CA ARCserve® D2D

User Guide

r16

CA Technologies Product References

This document references the following CA Technologies products:

- CA ARCserve® Central Applications
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Virtual Standby
- CA Nimsoft Monitor

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Support Links for CA ARCserve D2D:

CA Support Online offers a rich set of resources for resolving your technical issues and provides easy access to important product information. With CA Support, you have easy access to trusted advice that is always available. The following links let you access the various CA Support sites that are available to help you:

Understanding your Support

This link provides information about maintenance programs and support offerings, including terms and conditions, claims, and service hours.

https://support.ca.com/prodinfo/d2dsupportofferings

Registering for Support

This link takes you to the CA Support Online registration form which is used to activate your product support.

https://support.ca.com/prodinfo/supportregistration

Accessing Technical Support

This link takes you to the One-Stop Product Support page for CA ARCserve D2D.

https://support.ca.com/prodinfo/arcserved2d

Documentation Changes

The following CA ARCserve D2D r16 changes have been included in the documentation as of the last release:

Update 8

- Test Fixes installed. For more information, see Issues Fixed in the Release Notes.

- Microsoft Exchange 2010 SP3 support is added.

Update 7

- Option to create recovery sets (Disable infinite incremental backups when needed).

  You can configure how many recovery sets to retain, starting with a full backup, and when the number of recovery sets exceeds the user-specified one, the oldest recovery set will be deleted, instead of merged.

- Merge Multiple Sessions at the Same Time.

  This process separates the merge job in a dedicated application, allowing the merge job to merge multiple sessions at the same time. The merge job can be started/stopped and paused/resumed on demand and does not affect any other jobs.

  This new merge process avoids multiple reads and writes because it only merges the latest change for each block. The merge process ignores all the changes that have occurred to the same block during any intermediate incremental backups. Merging multiple sessions at the same time is faster than merging them individually.

- CA ARCserve D2D Probe for Nimsoft.

  The CA ARCserve D2D Probe for Nimsoft is a software module that sends the CA ARCserve D2D alerts and backup job status to the Nimsoft server. You can view the alerts from both the Nimsoft Infrastructure Manager and the Nimsoft Unified Management Portal (UMP). However, you can only view the job status data from the UMP. The advantage of using Nimsoft to monitor the alerts and status is that you can monitor multiple CA ARCserve D2D servers from one central location. Nimsoft also lets you run CA ARCserve D2D commands such as full backup, incremental backup, and verify backup using the Nimsoft Probe utility.

Update 6

- Support for all Amazon regions.

  The following regions are supported and can be selected as the file copy destination:

  - AP_Singapore

  - EU_Ireland

  - US_Standard

- US_West (Northern California)

- AP_Tokyo

- US_West (Oregon)

- SA_East (Sao Paulo)

■ Support for cloud vendor Fujitsu Cloud (Windows Azure).

■ Support for VMware Virtual Disk Development Kit (VDDK) 