
 - If the server having problems seeing the devices is the Primary server, then you need to restart the CA ARCserve Backup Tape Engine service on this server and then on all SAN-attached Member servers in that domain.

- Check if the “shared” devices can be seen by CA ARCserve Backup through the CA ARCserve Backup Device Manager, looking under each server.
 - If “shared” devices cannot be seen by CA ARCserve Backup, but Windows does see them, then you need to restart the Tape Engine service.
 - If the server having problems seeing the devices is the Primary server, then you need to restart the CA ARCserve Backup Tape Engine service on this server and then all SAN-attached Member servers in that domain.

Shared Devices Appear as Unavailable or Offline

Valid on Windows platforms.

Symptom:

The shared devices on SAN-attached Member servers are marked as unavailable or offline.

This could be caused by the order in which the CA ARCserve Backup Tape Engine services were started in the domain.

- If the CA ARCserve Backup Member server's Tape Engine service was started before the Primary server's Tape Engine has finished initializing, the Member server will wait for the Primary server for a period of time, but eventually will start without being able to “share” the devices.
- If the CA ARCserve Backup Member server's Tape Engine service was started before the Primary server's Tape Engine service was started, the Member server will wait for the Primary server, for a period of time, but eventually will start, without being able to “share” the devices.

Solution:

Check the CA ARCserve Backup Activity log to see when, and in what order the services might have started. Make sure all devices on the CA ARCserve Backup Primary server are initialized, then just restarting the Tape Engine service on the Member server(s) should be enough to resolve this.

Important! When starting the Tape Engine service in a CA ARCserve Backup Domain that is part of a SAN, it is important to always start the Primary server's service first and let it fully initialize before starting the Tape Engine service on any of the Member servers.

Shared IBM Devices Appear as Unavailable or Offline

Valid on Windows platforms.

Symptom:

The shared IBM tape devices on SAN-attached Member servers are marked as unavailable or offline.

If you have IBM Ultrium/LTO tape drives, in some cases the IBM LTO Tape driver (Windows 2000 and Windows Server 2003) will issue a SCSI Reserve command to the tape devices when the CA ARCserve Backup Primary server opens the devices. This is not a problem for the Primary server, but when the SAN-attached Member server tries to access these tape devices it will fail and the devices will not be usable from that server.

Solution:

In the CA ARCserve Backup Activity log for the Member server, you may see SCSI Port errors when the CA ARCserve Backup Tape Engine service is started and tries to access these drives.

You can configure the IBM tape driver to not issue the SCSI Reserve command by performing the following registry procedure.

1. In the registry editor, access the registry key:

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\

2. If the IBMtape driver is installed, search under the services key for a key name that is equal to the file name of the IBMtape driver.

For example, if the file name of the IBMtape driver `ibmtp2k3.sys`, the key name is `ibmtp2k3`.

Select the key, add a DWORD value named "DisableReserveUponOpen," and set it to 1.

3. Exit registry editor and reboot the server.

Backup Jobs Fail

Valid on Windows Platforms.

Symptom:

1. The CA ARCserve Backup SAN License for the server you are trying to run the backup on has expired.

Each SAN-attached server must have a SAN License. The licenses are all applied to the Primary server in the corresponding CA ARCserve Backup Domain.

2. The CA ARCserve Backup TLO License for the server you are trying to run the backup on has expired.

Each SAN-attached server sharing a multiple drive library must have a TLO License. The licenses are all applied to the Primary server in the corresponding CA ARCserve Backup Domain.

3. The CA ARCserve Backup Primary server Tape Engine service is no longer available.

Solution:

1. Check the CA ARCserve Backup Activity log for any SAN license errors.
If necessary add the applicable SAN license.
2. Check the CA ARCserve Backup Activity log for any TLO license errors.
If necessary add the applicable TLO license.
3. Check the CA ARCserve Backup Primary server Tape Engine service status
 - a. In the CA ARCserve Backup GUI, access the Server Admin screen and check the status of the Tape Engine service.
 - b. In the CA ARCserve Backup Activity log, check for a Primary server Tape Engine stop event.
 - c. In the Windows system Event Viewer, check for a Tape Engine service stop event or an exception.

If the problem is related to the Primary Tape Engine service being down, then restart and try again.

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

Appendix D: Using CA ARCserve Backup in a Cluster-aware Environment

The following topics provide an overview of CA ARCserve Backup cluster support, which allows you to back up and recover data in a cluster environment. In addition, these topics also provide information about configuring CA ARCserve Backup as a cluster-aware backup server with high availability capabilities.

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/AMD64/IA64 Windows Server
- NEC CLUSTERPRO/ExpressCluster for Windows 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, and NEC CLUSTERPRO/ExpressCluster X 2.0 for Windows

This section contains the following topics:

[Cluster Overview](#) (see page 719)

[Deployment Considerations](#) (see page 726)

[Protecting Your Cluster with CA ARCserve Backup](#) (see page 727)

[Deploy CA ARCserve Backup Server on MSCS](#) (see page 733)

[Deploy CA ARCserve Backup Server on NEC Cluster](#) (see page 747)

[Troubleshooting CA ARCserve Backup Cluster Support](#) (see page 769)

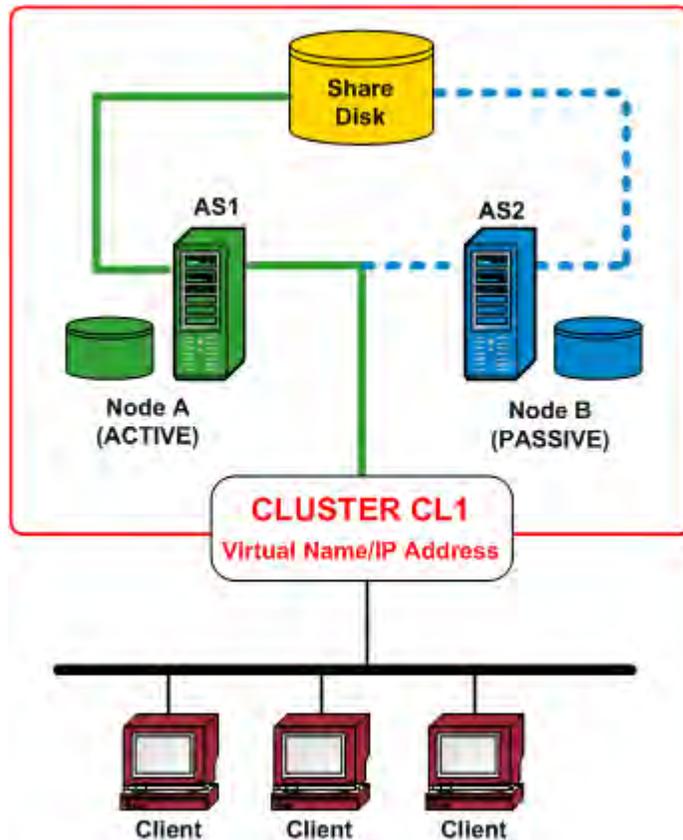
Cluster Overview

A computer cluster is a group of connected computers that work together closely so that in many respects they can be viewed as though they are a single computer. Clusters can be categorized in two types: HA (High Availability) and High Performance. Within HA clusters, there are two working modes: active/active or active/passive. Currently, CA ARCserve Backup can only be deployed in an active/passive HA mode.

The primary function of a cluster occurs when one server (or node) in a cluster fails or is taken offline. In a cluster environment, the other node in the cluster will then take over the failed server's operations. ARCserve Managers using server resources experience little or no interruption of their work because the resource functions move transparently from the active node to the failover node.

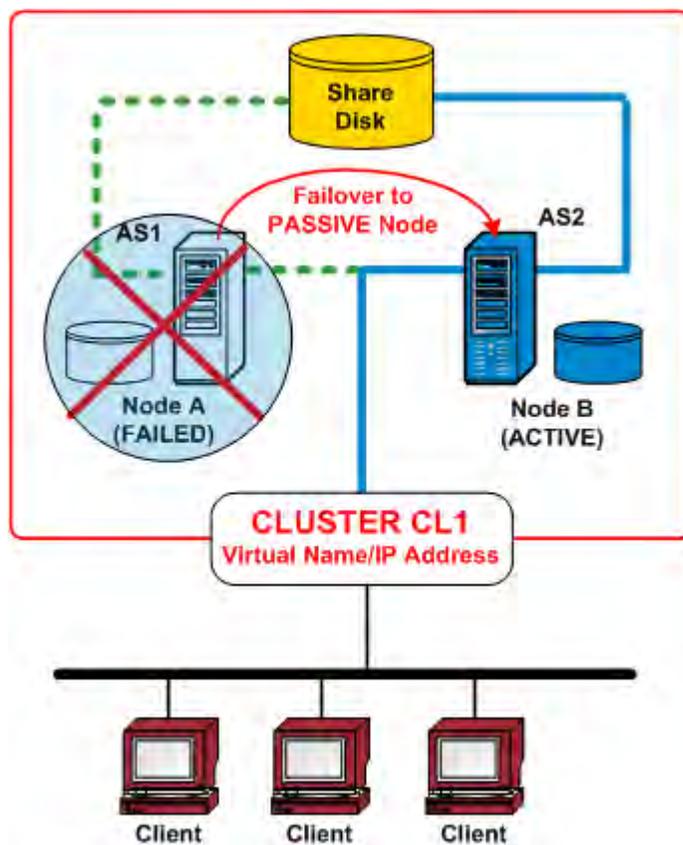
The servers within a cluster environment are not only connected physically by cables, but also programmatically through clustering software. This connection allows clustered servers to take advantage of features (such as fault tolerance and load balancing) that are unavailable to stand-alone server nodes. Clustered servers can also share disk drives that contain important information, such as a clustered database.

For example, assume node A and node B form a clustered CA ARCserve Backup HA server. The CA ARCserve Backup cluster server will work only in the "active/passive" mode, and as a result, only one CA ARCserve Backup instance is running at the same time. In this environment, ARCserve Managers could connect to the CA ARCserve Backup server AS1 or CA ARCserve Backup server AS2 without knowing which node is active and currently hosting their server. The virtual server name and IP address ensures that the server location is transparent to CA ARCserve Backup applications. To the ARCserve Manager, it appears that the CA ARCserve Backup server is running on a virtual server called CL1.



When one of the software or hardware resources fails or is shut down, a failover occurs. Resources (for example: applications, disks, or an IP address) migrate from the failed active node to the passive node. The passive node takes over the CA ARCserve Backup server resource group and now provides service.

If node A fails, node B automatically assumes the role of the active node. To an ARCserve Manager, it is exactly as if node A were turned off and immediately turned back on again. The location of the active node (A or B) in the Cluster (CL1) is transparent to CA ARCserve Backup.



How Failover Works

Failover is the process of having cluster resources migrate (or transfer) from an unavailable node to an available node. Failover is automatically initiated when a failure is detected on one of the cluster nodes. The cluster monitors resources to determine when a failure has occurred and then takes action to recover from the failure by moving the clustered resource(s) to another node in the cluster.

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 a passive node are referred to as the standby (or failover) server and the cluster system will only activate one of them in case of failover. If the active node fails, then all backup resources will migrate to a passive node, which then becomes the new active node. The new active node begins to function as the backup server, and continues the original backup operations and maintains all previous job scheduling and media management services.

CA ARCserve Backup provides the following types of failover protection:

- **Planned Failovers**--Planned failovers occur when it is necessary to perform maintenance on the active node within a cluster and you want CA ARCserve Backup to migrate the cluster resources from that active node to a passive node within the cluster. Examples for planned failovers are system maintenance, disaster recovery tests, and training. A planned failover can only be executed when no jobs are running and no other CA ARCserve Backup-related services (such as media operations, reporting, etc.) are occurring on both the primary and member backup servers.
- **Unplanned Failovers**--Unplanned failover can occur because of hardware or software failures. When the active node in a cluster fails, jobs are dispersed from the failed server and critical data (such as job information) is saved into a shared disk. When failover occurs, the cluster system will move the shared disk into a passive node and activate the CA ARCserve Backup instance in that node. After the CA ARCserve Backup services are resumed in the failover server, any failed jobs from the previous server are rerun in a new active cluster node. If checkpoint information was created by the job before failover occurred, the restarted job will resume from the checkpoint.

Resource Group

A cluster resource is any physical or logical component that can be physically shared between multiple cluster nodes, but can only be hosted (owned) by one active node at a time. The virtual IP address, virtual computer name, shared disk, and even the applications are considered cluster resources. A cluster system allows you to categorize these resources as a "group" for a specific functionality purposes. These resource groups can be treated as a "container" of resources. A cluster resource group is a logical unit for application deployment, which means that a cluster-aware application must be installed into a group and bind itself with the resources that are associated with that group. The resource group is the minimum unit for failover purposes.

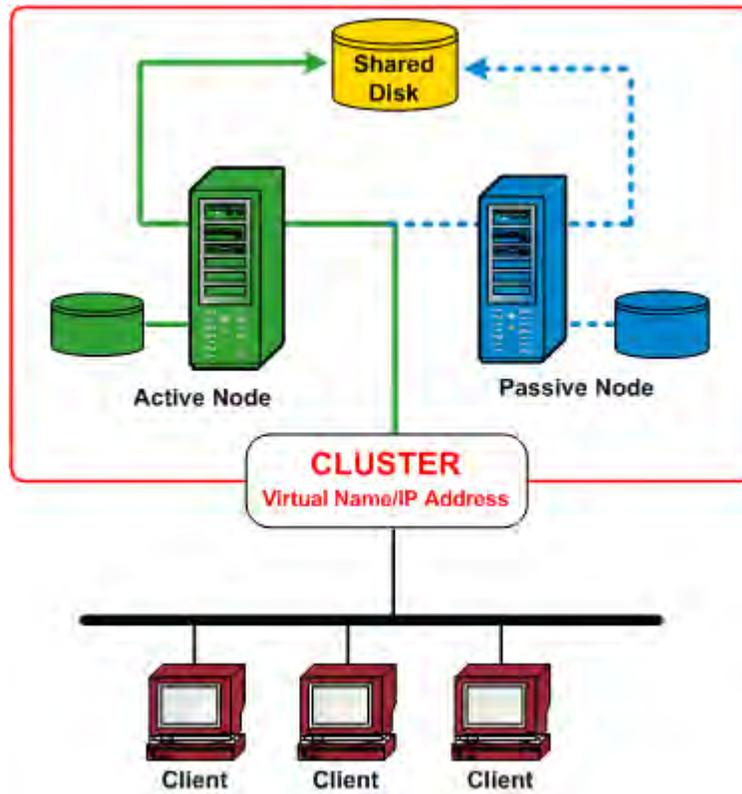
Virtual Name and Virtual IP Address

The virtual server name is independent of the name of the physical server on which the virtual server runs and can migrate from server to server. In a cluster environment, the active node will always use the cluster virtual name and IP address to provide service instead of the physical hostname and IP address. Through the use of clusters, virtual servers are created so that when another server takes it place, the services can still be available. The virtual name and IP address are linked with CA ARCserve Backup. Similarly, other cluster-aware applications (SQL/Exchange Cluster) often create a dedicated virtual name and IP address for high-availability purposes during their installation.

Unlike a physical server, a virtual server is not associated with a specific computer, and it can fail over from one server to another. If the server that is hosting the virtual server fails, clients can still access its resources by using the same virtual server name, but they will be redirected to a different server in the cluster.

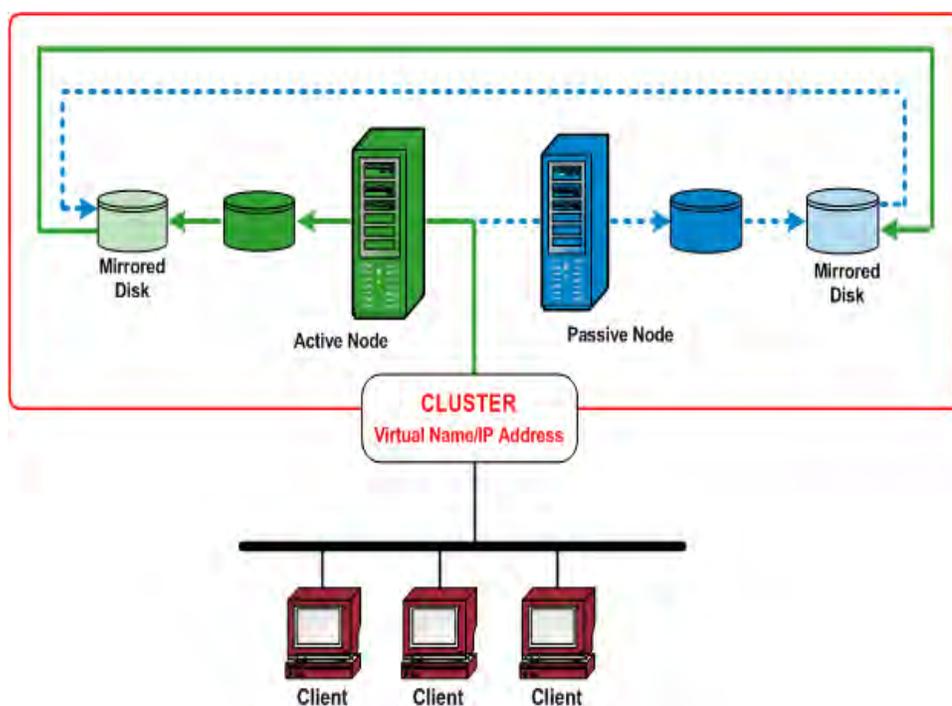
Shared Disks

Shared disks provide shared location for cluster-aware applications to save data. Shared disks allow cluster-aware applications, which might run on different nodes because of failover, to gain access to a logical volume in a consistent way, as if they are local at each of the nodes. Each virtual shared disk corresponds to a logical volume that is actually local at one of the nodes, which is called the server or primary node. Each node within the cluster must have access to a shared disk to operate within the cluster. The cluster system is configured so that only the active node can access the shared disk at any time.



Mirrored Disks

Mirrored disks provide a shared location for cluster-aware applications to save data. Mirrored disks (applicable to NEC clusters only) are separate disk devices that are physically attached to their host separately, but work like one single device logically. Mirrored disks contain an exact duplicate of the disk that it mirrors. Data is stored twice by writing to both the local disk and its remote mirrored disk. If a disk fails, data does not have to be rebuilt and can be easily recovered by copying it from the mirrored disk to the replacement disk. It is recommended that mirrored disks reside on different devices so that a single-point disk failure cannot damage both copies of the data. The main disadvantage of mirrored disks is that the effective storage capacity is only half of the total disk capacity because all data gets written twice. The cluster system is configured so that only the active node can access the mirrored volume and sync-up the data between different physical disks. The cluster system is configured so that only the active node can access the mirrored volume and sync-up the data between different physical disks.



Quorum Disks

In addition to the resource groups created for each clustered application, a cluster always has a resource group to represent the quorum of the cluster. This resource group, by default named Cluster Group, is created when the cluster is created. In a shared disk quorum, the disk containing the quorum resource is called the quorum disk, and it must be a member of the default Cluster Group. A quorum disk is used to store cluster configuration database checkpoints and log files which help manage the cluster as well as maintain consistency. The quorum resource is used to decide which nodes of the cluster are supposed to form the cluster. Because the cluster configuration is kept on a quorum disk resource, all nodes in the cluster must be able to access and communicate with the node that owns it.

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.

- **Upgrade Considerations:**

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

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

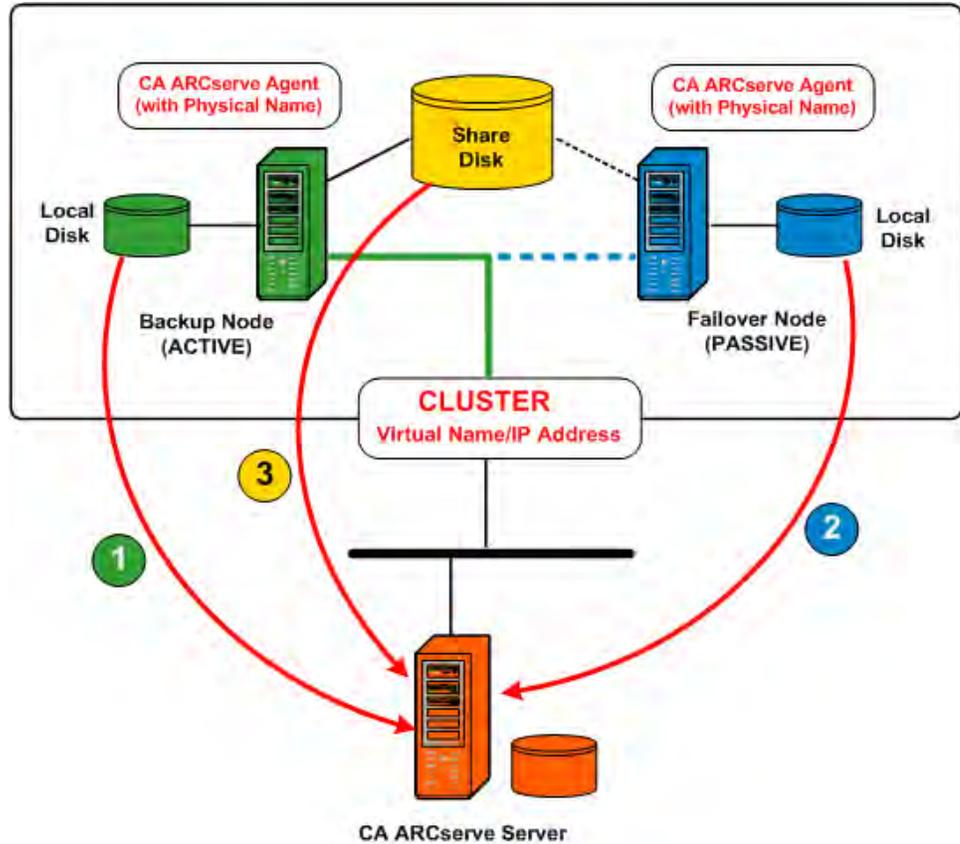
Note: For more information about using cstop and cstart, see the *Administration Guide*.

Protecting Your Cluster with CA ARCserve Backup

For mission-critical applications deployed into a cluster environment, the data is the most valuable investment and protection of this data is essential. A cluster environment always involves multiple physical nodes, a virtual name/IP address, and cluster-specific applications, all of which bring additional complexities for the backup and restore application. To address these complexities, CA ARCserve Backup provides multiple backup and restore capabilities for servers operating in a cluster environment.

Note: CA ARCserve Backup supports cluster environments for Microsoft Cluster Server (MSCS) and NEC Cluster Server (CLUSTERPRO/ExpressCluster).

The following diagram shows a typical active/passive cluster environment. The active node in this cluster is associated with two names and IP addresses: one for the physical name of the machine and the other for the virtual name created by the cluster itself or the cluster-aware application. The passive node is associated with only one name, the physical name of the machine. To fully protect the cluster, you need to install the CA ARCserve Backup agent into both of these physical nodes. In each of these instances, depending on the protected target, CA ARCserve Backup will be deployed to protect your cluster and back up your data using either the physical node or the virtual node.



- **Protect data using physical node**

To protect the system state of each cluster node and the local application data, you need to schedule the backup job based on the physical name/IP address of the machine. For the active node (1), you can back up all attached disks, including the local disks as well as shared disks. For a passive node (2), you can only back up the local disks. However, it is not a best practice to back up a shared disk based only on physical name. In a cluster environment, the role of each node (active and passive) may change dynamically due to a failover condition. If you specify the physical name of the failed node, the backup will fail and the data that is located on the shared disk will not be backed up.

- **Protect data using virtual node**

In a cluster-aware application (SQL Server cluster or MS Exchange cluster), all data is saved on a shared disk to provide HA capability. To back up this data, the CA ARCserve Backup agent (installed on each physical node) will archive the data into the shared disk via the virtual name and IP address of the cluster (3). Under normal conditions, CA ARCserve Backup will back up data from the shared disk using the virtual name and IP address of the cluster as the source rather than the physical name and IP address of the active node. The advantage of doing this is if the active node fails or is shut down, the failover mechanism of cluster will make the passive node become the new active node, and CA ARCserve Backup will automatically continue to perform backups from the shared disk. As a result, you can schedule rotation backup jobs to protect your data located in the shared disk regardless which cluster node is active.

Note: To back up any application specified data (for instance, a SQL Server database), you should deploy the corresponding CA ARCserve Backup agent and perform the backup using the virtual name associated with this cluster-aware application.

MSCS Protection

Microsoft Cluster Server (MSCS) software provides a clustering technology that keeps server-based applications highly available, regardless of individual component failures. For MSCS, there are two basic types of targets that need to be protected by backup: cluster self-protection, in which the cluster itself is protected (metadata and configuration information) and clustered-application protection.

MSCS Cluster Self-Protection

For MSCS, all cluster configuration information resides in a Cluster Database. The Cluster Database is located in the Windows registry on each cluster node and contains information about all physical and logical elements in a cluster, including cluster objects, their properties, and cluster configuration data. The Cluster Database contains the cluster state data that is replicated among nodes to ensure that all nodes in the cluster have a consistent configuration. The Cluster Database registry is located in %WINDIR%\CLUSTER\CLUSDB.

The Cluster Database is part of the Windows System State. When the System State is selected for backup, the Cluster Database is automatically included in this backup. Therefore, the Cluster Database is included in the system state backup only if the node is a part of a cluster and the cluster service is running on that node. If the cluster service is not running, the Cluster Database is not backed up.

To protect a cluster node itself and reduce the potential risk caused by accidental node failure, you should back up the following data using the physical name of the nodes:

- all data on the local disks contained in the Windows boot/system partitions
- system state data

During restore operations, you first need to determine the severity of the problem. If you cannot boot the node at all, see *Recovering Clusters in the CA ARCserve Backup Disaster Recovery Option Guide*. If you can boot the operating system and only the cluster database is damaged, you will not be able to selectively restore the Cluster Database as a single entity, it must be restored as part of a System State session restore.

Note: To back up and restore the Cluster Database, it is sufficient to back up and restore the Windows System State with the cluster service running. When a cluster node is in the Directory Service Restore mode, the Logon properties of the Cluster Service User Account must be set as Administrator to ensure that CA ARCserve Backup can be accessed while in Windows Safe Mode.

MSCS Cluster Application Protection

CA ARCserve Backup offers fast and intelligent backup and restore operations of applications such as Microsoft SQL Server and Microsoft Exchange Server installed on a cluster. For the most current list of available agents, see the readme file or access the CA web site at ca.com. For information on backing up and restoring applications installed on a cluster, see the corresponding CA ARCserve Backup agent guide. For example, for information on backing up and restoring a Microsoft SQL Server, see the *Agent for Microsoft SQL Server Guide*.

How CA ARCserve Backup Integrates with MSCS

CA ARCserve Backup is a fault-tolerant application, capable of supporting failover in cluster environments. CA ARCserve Backup protects cluster nodes by backing up and restoring cluster-specific resources such as shared disks, quorum resources, disk signatures, and cluster registry hives. Microsoft Cluster Server (MSCS) allows multiple Windows based servers to connect with one another so that they appear, to network clients, to be a single, highly available system.

With the MSCS support provided by CA ARCserve Backup, you can:

- Back up and restore MSCS nodes
- Run on, and take advantage of, MSCS high availability features such as:
 - Job failover from one CA ARCserve Backup node in a cluster to another node
 - High availability through automatic failover of CA ARCserve Backup services from one node in a cluster to another node
 - Install CA ARCserve Backup to an Active/Passive cluster as your SAN primary server and allow continuation of distributed server backups upon failover
 - Manageability through standard cluster management tools
- Provide disaster protection for MSCS nodes using the CA ARCserve Backup Disaster Recovery Option. For more information, see the *Disaster Recovery Option Guide*.
- Backup and restore applications, such as MS SQL Server and MS Exchange Server, installed on MSCS clusters using the CA ARCserve Backup agents. For more information on available agents, see the *Implementation Guide*.

NEC CLUSTERPRO/ExpressCluster Protection

NEC CLUSTERPRO/ExpressCluster is a high-availability clustering solution that provides fast recovery and high reliability to maximize critical applications and data availability. NEC clusters offer integrated application and data protection that enables fast, easy recovery and continuity of critical systems.

NEC clusters allow multiple Windows based servers to connect with one another so that they appear to network clients to be a single, highly available system. CA ARCserve Backup supports NEC CLUSTERPRO/ExpressCluster 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0, and NEC CLUSTERPRO/ExpressCluster X 2.0. Similar to MSCS, we can protect the Cluster itself and these clustered applications.

For NEC clusters, there are two basic types of targets that need to be protected by backup: cluster self-protection, in which the cluster itself is protected (metadata and configuration information) and clustered-application protection.

NEC Cluster Server Self-Protection

For NEC CLUSTERPRO/ExpressCluster, all cluster configuration information resides in a file system as regular files.

To protect a cluster node itself and reduce the potential risk caused by accidental node failure, you should back up the following data using the physical name of the nodes:

- all data on the local disks contained in the Windows boot/system partitions
- system state data

During restore operations, you first need to determine the severity of the problem. If you cannot boot the node at all, see *Recovering NEC Clusters* in the *CA ARCserve Backup Disaster Recovery Option Guide*. If you can boot the operating system and only the NEC cluster files are damaged, refer to the applicable NEC CLUSTERPRO/ExpressCluster document to manually restore these configuration files that are related to NEC clusters.

NEC CLUSTERPRO/ExpressCluster Application Protection

For NEC CLUSTERPRO/ExpressCluster, there are few applications that are native cluster-aware. Native cluster-aware refers to some applications that are aware they will run in cluster environment to support HA and take special considerations in design.

For NEC clusters, few applications are designed to be cluster-aware and many do not recognize the NEC virtual name/IP address. However, for some of the more popular applications, NEC provides specific documentation for configuring these applications as “cluster-aware” and deploying them so that you can perform backup and restore jobs. Refer to NEC website for a list of all supported applications and detailed information on how to configure them as cluster-aware. If you have deployed one of these supported applications, refer to the corresponding NEC documentation for details about how to perform a backup and restore with cluster support.

How CA ARCserve Backup Integrates with NEC CLUSTERPRO

CA ARCserve Backup is a fault-tolerant application, capable of handling failover and providing backup and restore capabilities for data residing in cluster environments.

NEC CLUSTERPRO/ExpressCluster allows multiple Windows based servers to connect with one another so that they appear to network clients to be a single, highly available system. CA ARCserve Backup supports NEC CLUSTERPRO/ExpressCluster for Windows 8.0 (SE and LE), NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, and NEC CLUSTERPRO/ExpressCluster X 2.0 for Windows. Similar to MSCS, we need protect Cluster itself and these clustered applications.

CA ARCserve Backup support for NEC CLUSTERPRO/ExpressCluster offers the following advantages:

- Ability to run on NEC CLUSTERPRO/ExpressCluster and take advantage of high availability features such as:
 - Automatic failover of CA ARCserve Backup services from one node in a cluster to another node
 - Ability to fail jobs over from one CA ARCserve Backup node in a cluster to another node when CA ARCserve Backup failover occurs
 - Ability to restart jobs after failover
 - Ability to install CA ARCserve Backup on an Active/Passive cluster as the SAN primary server to allow the continuation of distributed server backup operations after failover
 - Ability to use NEC cluster management tools
- Data backup and restore functionality for NEC cluster nodes.
- Disaster protection for NEC CLUSTERPRO/ExpressCluster nodes through the Disaster Recovery Option. For more information, see the *Disaster Recovery Option Guide*.

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.

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 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

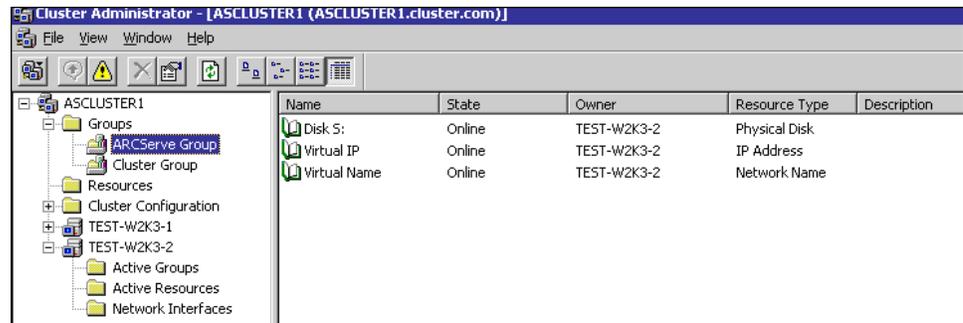
If you are installing CA ARCserve Backup into a dedicated group, you need to create the required resources into the new dedicated group, including a virtual IP address, virtual name, and a shared disk.

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.

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.

CA ARCserve Backup HA Server to Support of Job Failover

Clustered CA ARCserve Backup servers provide service through virtual name and support backup job failover capability. When the active CA ARCserve Backup server in a cluster fails, these backup jobs are dispersed from the failed server to other CA ARCserve Backup servers in the cluster. After CA ARCserve Backup services are resumed in another cluster node, any failed jobs from the previous server are rerun in a new cluster node.

CA ARCserve Backup HA server supports two types of failovers; planned failovers and unplanned failovers.

■ Planned Failovers

Planned failovers occur when it is necessary to perform maintenance on the active node within a cluster and you want CA ARCserve Backup to migrate the cluster resources from that active node to a passive node within the cluster. Examples for planned failovers are system maintenance, disaster recovery tests, and training.

When a planned failover occurs, CA ARCserve Backup recovers in another node with all scheduled jobs retained.

■ Unplanned Failovers

Unplanned failover can occur because of hardware or software failures. When unplanned failover occurs, CA ARCserve Backup recovers in another node, picks up the failed job from the CA ARCserve Backup job queue, and resumes the job from the point where it failed. If a failover occurs, the job resume is based on a checkpoint mechanism as follows:

- For a local backup job, the job will resume at the volume level after a failover.

For example, if a backup job involves two volumes: C and D, and a failover occurs when the backup for volume C was finished and the backup for volume D was ongoing. After the failover, the backup job will restart and skip the backup for volume C and continue to backup volume D.

- For a remote backup job, the job will resume at the host level.

For example, if a backup job involves Host1 and Host2, and a failover occurs when the backup for Host1 is finished, but the backup for Host2 is not. After the failover, the backup job will restart and skip the backup for Host1 and continue to backup Host2 (in this case, the backup for Host2 does not skip any volumes that might be backed up before failover).

Jobs running on other backup servers instead of the HA server of the domain will rarely be impacted by failover. For example, when the Primary server is HA server, and it fails over, the jobs running on member servers are not impacted except in one situation. If you are using a HA primary server, the jobs that run on the member servers may fail when an unplanned failover occurs on the HA primary server. (The failures only occur when the jobs on the member servers are finishing when the failover occurs)

Note: If you are using CA ARCserve Backup Agents to backup the active node of the cluster or the virtual node, and an unplanned failover occurs (the active node is down), the job would become incomplete. To ensure that these nodes could be backed up after failover, you should configure the jobs to create makeup jobs.

Stop HA Service Monitoring by MSCS

When a CA ARCserve Backup server is configured as cluster-aware, all critical CA ARCserve Backup services will be monitored by MSCS. If some service fails, MSCS will try to restart it or trigger a failover if the restart attempt fails. This means that you can no longer stop a service by using the CA ARCserve Backup Server Administrator. If you attempt to stop a CA ARCserve Backup service, you will get a pop-up message:



However, in some situations, you may want to stop some CA ARCserve Backup service. For example, you may want to stop the Tape Engine so that you can perform hardware maintenance.

To stop MSCS from monitoring CA ARCserve Backup services

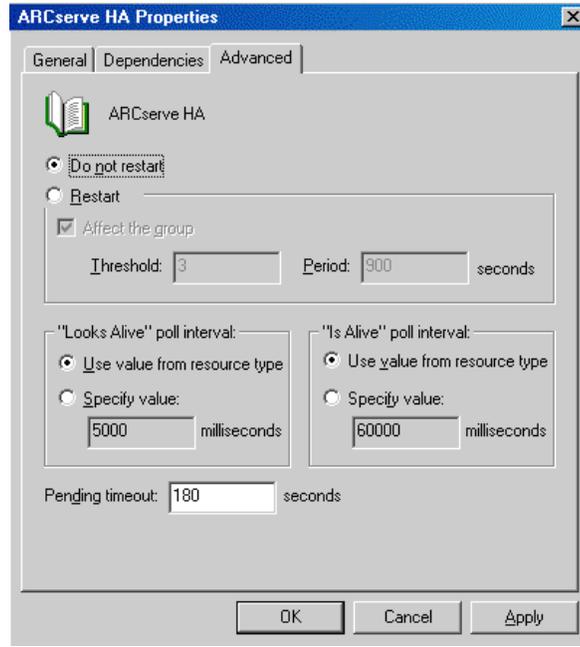
1. Access the Cluster Administrator.

The Cluster Administrator dialog appears.

Note: Cluster Administrator is a utility provided by Microsoft and is installed on servers that have MSCS installed. From the Cluster Administrator, you perform most of the configuration and management tasks associated with clusters.

2. Select the group that the ARCserve server is deployed in, and locate the applicable ARCserve resource. Right-click on the ARCserve resource and from the pop-up menu, select Properties.

The ARCserve Properties dialog appears.



3. From the Advanced tab, select the "Do not restart" option.

The automatic restart feature is disabled, allowing CA ARCserve Backup services to be stopped without MSCS automatically attempting to restart or initiating a failover.

Note: All CA ARCserve Backup services are controlled by the ARCserve HA resource. However, the Tape Engine service and ASDB service are also controlled by additional resources. See the following table to identify the resources that need to be changed for each CA ARCserve Backup service. For each of the applicable resources, you need to set the Advanced property to Do not restart.

Service Name	Controlling Resource(s)
Tape Engine	ARCserve HA ARCserve Registry
ASDB (only for SQL2005 Express)	ARCserve ASDB ARCserve HA ARCserve Registry
Others(DB Engine, Job Engine, ...)	ARCserve HA

4. Using the Windows Service manager, stop the applicable CA ARCserve Backup service to allow you to perform the necessary maintenance.
5. When you have completed the maintenance, restore all settings.

Rebuild Cluster Resources Manually

In most cases, the installation process will automatically create the necessary HA cluster resources without user interference. However, there may be cases where you need to create these cluster resources manually.

Prior to manually creating new resources, you should stop and delete all existing cluster resources from the group where CA ARCserve Backup is deployed. For more information on deleting cluster resources, see [Delete Cluster Resources](#) (see page 742).

Rebuild cluster resources manually

1. Open a command console and change current directory to %bab_home% (where, %bab_home% represents the actual CA ARCserve Backup install path).
2. Run the "babha.exe -postsetup" utility to set up new ARCserve cluster resources.

When a cluster-aware installation is successfully finished, a Post Setup pop-up screen appears with an option to create HA resources.

3. Select the "Create HA resources for MSCS" option and click OK to create new cluster resources.

Note: You should only check this option when you have completed the CA ARCserve Backup installation on the last node in the cluster.

The new ARCserve cluster resources (ARCserve HA, ARCserve ASDB, ARCserve Registry, and ARCserve Share) are created.

Delete CA ARCserve Backup Cluster Resources

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

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

Delete the ARCserve cluster resources

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

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

2. Access the Cluster Administrator.

The Cluster Administrator dialog appears.

Note: Cluster Administrator is a utility provided by Microsoft and is installed on servers that have MSCS installed. From the Cluster Administrator, you perform most of the configuration and management tasks associated with clusters.

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

The selected ARCserve cluster resources are deleted.

Manage CA ARCserve Backup Cluster Servers in a MSCS Cluster

The Server Configuration Wizard lets you perform various management tasks to specify how CA ARCserve Backup servers function in a cluster environment. In a cluster environment, these management tasks can only be made on the active node and must also be made for all nodes within the cluster. These management tasks include the following:

- Changing the database
- Promoting a member server to a primary server
- Demoting a primary server to a member server.

To manage the CA ARCserve Backup Cluster Servers in a MSCS cluster

1. Delete all cluster resources. For more information, see [Delete CA ARCserve Backup Cluster Resources](#) (see page 742).

All CA ARCserve Backup cluster resources are deleted.

2. From the ARCserve Backup home directory, run the cstart.bat utility to start all CA ARCserve Backup services.

All CA ARCserve Backup services are started.

3. From the Start menu, access the Server Configuration Wizard to run the ARCserveCfg.exe utility for the active node and make the necessary change. Do not check the "Last Cluster Node" checkbox on the last screen of the Server Configuration Wizard.

- For more information about changing the database, see [Specify a CA ARCserve Backup Database Application](#) (see page 609).

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

- For more information about promoting a member server to a primary server, see [Promote a Member Server to a Primary Server](#) (see page 515).
- For more information about demoting a primary server to a member server, see [Demote a Primary Server to a Member Server](#) (see page 518).

Note: When this utility is run on the first node within a cluster, it will run in the normal mode.

The first "active" cluster node is configured for the new property and a new arcservcfg.ICF configuration file is created.

4. From the ARCserve home directory, run the cstop.bat utility to stop all CA ARCserve Backup services.

All CA ARCserve Backup services are stopped.

5. 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".

6. From the Start menu, access the Server Configuration Wizard to run the ARCServeCfg.exe utility for the new active node and make the necessary change.

Note: When this utility is run again on any subsequent nodes in the same cluster, it will detect the existence of the arcservecfg.ICF configuration file and automatically run the utility in the cluster mode.

The next "active" cluster node is configured for the new property.

7. Repeat steps 5 and 6 for all remaining nodes in the cluster. When you are performing this configuration procedure on the last node in the cluster, check the "Last Node" checkbox on the last screen of the Server Configuration Wizard.

All nodes in the cluster are configured for the new property.

8. From the Cluster Administrator, right-click on the group name and from the pop-up menu, select Move Group to change the active node back to the original node.

The status of the last node will be changed to "passive" and the status of the original node within the cluster will be changed back to "active".

9. Create all CA ARCserve Backup cluster resources manually. For more information, see [Rebuild Cluster Resources Manually](#) (see page 741).

The new ARCserve cluster resources are created.

10. From the Cluster Administrator, right-click on the group name and from the pop-up menu, select Bring Online.

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

Change the CA ARCserve Backup Domain in a MSCS Cluster

In a MSCS cluster environment, you can move a member server to a different CA ARCserve Backup domain. Changes to the domain in a cluster environment can only be made on an active node and must be changed for all nodes within the cluster.

To change the CA ARCserve Backup domain in a MSCS cluster

1. Delete all cluster resources. For more information, see [Delete CA ARCserve Backup Cluster Resources](#) (see page 742).

All CA ARCserve Backup cluster resources are deleted.

2. From the ARCserve Backup home directory, run the cstart.bat utility to start all CA ARCserve Backup services.

All CA ARCserve Backup services are started.

3. From the Start menu, access the Server Configuration Wizard to run the ARCserveCfg.exe utility for the active node and specify the new CA ARCserve Backup domain. For more information about changing a domain, see [Move a Member Server to a Different CA ARCserve Backup Domain](#) (see page 522).

The first "active" cluster node is configured for the new domain.

4. From the ARCserve home directory, run the cstop.bat utility to stop all CA ARCserve Backup services.

All CA ARCserve Backup services are stopped.

5. 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".

6. From the ARCserve Backup home directory, run the cstart.bat utility to start all CA ARCserve Backup services.

All CA ARCserve Backup services are started.

7. From the ARCserve home directory, run the cstop.bat utility to stop all CA ARCserve Backup services.

All CA ARCserve Backup services are stopped.

8. Repeat steps 5 through 7 for all remaining nodes in the cluster.

All nodes in the cluster have been changed to the new domain.

9. From the Cluster Administrator, right-click on the group name and from the pop-up menu, select Move Group to change the active node back to the original node.

The status of the last node will be changed to "passive" and the status of the original node within the cluster will be changed back to "active".

10. Create all CA ARCserve Backup cluster resources manually. For more information, see [Rebuild Cluster Resources Manually](#) (see page 741).

Note: You should create Cluster resources based on new ARCserve database type.

The new ARCserve cluster resources are created.

11. From the Cluster Administrator, right-click on the group name and from the pop-up menu, select Bring Online.

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

Uninstall CA ARCserve Backup from an MSCS Cluster

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

To uninstall CA ARCserve Backup from a MSCS Cluster

1. Delete all cluster resources. For more information, see [Delete CA ARCserve Backup Cluster Resources](#) (see page 742).

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, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, and NEC CLUSTERPRO/ExpressCluster X 2.0 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 Windows 2000 and Windows Server 2003

Note: NEC CLUSTERPRO/ExpressCluster is not supported on IA-64 (Intel Itanium) operating systems.

- HA platform is configured for NEC CLUSTERPRO/ExpressCluster for Windows 8.0, NEC CLUSTERPRO/ExpressCluster X 1.0 for Windows, or NEC CLUSTERPRO/ExpressCluster X 2.0 for Windows.

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.

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 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.

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.

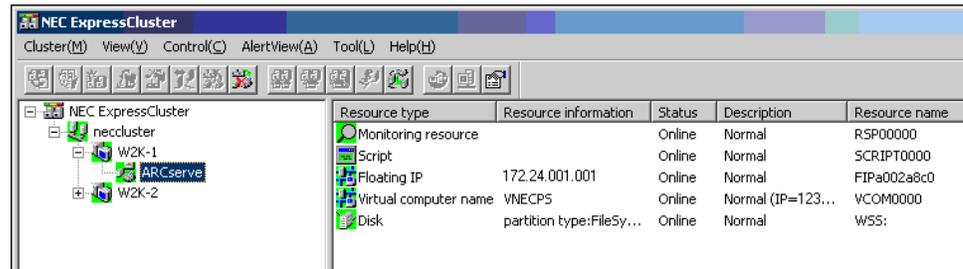
Cluster Manager and Task Manager are utilities provided by NEC and are installed on servers that have NEC CLUSTERPRO/ExpressCluster installed.

- 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.

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 752).
- 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 753).
- For SQL Express primary servers only, use the start.bat script contained in [start.bat Script Changes for SQL Express Primary Servers](#) (see page 754).
- For SQL Express primary servers only, use the stop.bat script contained in [stop.bat Script Changes for SQL Express Primary Servers](#) (see page 755).

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$arcsserve_db

:CA_SERVICES
net start CASDiscovery
net start CASportmappe
armload CASSvcControlSvr /S /R 3 /FOV CASSvcControlSvr
armload CASunivDomainSvr /S /R 3 /FOV CASunivDomainSvr
armload CASDBEngine /S /R 3 /FOV CASDBEngine
armload CASMessageEngine /S /R 3 /FOV CASMessageEngine
armload CASTapeEngine /S /R 3 /FOV CASTapeEngine
armload CASJobEngine /S /R 3 /FOV CASJobEngine
armload CASMgmtSvc /S /R 3 /FOV CASMgmtSvc
net start "CA ARCserve Communication Foundation"

:end
REM Exit out of the batch file
```

stop.bat Script Changes for 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
armkill CASjobengine
%ARCSERVE_HOME%\babha.exe -killjob
armkill CASMgmtSvc
armkill CASTapeEngine
armkill CASJobEngine
armkill CASDBEngine
armkill CASMessageEngine
armkill CASunivDomainSvr
armkill CASSvcControlSvr
net stop "CA ARCserve Communication Foundation"
net stop CASportmapper

if %PRIMARY_SQLE_FLAG%==0 GOTO end
net stop mssql$arcserve_db

:end
REM Exit out of the batch file
```

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$arcsserve_db

:CA_SERVICES
net start CASDiscovery
net start CASportmappe
armload CASSvcControlSvr /S /R 3 /FOV CASSvcControlSvr
armload CASunivDomainSvr /S /R 3 /FOV CASunivDomainSvr
armload CASDBEngine /S /R 3 /FOV CASDBEngine
armload CASMessageEngine /S /R 3 /FOV CASMessageEngine
armload CASTapeEngine /S /R 3 /FOV CASTapeEngine
armload CASJobEngine /S /R 3 /FOV CASJobEngine
armload CASMgmtSvc /S /R 3 /FOV CASMgmtSvc
net start "CA ARCserve Communication Foundation"

:end
REM Exit out of the batch file
```

stop.bat Script Changes for SQL Express Primary Servers

After installation, you need to modify the stop.bat script by adding text in two locations: after NORMAL and after FAILOVER. The following script changes apply only to SQL Express primary servers.

Copy the following script and paste it in the stop.bat file after NORMAL and after FAILOVER:

```
REM Set the following variable 'process' to 1 for normal
REM operation. During upgrade / migration, modify this
REM script to set the value to zero
SET process=1

REM Set this flag to 1 if it's a primary server and using
REM MS SQL Express 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
armkill CASjobengine
%ARCSERVE_HOME%\babha.exe -killjob
armkill CASMgmtSvc
armkill CASTapeEngine
armkill CASJobEngine
armkill CASDBEngine
armkill CASMessageEngine
armkill CASunivDomainSvr
armkill CASSvcControlSvr
net stop "CA ARCserve Communication Foundation"
net stop CASportmapper

if %PRIMARY_SQLE_FLAG%==0 GOTO end
net stop mssql$arcserve_db

:end
REM Exit out of the batch file
```

CA ARCserve Backup HA Server to Support of Job Failover

Clustered CA ARCserve Backup servers provide service through virtual name and support backup job failover capability. When the active CA ARCserve Backup server in a cluster fails, these backup jobs are dispersed from the failed server to other CA ARCserve Backup servers in the cluster. After CA ARCserve Backup services are resumed in another cluster node, any failed jobs from the previous server are rerun in a new cluster node.

CA ARCserve Backup HA server supports two types of failovers; planned failovers and unplanned failovers.

■ Planned Failovers

Planned failovers occur when it is necessary to perform maintenance on the active node within a cluster and you want CA ARCserve Backup to migrate the cluster resources from that active node to a passive node within the cluster. Examples for planned failovers are system maintenance, disaster recovery tests, and training.

When a planned failover occurs, CA ARCserve Backup recovers in another node with all scheduled jobs retained.

■ Unplanned Failovers

Unplanned failover can occur because of hardware or software failures. When unplanned failover occurs, CA ARCserve Backup recovers in another node, picks up the failed job from the CA ARCserve Backup job queue, and resumes the job from the point where it failed. If a failover occurs, the job resume is based on a checkpoint mechanism as follows:

- For a local backup job, the job will resume at the volume level after a failover.

For example, if a backup job involves two volumes: C and D, and a failover occurs when the backup for volume C was finished and the backup for volume D was ongoing. After the failover, the backup job will restart and skip the backup for volume C and continue to backup volume D.

- For a remote backup job, the job will resume at the host level.

For example, if a backup job involves Host1 and Host2, and a failover occurs when the backup for Host1 is finished, but the backup for Host2 is not. After the failover, the backup job will restart and skip the backup for Host1 and continue to backup Host2 (in this case, the backup for Host2 does not skip any volumes that might be backed up before failover).

Jobs running on other backup servers instead of the HA server of the domain will rarely be impacted by failover. For example, when the Primary server is HA server, and it fails over, the jobs running on member servers are not impacted except in one situation. If you are using a HA primary server, the jobs that run on the member servers may fail when an unplanned failover occurs on the HA primary server. (The failures only occur when the jobs on the member servers are finishing when the failover occurs)

Note: If you are using CA ARCserve Backup Agents to backup the active node of the cluster or the virtual node, and an unplanned failover occurs (the active node is down), the job would become incomplete. To ensure that these nodes could be backed up after failover, you should configure the jobs to create makeup jobs.

Stop HA Service Monitoring by NEC CLUSTERPRO/ExpressCluster

When a CA ARCserve Backup server is configured as cluster-aware, all critical CA ARCserve Backup services will be monitored by NEC CLUSTERPRO/ExpressCluster. If some service fails, NEC CLUSTERPRO/ExpressCluster will try to restart it or trigger a failover if the restart attempt fails. This means that you can no longer stop a service by using the CA ARCserve Backup Server Administrator. If you attempt to stop a CA ARCserve Backup service, you will see a pop-up message:



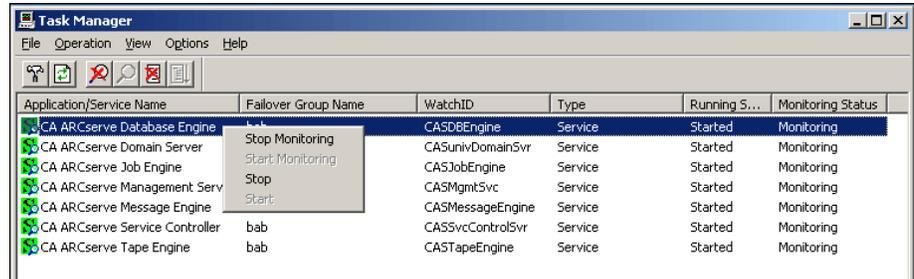
However, in some situations, you may want to stop some CA ARCserve Backup service. For example, you may want to stop the Tape Engine so that you can perform hardware maintenance.

To stop NEC CLUSTERPRO/ExpressCluster from monitoring CA ARCserve Backup services

1. Access the Task Manager.

The Task Manager window appears.

Note: You can only stop monitoring services from the active node. If you attempt to perform this task on a passive node, the Application/Service Name list on the Task Manager will be empty.



2. Locate and select the applicable CA ARCserve service. Right-click on the service and from the pop-up menu, select Stop Monitoring. A confirmation screen appears asking you to confirm or cancel your request to stop monitoring the selected service. Click OK.

The selected CA ARCserve Backup service is no longer being monitored by NEC CLUSTERPRO/ExpressCluster.

Change the CA ARCserve Backup Domain in NEC CLUSTERPRO/ExpressCluster

In a NEC CLUSTERPRO/ExpressCluster cluster environment, you can move a member server to a different CA ARCserve Backup domain. Changes to the domain in a cluster environment can only be made on an active node and must be changed for all nodes within the cluster.

To change the CA ARCserve Backup domain in a NEC cluster

1. Stop the cluster group. For more information, see [Stop NEC Cluster Groups](#) (see page 761).

Note: You must stop the group to edit the group properties.

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 765).
3. From the ARCserve Backup home directory, run the cstart.bat utility to start all CA ARCserve Backup services.

All CA ARCserve Backup services are started.

4. From the Start menu, access the Server Configuration Wizard to run the ARCserveCfg.exe utility for the active node and specify the new CA ARCserve Backup domain. For more information about changing a domain, see [Move a Member Server to a Different CA ARCserve Backup Domain](#) (see page 522).

The first "active" cluster node is configured for the new domain.

5. From the ARCserve home directory, run the cstop.bat utility to stop all CA ARCserve Backup services.

All CA ARCserve Backup services are stopped.

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 back to online (active).

7. From the ARCserve Backup home directory, run the cstart.bat utility to start all CA ARCserve Backup services.

All CA ARCserve Backup services are started.

8. From the ARCserve home directory, run the cstop.bat utility to stop all CA ARCserve Backup services.

All CA ARCserve Backup services are stopped.

9. Repeat steps 6 through 8 for all remaining nodes in the cluster.

All nodes in the cluster have been changed to the new domain.

10. From the Cluster Manager, right-click on the group name and from the pop-up menu, select Move Group to change the active node back to the original node.

The status of the last node will be changed to offline (passive) and the status of the original node within the cluster will be changed back to online (active).

11. Rebuild the NEC Cluster Scripts and Registry Sync. For more information, see [Enable CA ARCserve Backup in NEC Cluster Scripts](#) (see page 762).

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

12. Start the cluster group.

Manage CA ARCserve Backup Cluster Servers in NEC CLUSTERPRO/ExpressCluster

The Server Configuration Wizard lets you perform various management tasks to specify how CA ARCserve Backup servers function in a cluster environment. In a cluster environment, these management tasks can only be made on the active node and must also be made for all nodes within the cluster. These management tasks include the following:

- Changing the database
- Promoting a member server to a primary server
- Demoting a primary server to a member server.

To manage the CA ARCserve Backup Cluster Servers in NEC CLUSTERPRO/ExpressCluster

1. Stop the cluster group. For more information, see [Stop NEC Cluster Groups](#) (see page 761).

Note: You must stop the group to edit the group properties.

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 765).
3. From the Start menu, access the Server Configuration Wizard to run the ARCserveCfg.exe utility for the active node and make the necessary change. Do not check the "Last Cluster Node" checkbox on the last screen of the Server Configuration Wizard.

- For more information about changing the database, see [Specify a CA ARCserve Backup Database Application](#) (see page 609).

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

- For more information about promoting a member server to a primary server, see [Promote a Member Server to a Primary Server](#) (see page 515).
- For more information about demoting a primary server to a member server, see [Demote a Primary Server to a Member Server](#) (see page 518).

Note: When this utility is run on the first node within a cluster, it will run in the normal mode.

The first "active" cluster node is configured for the new property and a new arcservecfg.ICF configuration file is created.

4. From the Start menu, access the Server Configuration Wizard to run the ARCServeCfg.exe utility for the new active node and make the necessary change.

Note: When this utility is run again on any subsequent nodes in the same cluster, it will detect the existence of the arcservecfg.ICF configuration file and automatically run the utility in the cluster mode.

The next "active" cluster node is configured for the new property.

5. Repeat steps 3 and 4 for all remaining nodes in the cluster. When you are performing this configuration procedure on the last node in the cluster, check the "Last Node" checkbox on the last screen of the Server Configuration Wizard.

All nodes in the cluster are configured for the new property.

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 back to the original node.

The status of the last node will be changed to offline (passive) and the status of the original node within the cluster will be changed back to online (active).

7. Rebuild the NEC Cluster Scripts and Registry Sync. For more information, see [Enable CA ARCserve Backup in NEC Cluster Scripts](#) (see page 762).

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

8. Start the cluster group.

Stop NEC Cluster Groups

If you need to edit the group properties (for example to edit the start.bat or stop.bat files, or remove or add registry sync) you must first stop the group. In addition, if you need to remove CA ARCserve Backup from NEC CLUSTERPRO/ExpressCluster, you must also stop the group.

To stop the NEC cluster group

1. Access the Cluster Manager.

The Cluster Manager window appears.

- From the tree listing, right-click on the ARCserve group, and from the pop-up menu select Stop group.

A confirmation pop-up screen appears.



- Click OK.

The selected group is stopped.

Enable CA ARCserve Backup in NEC Cluster Scripts

Cluster scripts and registry keys are inserted during the NEC post-setup process. During the upgrade process from BrightStor ARCserve Backup r11.5 to CA ARCserve Backup r12.5, 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

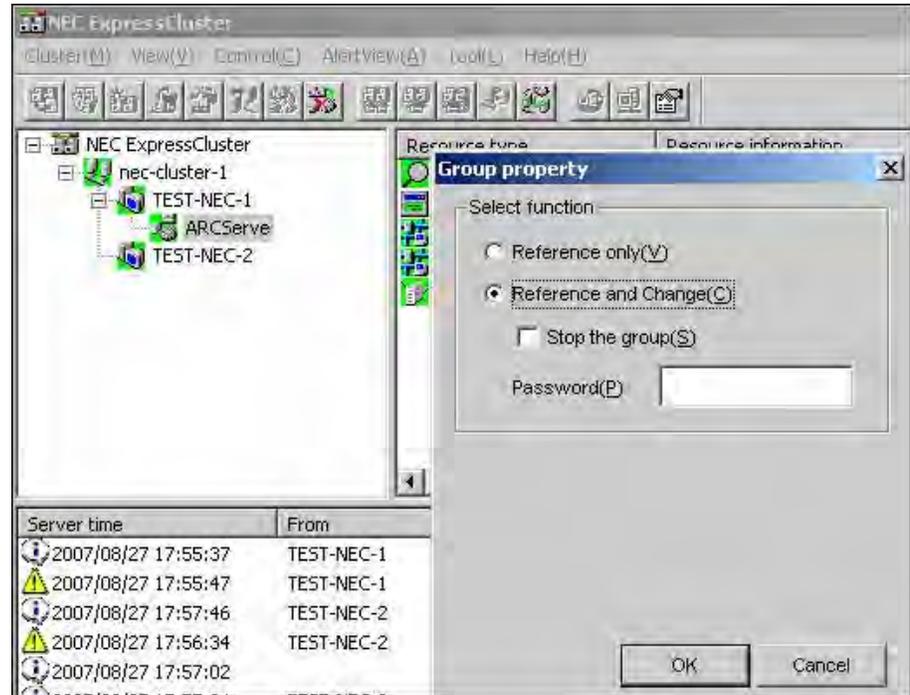
- Access Cluster Manager.

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.

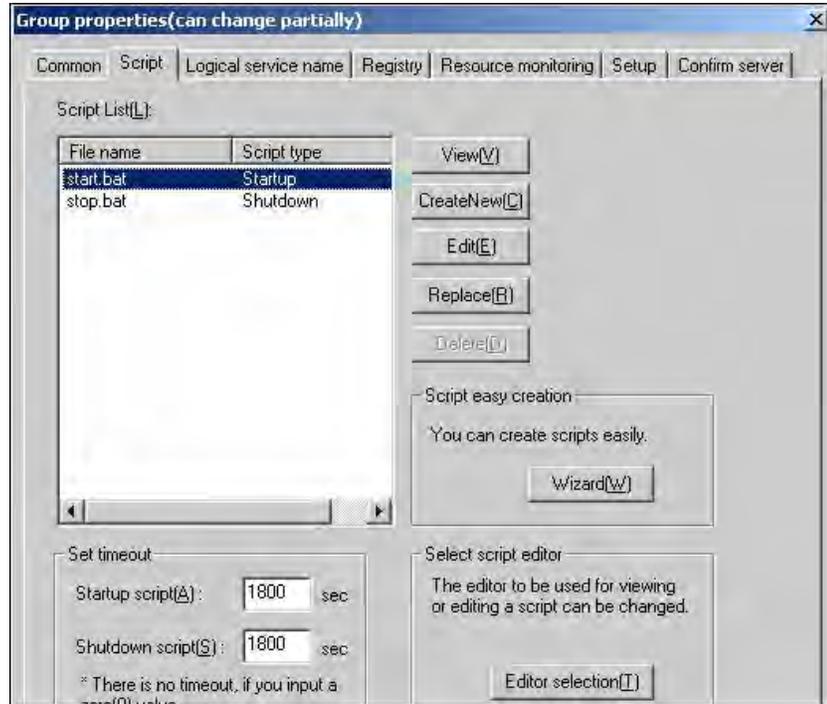
2. Select the NEC Group that the ARCserve server is deployed in, and locate the corresponding ARCserve cluster resources. Right-click on each ARCserve cluster resource and from the pop-up menu, select Property.

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:

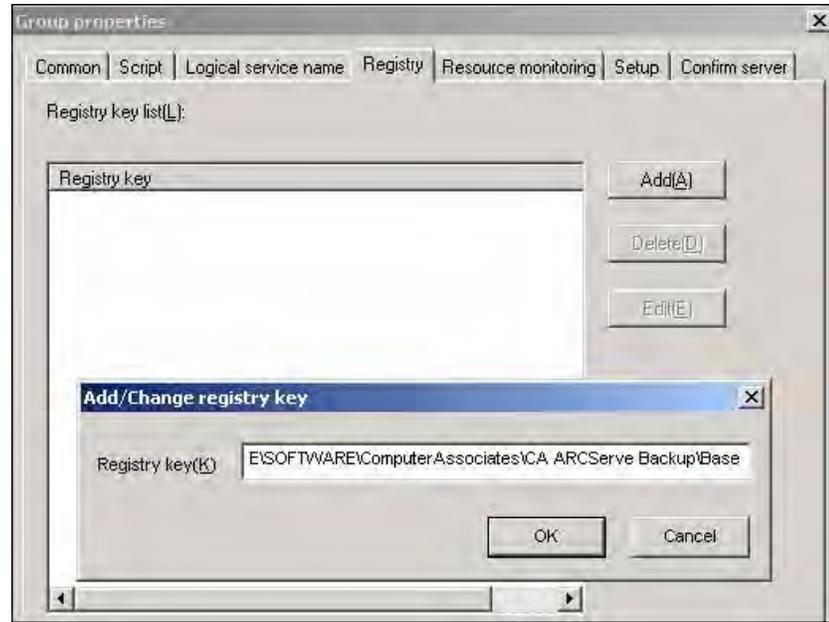
```
SET process=1
```

Note: In the stop.bat file, the REM SET process script is located after NORMAL and after FAILOVER.

The stop.bat script is modified.

- From the Group properties dialog, select the Registry tab. When the Registry dialog opens, click Add.

The Add/Change registry key dialog appears.



- Add the Registry key and click OK.

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

Disable CA ARCserve Backup in NEC Cluster Scripts

Cluster scripts and registry keys are inserted during the NEC post-setup process. When upgrading to from BrightStor ARCserve Backup r11.5 to CA ARCserve Backup r12.5, these cluster scripts need to be disabled and the registry key need to be deleted.

To disable the NEC Cluster Scripts and Registry Key

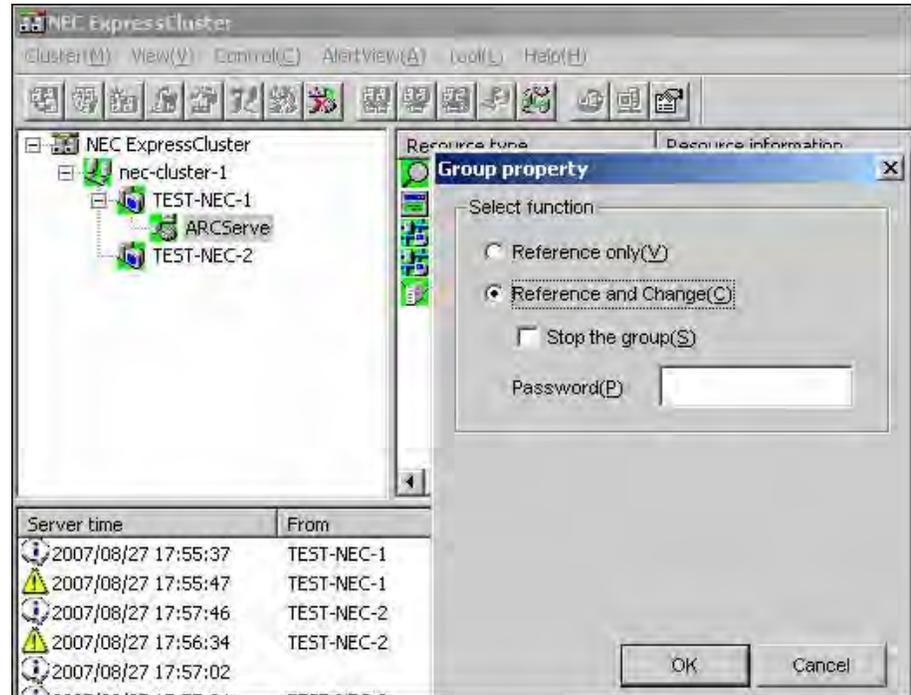
- Access the Cluster Manager.

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.

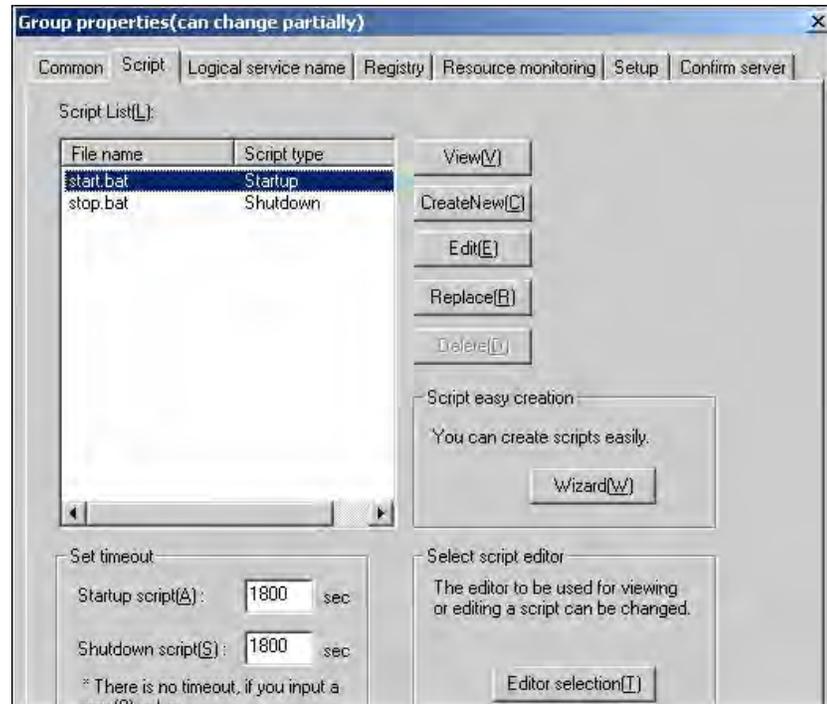
2. Select the NEC Group that the ARCserve server is deployed in, and locate the corresponding ARCserve cluster resources. Right-click on each ARCserve cluster resource and from the pop-up menu, select Property.

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:

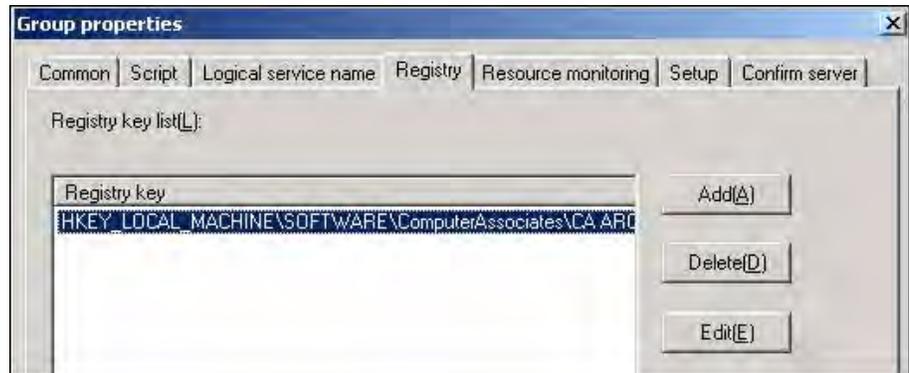
```
SET process=0
```

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.

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](#) (see page 761).
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 765).
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.

Troubleshooting CA ARCserve Backup Cluster Support

The following sections provide suggestions for solving problems you may encounter with CA ARCserve Backup cluster support.

Prevent Job Failures

Valid on Windows platforms.

Symptom:

How do I stop CA ARCserve Backup services in a cluster node without failover occurring?

Solution:

When a CA ARCserve Backup server is configured as cluster-aware, all critical CA ARCserve Backup services will be monitored by the cluster application (MSCS or NEC CLUSTERPRO/ExpressCluster). If some service fails, the cluster application will try to restart it or trigger a failover if the restart attempt fails. This means that you can no longer stop a service by using the CA ARCserve Backup Server Administrator. If you attempt to stop a CA ARCserve Backup service, you will get a pop-up message indicating that it is not permitted.

To shut down any CA ARCserve Backup services for maintenance or configuration changes when you do not want CA ARCserve Backup to fail over to another node, perform the following procedure:

- For MSCS clusters, see [Stop HA Service Monitoring by MSCS](#) (see page 739).
- For NEC CLUSTERPRO/ExpressCluster clusters, see [Stop HA Service Monitoring by NEC CLUSTERPRO/ExpressCluster](#) (see page 757).

Back Up MSCS Nodes on Remote Machines

Valid on Windows platforms.

Symptom:

How can I reliably back up MSCS Nodes with CA ARCserve Backup installed on remote machines?

For information about recovering clusters, see the *CA ARCserve Backup Disaster Recovery Option Guide*.

Solution:

The CA ARCserve Backup Windows File System Agent must be installed on each node of the cluster.

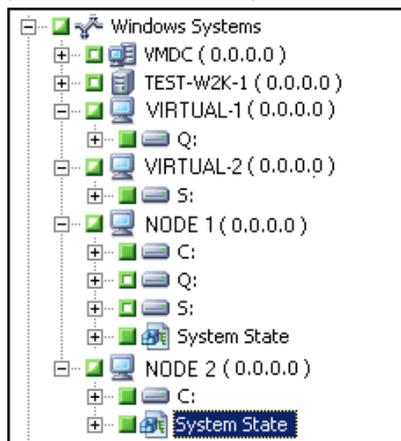
The challenge is to back up the shared disk reliably even if cluster shared disks fail over from one node to another. This can be done as follows:

1. Back up each of the nodes with their private disks and system state, using the hostname when submitting the backup jobs.

Note: Because shared disks can move from one node to another and there is no reliable way of predicting which node will own the shared disks during backup, **do not** back up shared disks using the machine hostname.

2. Back up the shared disks, using the cluster virtual name when submitting the backup job. If the shared disks fail over from one node to another, the cluster virtual node name fails over with it, so that CA ARCserve Backup always backs up the cluster shared disks. To ensure this, set up the cluster dependencies so that the cluster name and cluster shared disks fail over at the same time.

Note: To provide disaster protection for your cluster nodes, you must perform a full backup of each node.



Back Up CA ARCserve Backup Database in a Cluster Environment

Valid on Windows platforms.

Symptom:

How do I effectively backup the CA ARCserve Backup database (ASDB) in a cluster environment? (so that it can be recovered using the recoverdb operation)

Solution:

To ensure the backed up ASDB session can be used by the recoverdb operation you must backup the ASDB through the network name which you set during the setup phase.

For example:

1. For MS SQL Server 2005 express, you must use the virtual name which the CA ARCserve Backup is deployed on.
2. For MS SQL Server 2005 cluster, you must use the virtual name which the SQL Server Cluster is deployed on. (In this case, make sure that you set the correct virtual name of the SQL Server cluster when installing CA ARCserve Backup. To find out the SQL Server Cluster virtual name, refer to the SQL Server Cluster document.

Job Failure: Media Not Mounted

Valid on Windows platforms.

Symptom:

When my jobs fail over from one cluster node to another, I receive messages such as "Please mount media XYZ, 1234." How do I resolve this problem?

Solution:

If you select a backup media on the Destination tab of the Backup Manager when submitting a backup job, the job backs up only to that specific media. If the backup device is not shared among the cluster nodes, the specific media is not available after failover. As a result, the backup operation fails. To resolve this problem, select Destination at Group Level in the Backup Manager when submitting backup jobs.

This problem does not occur if you are backing up to a shared device.

Appendix E: Using CA ARCserve Backup for Microsoft Windows Essential Business Server

This section contains the following topics:

[CA ARCserve Backup for Microsoft Windows EBS Overview](#) (see page 773)

[Microsoft Windows EBS Overview](#) (see page 775)

[How CA ARCserve Backup Communicates with CA ARCserve Backup for Microsoft Windows EBS](#) (see page 777)

[Install CA ARCserve Backup for Microsoft Windows EBS](#) (see page 777)

[Uninstall CA ARCserve Backup for Microsoft Windows EBS](#) (see page 778)

[Microsoft Windows EBS Administration Console](#) (see page 778)

[Troubleshooting](#) (see page 787)

CA ARCserve Backup for Microsoft Windows EBS Overview

CA ARCserve Backup for Microsoft Windows EBS is an add-in for Microsoft Windows Essential Business Server (Microsoft Windows EBS) that provides the ability to view and manage CA ARCserve Backup jobs from the Administration Console. It contains a subset of the functionality in the Job Status Manager with the additional ability to manage backup and restore jobs and view reports, using the CA ARCserve Backup Managers.

Using CA ARCserve Backup for Microsoft Windows EBS, you can perform CA ARCserve Backup tasks, such as the following:

- Launch the CA ARCserve Backup Manager Console
- Display jobs in the queue (local or remote server)
- Create new backup jobs *
- Create new restore jobs *
- Manage jobs by launching the CA ARCserve Backup Job Status Manager

- View reports *
- Manage a different server
- Run a job now
- Put a job on hold
- Put a job in the ready state
- Delete a Job

* Functionality is available by launching the CA ARCserve Backup Manager Console.

You will need to continue using CA ARCserve Backup Manager for any advanced operations or functionality that falls outside the scope of CA ARCserve Backup for Microsoft Windows EBS.

CA ARCserve Backup for Microsoft Windows EBS is not meant to duplicate or replace the CA ARCserve Backup Manager Console. Instead the goal is to reuse the CA ARCserve Backup Manager Console as much as possible while also accessing the Microsoft Windows EBS Administration Console.

Central Management

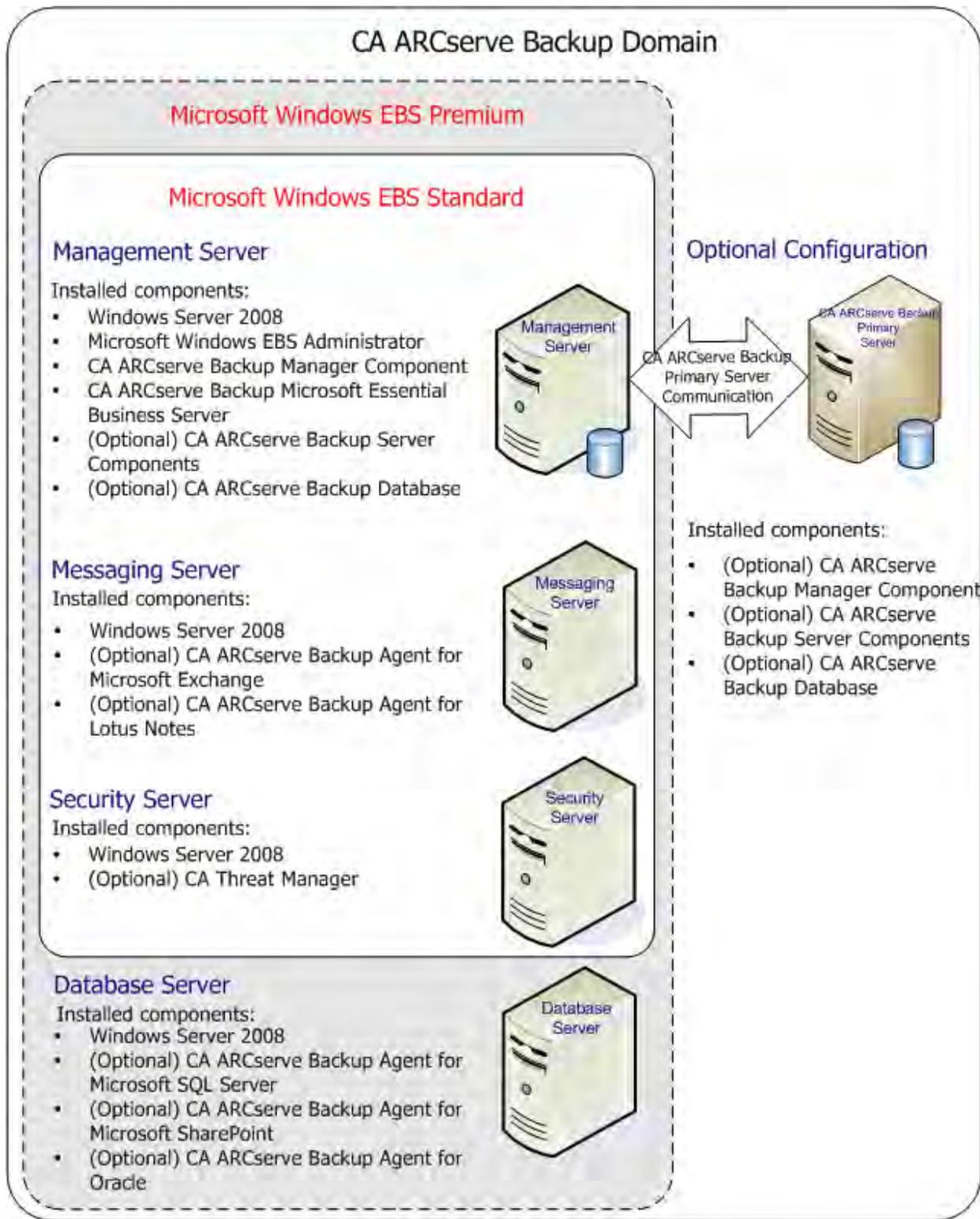
Just as the default functionality of the Job Status Manager, CA ARCserve Backup for Microsoft Windows EBS displays jobs from all servers in a CA ARCserve Backup domain. This allows you to interact with jobs from any server in a domain.

Microsoft Windows EBS Overview

Microsoft Windows EBS is a solution from Microsoft that targets mid-sized businesses with 50-250 workstations. Microsoft Windows EBS Standard Edition is comprised of a Management Server, a Messaging Server, and a Security Server, each on a separate 64-bit machine running Windows Server 2008 as their base operating system. Microsoft Windows EBS Premium Edition adds a Database Server to its managed capabilities.

Microsoft Windows EBS contains an Administration Console that provides a single interface to perform many common IT administration tasks. The Administration Console allows third party add-ins that can interface with non-Microsoft products. One such add-in is CA ARCserve Backup for Microsoft Windows EBS.

The following diagram illustrates the core components of Microsoft Windows EBS Standard Editions and Microsoft Windows EBS Premium Editions, and how you can configure your environment to integrate CA ARCserve Backup with Microsoft Windows EBS.



How CA ARCserve Backup Communicates with CA ARCserve Backup for Microsoft Windows EBS

The CA ARCserve Backup Manager components must be installed as a prerequisite in order for CA ARCserve Backup for Microsoft Windows EBS to function. Removal of the CA ARCserve Backup Manager will cause CA ARCserve Backup for Microsoft Windows EBS to cease functioning.

Install CA ARCserve Backup for Microsoft Windows EBS

Before you install CA ARCserve Backup for Microsoft Windows EBS, review the following installation considerations:

- Ensure that your system meets the minimum system requirements to install CA ARCserve Backup.

For more information, see the CA ARCserve Backup readme file.

- Ensure that your Microsoft Windows EBS environment is configured properly.

For more information, see [Microsoft Windows EBS Overview](#) (see page 775) and your Microsoft Windows EBS documentation.

After you have reviewed the installation considerations, you can install CA ARCserve Backup for Microsoft Windows EBS using the standard installation procedure for all CA ARCserve Backup system components, agents, and options. For information about installing CA ARCserve Backup, see the *Implementation Guide*.

Uninstall CA ARCserve Backup for Microsoft Windows EBS

The CA ARCserve Backup for Microsoft Windows EBS Option can be installed when you install CA ARCserve Backup or after you install CA ARCserve Backup. Based on the manner in which you installed the option, there are two methods that you can use to uninstall the option.

- If you installed the option when you installed CA ARCserve Backup, you must uninstall CA ARCserve Backup to uninstall the option.
- If you installed the option after you installed CA ARCserve Backup, you can uninstall the option using the Windows Add and Remove Programs application.

To uninstall CA ARCserve Backup for Microsoft Windows EBS

1. Open the Windows Control Panel and double-click the Add or Remove Programs application.

The Add or Remove Programs dialog opens.

2. Locate and click CA ARCserve Backup for Microsoft Windows EBS Option or CA ARCserve Backup, and then click Remove.

The uninstallation wizard appears.

3. Follow the prompts and complete the required fields on the wizard to complete the uninstallation.

Microsoft Windows EBS Administration Console

The Microsoft Windows EBS Administration Console provides the framework into which CA ARCserve Backup for Microsoft Windows EBS is used. It contains the following:

List pane

Displays a list of all CA ARCserve Backup jobs.

Job Information pane

Displays the name of the job with job summary and job detail information.

Job Summary

Displays information such as the description of the job, the name of the backup server, the execution time, and the status of the last result.

Job Details

Displays information such as the job type, job number, and status.

CA ARCserve Backup Tasks pane

Displays the various CA ARCserve Backup tasks you can perform using the Administration Console.

Job Tasks pane

Displays the various job management tasks you can perform using the Administration Console.

More information:

[Access CA ARCserve Backup for Microsoft Windows EBS](#) (see page 779)
[CA ARCserve Backup Tasks You Can Execute Using the Administration Console](#)
(see page 780)
[Job Management Tasks You Can Execute Using the Administration Console](#)
(see page 782)
[Microsoft Windows EBS Tasks You Can Execute Using the Administration Console](#)
(see page 784)

Access CA ARCserve Backup for Microsoft Windows EBS

To access CA ARCserve Backup for Microsoft Windows EBS, you must meet the following prerequisites:

- Windows Server 2008
- Microsoft Windows EBS
- CA ARCserve Backup

To access CA ARCserve Backup for Microsoft Windows EBS, open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.

How to Execute Tasks Using the Administration Console

The Administration Console lets you perform the following types of tasks:

- CA ARCserve Backup tasks
- Job Management tasks
- Microsoft Windows EBS tasks

When you select a CA ARCserve Backup task, the corresponding job management tasks will display.

More information:

[CA ARCserve BackupTasks You Can Execute Using the Administration Console](#)
(see page 780)

[Job Management Tasks You Can Execute Using the Administration Console](#)
(see page 782)

[Microsoft Windows EBS Tasks You Can Execute Using the Administration Console](#)
(see page 784)

CA ARCserve BackupTasks You Can Execute Using the Administration Console

The Administration Console lets you perform CA ARCserve Backup tasks, job management tasks, and Microsoft Windows EBS tasks for jobs in the job queue.

From the Administration Console, you can execute the following CA ARCserve Backup tasks:

Launch the CA ARCserve Backup Manager Console

Lets you launch the CA ARCserve Backup Manager Console so that you can manage the data ins your CA ARCserve Backup environment.

Manage Jobs

Lets you launch the Job Status Manager so that you can manage the jobs in the job queue.

Back Up Data

Lets you launch the Backup Manager so that you can protect, manage, and submit backup jobs in your CA ARCserve Backup environment.

Restore Data

Lets you launch the Restore Manager so that you can restore data that was backed up in your CA ARCserve Backup environment.

View CA ARCserve Backup Reports

Lets you launch the Report Manager so that you can view CA ARCserve Backup reports.

Connect to a new server

Lets you view the job queue and manage other CA ARCserve Backup servers.

More information:

[Manage a Different CA ARCserve Backup Server](#) (see page 781)

Manage a Different CA ARCserve Backup Server

CA ARCserve Backup for Microsoft Windows EBS supports querying and executing tasks on a single CA ARCserve Backup server at a time. To work with multiple separate CA ARCserve Backup servers that are not in the same CA ARCserve Backup Domain, you will need to switch servers through a task in CA ARCserve Backup for Microsoft Windows EBS. CA ARCserve Backup for Microsoft Windows EBS may then need to create equivalence again on the new CA ARCserve Backup server.

To manage a different CA ARCserve Backup server

1. Open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.
The Administration Console appears.
2. From the CA ARCserve Backup tasks pane, click Connect to a new server.
The Default Server Information dialog opens.
3. Click Connect to a remote CA ARCserve Backup server.

In the Primary Server Name field, specify the name of the CA ARCserve Backup primary server, stand-alone server, or member server that you want to manage and click OK.

After you click OK, one of the following results occurs:

- If CA ARCserve Backup detects equivalence, the jobs in the job queue for the specified server display in the Administration Console.
- If CA ARCserve Backup does not detect equivalence, the Create Equivalence dialog appears.

In the Create Equivalence dialog, specify the caroot password and click OK.

The jobs in the job queue for the specified server display in the Administration Console.

Note: If the server is a member server, the jobs in the job queue associated with the domain in which the member server resides display in the Administration Console.

Job Management Tasks You Can Execute Using the Administration Console

The Administration Console lets you perform CA ARCserve Backup tasks, job management tasks, and Microsoft Windows EBS tasks for jobs in the job queue.

From the Administration Console, you can perform the following job management tasks:

Run Now

Lets you run a scheduled job now.

Note: This options is available only for jobs with a Ready status.

Hold

Lets you status a scheduled job with Ready status to a Hold status.

Note: A Hold status signifies that the job is not scheduled to be executed.

Ready

Lets you status a scheduled job with a Hold status to a Ready status.

Note: A Ready status signifies that the job can be executed.

Delete

Lets you cancel the job and delete it from the CA ARCserve Backup job queue.

More information:

[Change the Status of Jobs in the Job Queue](#) (see page 782)

Change the Status of Jobs in the Job Queue

The CA ARCserve Backup for Microsoft Windows EBS Administration Console lets you view job status information and manage jobs that reside in the CA ARCserve Backup job queue.

To change the status of jobs in the Job Queue

1. Open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.

The Administration Console appears.

2. Locate the job where you want to change the status.

Right-click the job.

From the pop-up menu, select one of the following statuses:

Run Now

Lets you run a scheduled job now.

Note: This options is available only for jobs with a Ready status.

Hold

Lets you status a scheduled job with Ready status to a Hold status.

Note: A Hold status signifies that the job is not scheduled to be executed.

Ready

Lets you status a scheduled job with a Hold status to a Ready status.

Note: A Ready status signifies that the job can be executed at the next execution time.

Delete

Lets you cancel the job and delete it from the CA ARCserve Backup job queue.

The new status is applied to the job.

Microsoft Windows EBS Tasks You Can Execute Using the Administration Console

The Administration Console lets you perform CA ARCserve Backup tasks, job management tasks, and Microsoft Windows EBS tasks for jobs in the job queue.

From the Administration Console, you can perform the following Microsoft Windows EBS tasks:

Save As CSV

Lets you export job data to a comma-separated value text file (.csv).

Refresh

Lets you synchronize the data between CA ARCserve Backup and what you see in the Administration Console.

Sort By

Lets you sort jobs in the Job Queue in ascending or descending order based on the sort order of the field headings.

Group By

Lets you group jobs in the Job Queue based on the Job Type, the Job Status, and the Last Result.

Customize Results View

Lets you order, resize, and sort the columns for the jobs displayed.

More information:

[Export Data to a CSV File](#) (see page 785)

[Refresh Data Manually](#) (see page 785)

[Sort Job Data](#) (see page 786)

[Group Job Data](#) (see page 786)

[Customize the Results View](#) (see page 787)

Export Data to a CSV File

Job data displayed in CA ARCserve Backup for Microsoft Windows EBS can be exported to a comma-separated value text file (.csv). You can use this text file to import the data into spreadsheet applications, which allow you to sort the data and generate reports.

To export data to a comma-separated value text file

1. Open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.
The Administration Console appears.
2. From the File menu, choose Save As CSV.
The Save As dialog opens.
3. Select a path where the file should be created and saved, and then click Save.
The job data is saved to a comma-separated value text file.

Refresh Data Manually

CA ARCserve Backup for Microsoft Windows EBS synchronizes with CA ARCserve Backup in five second intervals. This process ensures data and tasks performed in one is automatically updated in the other. The screen is automatically refreshed every five seconds. However, if you wish to refresh the screen sooner, you can do it manually.

To refresh data manually

1. Open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.
The Administration Console appears.
2. From the View menu, choose Refresh.
The data is synchronized with CA ARCserve Backup and the screen is refreshed.

Sort Job Data

Sort By lets you sort jobs in the Job Queue in ascending or descending order based on the sort order of the field headings. You can sort the data based on any of the column headings.

To sort job data

1. Open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.
The Administration Console appears.
2. Do one of the following:
 - Click the heading of the column that you want to sort by. To reverse the sort-order, click the heading of the column again.
 - From the View menu, choose Sort By or right-click in the Job Queue and select Sort By from the pop-up menu. Then select the name of the column that you want to sort the jobs in the Job Queue. To reverse the sort order, right click-click in the Job Queue, select Sort By from the pop-up menu, and click Ascending or Descending.

The job data is sorted.

Group Job Data

Group By lets you group jobs in the Job Queue based on the Job Type, the Job Status, and the Last Result.

To group job data

1. Open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.
The Administration Console appears.
2. From the View menu, choose Group By or right-click in the Job Queue and select Group By from the pop-up menu. Then select the value that you want to group by.

The data is grouped.

Note: To ungroup the jobs in the Job Queue, select Ungroup from the pop-up menu.

Customize the Results View

The Customize Results View option lets you order, resize, and sort columns for the jobs displayed. You can arrange the order of the columns you want to appear, select the width of each column, and sort the results on a particular column heading in ascending or descending order.

To customize the results view

1. Open Microsoft Windows EBS, select the System Applications tab, and select the CA ARCserve Backup tab.

The Administration Console appears.

2. From the View menu, choose Customize Results View.

The Customize the Results View dialog appears.

3. Under the Columns heading, select the name of the column and click Move up or Move down to arrange the columns in the desired order.

The columns appear rearranged in the order selected.

4. Enter the width (in pixels) for each column.

5. In the Sort results by field, click the drop-down arrow and select the name of the column that you want to sort the jobs by and click Ascending or Descending.

6. Click OK.

The results view is customized.

Note: You can also use the mouse to drag a column to arrange it in a particular order, click and drag a column to resize the width of the column, or click the heading of the column that you want to sort by.

Troubleshooting

This section provides troubleshooting information to help you identify and resolve problems that you may encounter when using CA ARCserve Backup for Microsoft Windows EBS.

Failed to Create Equivalence

Valid on Windows Server 2008

Symptom:

You attempted to create equivalence through the dialog and either entered an invalid user name or password. You will see the message "Failed to create equivalence. Please try again."

Solution:

Click OK and enter a valid caroot password.

Equivalence was Not Created

Valid on Windows Server 2008

Symptom:

You cancelled the Create Equivalence dialog. (Equivalence is not created and CA ARCserve Backup for Microsoft Windows EBS cannot show any jobs). You will see the message "Equivalence was not created. Create the equivalence through the command line."

Solution:

Click OK. Wait ten seconds and the dialog should appear again.

Failed to Get the CA ARCserve Backup Job List

Valid on Windows Server 2008

Symptom:

You tried to retrieve the job list and nothing was returned. You will see the message "Failed to get the CA ARCserve Backup job list."

Solution:

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

Failed to Parse the CA ARCserve Backup Job List

Valid on Windows Server 2008

Symptom:

You tried to retrieve the job list and something unexpected was returned. Since what was returned was not in the correct format, the job data could not be retrieved. You will see the message "Failed to parse the CA ARCserve Backup job list."

Solution:

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

CA ARCserve Backup was Not Detected

Valid on Windows Server 2008

Symptom:

CA ARCserve Backup for Microsoft Windows EBS was installed without installing CA ARCserve Backup. Setup should not allow this, but if it does, you will see the message "CA ARCserve Backup was not detected. Please install CA ARCserve Backup."

Solution:

Reinstall CA ARCserve Backup.

Appendix F: Using JIS2004 Unicode Characters with CA ARCserve Backup

This section contains the following topics:

[Introduction to JIS2004 Unicode Characters](#) (see page 791)

[Configuration Requirements](#) (see page 792)

[Platforms Supporting JIS2004 Unicode Characters](#) (see page 792)

[Tasks You Can Perform Using JIS2004 Unicode Characters with CA ARCserve Backup](#) (see page 793)

[CA ARCserve Backup Applications Supporting JIS2004 Unicode Characters](#) (see page 794)

[Limitations of Using JIS2004 Unicode Characters with CA ARCserve Backup](#) (see page 795)

Introduction to JIS2004 Unicode Characters

Various Windows platforms support the capability to process data and display text and symbols using Unicode characters. For this release, CA ARCserve Backup supports the capability to display JIS2004 Unicode characters that relate to the following Windows system attributes:

- On client agent systems, CA ARCserve Backup displays folder names, file names, and registry strings using JIS2004 Unicode characters.
- On systems hosting application agents, CA ARCserve Backup displays database names, table names, and database instance names using JIS2004 Unicode characters.

Configuration Requirements

The following configuration requirements apply when you require support for JIS2004 Unicode characters in your CA ARCserve Backup environment:

- All servers in a CA ARCserve Backup domain (primary and member servers) must be running CA ARCserve Backup r12.5 and have the same language packs installed.
- CA ARCserve Backup for Windows r12.5 and CA ARCserve Backup r12 Service Pack 1 for Windows agents or CA ARCserve Backup for Windows r12 agents cannot co-exist on the same computer. However, CA ARCserve Backup for Windows r12.5 and CA ARCserve Backup for Windows r12 Service Pack 1 agents and CA ARCserve Backup for Windows r12 agents can co-exist on the same network.
- To back up and restore Microsoft Exchange and Microsoft SharePoint data with support for JIS2004 Unicode characters, you must enable the ARCserve Catalog database.
- All CA ARCserve Backup servers sharing a single Microsoft SQL Server database should be upgraded to the same version of CA ARCserve Backup.
- All CA ARCserve Backup domains sharing a single Microsoft SQL Server database must specify the same SQL Server collation setting. You can specify the SQL Server collation setting from a primary and stand-alone server using the Server Configuration Wizard.

Platforms Supporting JIS2004 Unicode Characters

The following Windows operating systems support JIS2004 Unicode characters:

- Windows Server 2008, Japanese version.
- Windows Vista, Japanese version.
- Windows Server 2003, Japanese version, with the Japanese fonts patch.
Note: For more information, see the Microsoft website.
- Windows XP Japanese version, with the Japanese fonts patch.
Note: For more information, see the Microsoft website.

Tasks You Can Perform Using JIS2004 Unicode Characters with CA ARCserve Backup

You can perform the following tasks when you run CA ARCserve Backup on JIS2004 Unicode character-based operating systems:

- Browse and view system and volume information in the CA ARCserve Backup managers, view logs, and generate reports without displaying unrecognized text.
- Back up systems hosting CA ARCserve Backup agents.
- Back up files, folders, databases, tables, instances, and Microsoft Exchange messages.
- Restore data by tree, session, query, and media.
- View job details and Activity Log data in the Job Status Manager.
- Specify local and global filters using JIS2004 characters.
- Generate Alert Manager email messages with JIS2004 Unicode text attachments (for example, a Job Log).
- Execute job scripts using scripts created in previous releases of CA ARCserve Backup.

Note: This capability is limited to scripts created using BrightStor ARCserve Backup r11, BrightStor ARCserve Backup r11.1, BrightStor ARCserve Backup r11.5, and CA ARCserve Backup r12.

- Execute CA ARCserve Backup command line operations using JIS2004 characters.

CA ARCserve Backup Applications Supporting JIS2004 Unicode Characters

The CA ARCserve Backup applications listed below support JIS2004 Unicode characters.

- CA ARCserve Backup r12.5 and CA ARCserve Backup r12 Service Pack 1 base product on x86 and x64 systems.

Note: Unicode support is only applicable to local backup, restore, and compare operations.

- Client Agent for Windows r12.5 and Client Agent for Windows r12 Service Pack 1 on x86, x64, and Itanium systems.
- Agent for Microsoft Exchange r12.5 and Agent for Microsoft Exchange r12 Service Pack 1 document level and database level backups and restores on x86 and x64 systems.
- Agent for Microsoft SQL Server r12.5 and Agent for Microsoft SQL Server r12 Service Pack 1 on x86, x64, and Itanium systems.
- Agent for Microsoft SharePoint 2007 r12.5 and Agent for Microsoft SharePoint 2007 r12 Service Pack 1 on x86 and x64 systems.
- Agent for Virtual Machines r12.5 and Agent for VMware r12 Service Pack 1 with VCB Proxy systems.
- CA XOssoft agents on x86 and x64 systems.
- Agent for Open Files r12.5 and Agent for Open Files r12 Service Pack 1 on x86, x64, and Itanium systems.

Note: Unicode support is only applicable to VSS-based backup and restore operations.

- Disaster Recovery Option.

Note: Some non-English language-based characters may appear as garbled characters when the CA ARCserve Backup base product is installed on any Windows operating system. This limitation does not affect the outcome of backup and restore jobs.

Limitations of Using JIS2004 Unicode Characters with CA ARCserve Backup

The following limitations apply when using JIS2004 Unicode characters with CA ARCserve Backup:

Operating Systems

The operating systems that the following agents protect do not support JIS2004 Unicode characters:

- Client Agent for UNIX
- Client Agent for Linux
- Client Agent for Mac OS X
- Client Agent for AS400
- Client Agent for OpenVMS
- Client Agent for NetWare

CA ARCserve Backup Agents and Options

The CA ARCserve Backup agents and options listed below do not support JIS2004 Unicode characters.

You can work around this limitation by backing up and restoring data from the parent-level path instead of the path containing the JIS2004 characters.

Important! To display ANSI character-based agents properly, you must set the locale and the product language options on the system hosting these agents to the same locale and product language as that of the system hosting the CA ARCserve Backup database before you install CA ARCserve Backup.

- Agent for Informix: all supported releases and service packs
- Agent for Lotus Domino: all supported releases and service packs
- Agent for Microsoft Exchange 2000 and 2003: all supported releases and service packs
- Agent for Microsoft Exchange 2007 on Windows Server 2003: all supported releases and service packs
- Agent for Microsoft Exchange 2007 Service Pack 1 on Windows Server 2008: r12
- Agent for Microsoft SharePoint 2003: all supported releases and service packs
- Agent for Microsoft SharePoint 2007: r12
- Agent for Microsoft SQL Server: r12, r11.5 (all service packs), and r11.1 (all service packs)
- Agent for Open Files: r12, r11.5 (all service packs), and r11.1 (all service packs)
- Agent for Oracle: r12, r12 Service Pack 1, r11.5 (all service packs), and r11.1 (all service packs)
- Agent for Sybase: all supported releases and service packs
- Client Agent for Windows: r12, r11.5 (all service packs), and r11.1 (all service packs)
- Enterprise Option for SAP R3 for Oracle: all supported releases and service packs

- NDMP NAS Option: all supported releases and service packs
Note: EMC/Celera and NetApp NAS filers do not support JIS2004 Unicode characters.
- Image Option-based backups and restores: all supported releases and service packs
Note: The CA ARCserve Backup Enterprise Module is a prerequisite component for the Image Option.

CA ARCserve Backup Components

The CA ARCserve Backup components listed below do not support JIS2004 Unicode characters.

- Alert Manager
- Alert options specified as Global Options in the CA ARCserve Backup managers and utilities that follow:
 - Backup Manager
 - Restore Manager
 - Media Assure & Scan Utility
 - Merge Utility
 - Count Utility
 - Purge Utility
- BConfig.exe
Note: This component lets you configure the CA ARCserve Backup server when you are installing or upgrading CA ARCserve Backup.
- DBAConfig.exe
Note: This component lets CA ARCserve Backup configure database instances during the installation process.
- Discovery Configuration
- License Management dialog
Note: This component lets you manage CA ARCserve Backup licenses. You can open the License Management dialog by clicking Manage Licenses on the the Help, About CA ARCserve Backup dialog.
- CA ARCserve Backup for Windows Registration dialog
Note: This component lets you register CA ARCserve Backup products. You can open the CA ARCserve Backup for Windows Registration dialog by clicking Register on the Help, About CA ARCserve Backup dialog.
- Report Writer
- Server Configuration Wizard

- Server Migration Component
- SetupSQL.exe

Note: This component lets the installation wizard create the CA ARCserve Backup database with Microsoft SQL Server when you are installing CA ARCserve Backup or upgrading CA ARCserve Backup from a previous release.

CA ARCserve Backup Tasks

CA ARCserve Backup does not support performing the following tasks:

- Installing CA ARCserve Backup agents on remote systems using Agent Deployment. Agent Deployment does not support using JIS2004 Unicode characters for host names, user names, and passwords.
- Using JIS2004 Unicode characters to specify customer information on the Customer Information dialog when installing CA ARCserve Backup.
- Browsing JIS2004 Unicode-based agent machine names, user names, and passwords.
- Specifying JIS2004 Unicode-based names on CA ARCserve Backup host names, primary server names, stand-alone server names, and member server names.
- Specifying JIS2004 Unicode-based directory paths for installing CA ARCserve Backup or any CA ARCserve Backup component, specifying file system device paths, catalog database path, and so on.
- Importing a host list from a text file with a file name that contains Unicode characters when you install and upgrade CA ARCserve Backup, agents, and options on remote systems.
- Importing a host list from a text file with a file name that contains Unicode characters when running Remote Agent Deployment.
- Specifying JIS2004 Unicode-based names on ARCserve-specific objects. For example, job names, Device Group names, Media Pool names, media names, location names, and session passwords for encryption.
- Specifying file names and file paths as criteria for creating a Vault Schedule using the Media Management Administrator using JIS2004 Unicode characters.
- Specifying JIS2004 Unicode characters on network directory and file shares.
- Specifying JIS2004 Unicode characters for the caroot password using the CA ARCserve Backup Server Configuration Wizard. The Server Configuration Wizard interprets Unicode characters as the question mark symbol "?," which is an acceptable character for the caroot password. However, after you set the caroot password using the Server Configuration Wizard, you will not be able to change the caroot password from the Manager Console.

- Sending Alert email messages with file attachments when the file attachments are stored in directories that are named with Unicode characters.

Note: The file attachment itself can contain Unicode characters.

- Renaming and editing XML content in the report template files using JIS2004 Unicode Characters. The generated reports will not display properly. The report template files are stored in the following directory:

ARCserve_Home\template\reports

CA ARCserve Backup Reports

CA ARCserve Backup does not support creating the following reports when using an ARCserve server that is running CA ARCserve Backup for Windows r12.5 connect remotely to an ARCserve server that is running CA ARCserve Backup for Windows r12 Service Pack 1 or CA ARCserve Backup for Windows r12.

- 7 days Backup Status Report.xml
- 7 days Job Status Report.xml
- 7 days Media Usage History Report.xml
- ARCserve Backup for Laptops and Desktops Session Details Report.xml
- Backup Client Data Size Report.xml
- Backup Clients And Job Associations Report.xml
- Backup Window And Throughput Comparison Report.xml
- Daily Backup Status Report.xml
- Daily Failed Backups Report.xml
- Daily Job Status Report.xml
- Detailed Media Pool Report.xml
- Detailed Media Usage By Backup Clients Report.xml
- Failed Backups Report.xml
- Media Required For Data Recovery Report.xml
- Staging Migration Report.xml
- Staging Purge Failed Report.xml
- Staging SnapLock Report.xml
- Staging Summary Report.xml
- Custom Report (New Report)

Index

6

64-bit Windows platform support • 40, 137

A

Activity Log

- data • 312, 313, 619, 653
- organizing • 314
- pruning • 314

administrative shared drives • 127

Agent for Open Files, managing • 177

Alert Manager • 25, 643

- configuration options • 645

ARCserve database

- database protection job, about • 562
- database protection job, deleting • 574
- database protection job, modifying • 564
- database protection job, recreating • 575
- database protection job, starting • 573
- device records • 555
- error reporting • 555
- MS SQL index rebuilding • 555
- protecting • 557
- pruning • 554
- restoring • 576

Audit Log Reports • 623

B

backing up data

- backing up data, deduplication • 686
- BrightStor ARCserve Backup for Laptops & Desktops • 238
- destination options, backing up • 138
- differential backup • 289
- entire nodes • 187
- incremental backup • 289
- multiplexing • 180, 183, 184
- multistreaming, defined • 178
- schedules and rotations • 139
- setting up jobs • 133
- specifying a backup destination • 138
- submitting backup jobs • 131
- using the Disk Staging Option • 217

Backup Manager • 25, 132

- global backup options • 142

bar codes • 406

broadcast option • 646

C

CA Antivirus

- updating • 443, 446

ca_auth command • 36, 37, 493

ca_devmgr command • 196, 224

ca_jobsecmgr command • 38

ca_log command • 313

ca_mmo command • 422, 423, 428, 432

cabatch command • 35

CAReports command • 631, 633

catalog database

- about • 599
- enabling media pool maintenance • 557
- enabling the catalog database • 602

central management

- administering ARCserve servers • 52
- managing devices • 52
- managing jobs • 48
- managing licenses • 54
- managing the ARCserve database • 50
- monitoring jobs • 49
- using alerts • 52
- using job history • 56
- using logs • 50
- using reports • 51

change password, system account • 480

change the ARCserve system account password • 524

changing an ARCserve computer name

- about • 496
- changing a Manager Console system • 506
- changing a member server computer name • 504
- changing a primary server computer name • 497
- changing a stand-alone server computer name • 506

clean media • 375

cleaning tape heads • 366, 375

clusters

- cluster, deployment considerations • 730
- failover • 726
- mirrored disk • 729
- overview • 723

-
- protection • 731
 - MSCS application protection • 734
 - MSCS self-protection • 733
 - NEC CLUSTERPRO application protection • 736
 - NEC CLUSTERPRO self-protection • 736
 - quorum disk • 730
 - resource group • 727
 - shared disk • 728
 - virtual name • 727
 - clusters, NEC clusters • 751
 - change cluster domain • 762
 - change database • 764
 - demote primary server • 764
 - deployment planning • 738
 - disable cluster scripts • 769
 - enable cluster scripts • 766
 - failover support • 741
 - hardware requirements • 751
 - installation • 755
 - promote member server • 764
 - remove CA ARCserve Backup from cluster • 772
 - resource preparation • 754
 - software requirements • 751
 - stop cluster groups • 765
 - stop HA service monitoring • 761
 - compressing media • 362
 - configuration tools
 - Device Configuration • 203, 393
 - device group configuration • 206, 393
 - configure node tiers • 481
 - configure SQL Server as the ARCserve database • 612
 - configure SQL Server Express as the ARCserve database • 618
 - contacting technical support • v
 - Copy Utility • 33
 - cstart command • 438
 - cstop command • 438
 - customer support, contacting • v
- D**
- database
 - agents • 127, 241
 - Database Engine • 435, 474
 - Database Manager • 25, 554
 - MS SQL configuration • 607, 610, 611
 - MS SQL index rebuilding • 555
 - ODBC data source configuration • 610
 - pruning • 311, 314, 554
 - Database Manager • 25, 554
 - database protection job
 - about • 562
 - deleting • 574
 - modifying • 564
 - recreating • 575
 - starting • 573
 - decryption, data • 102
 - deduplication
 - deduplication, configure groups option • 355
 - deduplication, create device • 343
 - deduplication, device group • 350
 - deduplication, modify device • 349
 - deduplication, remove device • 348
 - defined • 677
 - demote a primary server to a member server • 520
 - demote a primary server to a member server • 520
 - demote a primary server to a member server (MSCS clusters) • 747
 - demote a primary server to a member server (NEC cluster) • 764
 - Device Configuration • 203, 393
 - Device Configuration, deduplication device configuratio • 343, 350, 355
 - Device Wizard • 109
 - file system device configuration • 339
 - RAID device configuration • 336
 - Removable Storage Management, controlling devices • 338
 - replacing devices • 380
 - tape and optical library configuration • 331
 - virtual library configuration • 337
 - device group configuration • 206, 393
 - Device Manager • 25, 331, 357
 - Device Wizard • 109
 - Diagnostic Wizard • 634
 - viewing reports, Diagnostic Wizard • 638
 - Discovery Configuration • 544
 - Disk to Disk to Tape Option
 - alerting options • 212
 - architecture • 193, 226
 - configuration tasks • 202, 229
 - disabling staging • 222
 - disk staging license requirements • 217
 - Disk Staging, deduplication • 687
-

- features • 196
- FSD configuration • 203
- modify a schedule • 220
- multistreaming, Disk Staging Option • 196, 199
- overview • 194
- pause migration • 196, 221
- postscripts • 215
- reports • 196
- restoring data, staging backup • 267
- rotation scheme, modifying • 220
- SnapLock • 196
- staging group configuration • 206
- submit a disk staging backup job • 217
- submit a tape staging backup job • 232
- tape staging license requirements • 232

DLTSage error handling

- curing errors • 394
- overview • 393

Duplicate Sessions dialog • 267

E

- ejecting media • 358, 362
- email option • 648
- encryption algorithm • 104
- encryption, data,
 - about • 102
 - at the agent server • 105
 - during backups • 107
 - during migration • 108
 - encryption, data, with deduplication • 690
- engines
 - about • 435
 - Database Engine • 435, 474
 - Job Engine • 435, 452
 - service state icons • 437
 - status • 436
 - Tape Engine • 435, 464
- Enterprise Module • 39
- erasing media • 358, 359
 - options described • 359
- error log, devices • 555

F

- failover • 726
- Federal Information Processing Standards (FIPS) • 103
- filters
 - filtering options • 296

- filters, wildcards • 293
 - job filters • 293
 - types • 296
- firewall configuration • 551
- formatting media • 358
- full backup • 289

G

- GFS media pools • 407
- GFS rotations • 289, 407, 410, 411
- global backup options • 142
 - advanced backup options • 145
 - alert options • 143
 - backup media options • 152
 - global backup options, encryption options • 148
 - job log options • 174
 - media exporting options • 145
 - operation options • 157
 - retry options • 155
 - verification options • 154
 - virus options • 174
 - Volume Shadow Copy Service options • 150
- global password changes • 38
- global restore options • 256
 - alert options • 265
 - backup media options • 257
 - destination options • 258
 - job log options • 264
 - operation options • 261
 - pre/post options • 263
 - virus options • 264

H

- home page • 23

I

- importing and exporting media • 366
- installation considerations
 - Microsoft SQL Server • 607
- integrating products
 - BrightStor ARCserve Backup for Laptops & Desktops • 238
- interact with the desktop • 473
- inventory slots • 366
- inventorying slots • 369

J

- Job Scheduler Wizard • 324

- schedule a custom report, Job Scheduler wizard • 631
- job scripts • 325, 326
- Job Status Manager • 25, 300
 - Job Detail tab • 316, 620
 - Job Log tab • 316
 - job queue • 304
 - job status, types • 306
 - multiple jobs, managing • 303
 - Tape Log tab • 316, 619
- job status, types • 306

L

- labeling • 367
- library functions • 366
 - cleaning tape heads • 366, 375
 - importing and exporting media • 366
 - inventory slots • 366
 - mounting and dismounting media • 366
 - online and offline libraries • 366, 378
- library groups
 - assigning slots • 384
 - creating • 383
 - deleting • 387
 - removing slots • 387
 - renaming • 387
- log in to CA ARCserve Backup • 88
- logs • 649
 - Job Log data • 620
 - Tape Log data • 619

M

- magazines, mounting and dismounting • 371
- Manager Console
 - opening • 44
- managing domain servers • 492
- managing jobs
 - Job Detail tab • 316, 620
 - Job Log data • 620
 - Job Log tab • 316
 - job queue • 304
 - job templates • 326, 327
- media
 - cleaning • 375
 - consolidation during migration • 399
 - expiration Date • 367
 - media maximization • 398
 - online and offline removable drives • 378
- Media Assure & Scan Utility • 32

- Media Pool Manager • 25, 331, 413
- media pools • 403
 - GFS media pools • 407
 - media pools, with deduplication devices • 702
- Microsoft SQL Agent Configuration utility • 559
- Microsoft SQL Server
 - ARCserve database, backup options • 569
 - database consistency check • 611
 - installation considerations • 607
 - ODBC configuration • 610
 - SQL connections • 610
- Microsoft SQL Server 2005 Express Edition
 - ARCserve database, backup options • 567
- migration consolidation • 399
- mirrored disk • 729
- MM Admin
 - find media in vault object • 422, 431
 - overview • 25, 331, 415
 - reports object • 420
 - rotation object • 419
 - schedule object • 418
 - special tape volume movement, permanent retention • 429, 431
 - special tape volume movement, temporary check in • 429, 430
 - status object • 422
 - vault criteria descriptor object • 418
- mounting and dismounting media • 366
- move a member server to a different domain • 524
- moving media • 383
- MSCS clusters • 737
 - change cluster domain • 748
 - change database • 747
 - cldelete cluster resources • 746
 - clrebuild cluster resources • 745
 - delete cluster resources • 746
 - demote primary server • 747
 - deployment planning • 738
 - failover support • 741
 - hardware requirements • 737
 - installation • 741
 - promote member server • 747
 - rebuild cluster resources • 745
 - remove CA ARCserve Backup from cluster • 750
 - resource preparation • 740
 - software requirements • 738
 - stop HA service monitoring • 743

multiple jobs, managing • 303

N

navigation bar • 23

NEC clusters • 751

- change cluster domain • 762

- change database • 764

- demote member server • 764

- deployment planning • 738

- disable cluster scripts • 769

- enable cluster scripts • 766

- failover support • 741

- hardware requirements • 751

- installation • 755

- promote member server • 764

- remove CA ARCserve Backup from cluster • 772

- resource preparation • 754

- software requirements • 751

- stop cluster groups • 765

- stop HA service monitoring • 761

network interface cards, configuring multiple • 485

node tier • 481

O

online and offline libraries • 366, 378

Optimize Restore feature • 196

options

- Compare Utility options • 33

- Count Utility options • 33

- Discovery Configuration options • 543, 545

- filtering options • 296

- local backup options • 128, 141

- Media Assure & Scan Utility options • 32

- options, deduplication device group • 350, 355

- Purge Utility options • 34

- staging options • 203, 206, 217, 220, 221, 222

P

password changes, global • 38

pfc command • 186

Preflight Check Utility • 186

promote a member server to a primary server • 517

- promote a member server to a primary server • 517

promote a member server to a primary server (MSCS clusters) • 747

promote a member server to a primary server (NEC clusters) • 764

Q

Quick Start menu • 23

quorum disk • 730

R

rebuild media • 358, 364

removable drive support • 391

removable media support • 389

replacing devices • 380

Report Manager • 25, 620, 622, 633

- custom reports • 622

- report categories • 623

- schedule a custom report, Report Manager • 630

- standard reports • 622

Report Writer Utility • 34

- creating custom reports • 631

Restore Manager • 25, 241

- global restore options • 256

restoring data

- destination options • 254

- duplicate backup sessions • 250

- Smart Restore • 196, 250

- source options • 243

- staged backups • 267

- version history • 249

retensioning media • 358, 361

rotation • 429

- creating a rotation • 414

- deleting a rotation • 432

- modifying a rotation • 431

rotations • 287, 289, 299

S

SAN

- backup plans • 708

- benefits • 709

- control job run time • 717

- create shared device groups • 713

- data backup and restoration • 715

- device management • 716

- environment • 706

- how the option works • 707

- installation • 711

- installation prerequisites • 710
- licensing • 705
- media management • 716
- operating system compatability • 710
- reports and logs • 717
- server management • 708
- terminology • 709
- troubleshooting • 718
- using the option • 713
- virtual libraries • 718
- save sets • 405
- scanning devices • 358, 364
- schedule a custom report, Job Scheduler wizard • 631
- scheduling jobs • 287, 289, 298, 299
 - backup jobs • 139
 - restore jobs • 254
- scratch sets • 405
- serial numbers and bar codes • 406
- Server Admin • 25
- Server Configuration Wizard
 - about • 511
 - change the ARCserve database application • 612, 618
 - change the domain administrator password • 524
 - demote a primary server • 520
 - how to start • 516
 - move a member server • 524
 - move the ARCserve database to a different system or instance • 615
 - promote a member server • 517
 - tasks • 513
- service state icons • 437
- shared disk • 728
- signatures, eTrust • 443, 446
- SnapLock • 196
- SNMP alerts • 651
- stopping and starting services • 438, 439
- Storage Area Network (SAN) • 706
- support, contacting • v
- system account • 36, 37, 480, 493
- system state restore options • 266

T

- Tape Engine
 - changing the system account • 480
 - configuration • 464, 465, 468
 - location, log file • 470

- manage the size of the log file, Circular Logging • 471, 472
- message log options • 465
- pruning, tape log file • 472
- Tape Log data • 619
- Tape Log tab • 316, 619
- tape movement, scheduling MM Admin
 - deleting a schedule • 426
- tape staging
 - alerting options • 212
 - architecture • 226
 - migration policies • 229
 - miscellaneous policies • 230
 - overview • 228, 229
 - postscripts • 215
 - submit a backup job • 232
- tape usage optimization • 398
- tapecopy command • 224, 250, 290
- technical support, contacting • v
- tier • 481

U

- Unicenter TNG option • 646
 - Unicenter Monitoring Agent • 633
- uninstall CA ARCserve Backup
 - MSCS cluster • 750
 - NEC cluster • 772
- updating • 443, 446
- USB storage devices • 358, 364, 388
- User Profile Utility
 - adding or deleting a user • 494
 - assigning a user to a group • 495
 - changing a user password • 495
- user profiles
 - administrator profile • 36
 - equivalence • 36, 37
- utilities • 23, 28
 - Compare Utility • 33
 - Count Utility • 33
 - Diagnostic Utility • 634
 - INODIST utility • 446
 - Media Assure & Scan Utility • 32
 - Preflight Check Utility • 186
 - Purge Utility • 34
 - Report Writer Utility • 34
 - User Profile Utility • 35, 494

V

- vault criteria descriptor (VCD) • 427

- creating a VCD • 428
- deleting a VCD • 428
- modifying a VCD • 428
- vault criteria descriptor object • 418
- vaults • 424
 - creating a vault • 425
 - deleting a vault • 426
 - modifying a vault • 425
- VMware • 40

W

- wildcards • 293
- Windows-powered NAS • 327, 328
- wizards • 23
 - Diagnostic Wizard • 634
 - Job Scheduler Wizard • 324
 - Server Configuration Wizard • 511
- WORM media • 391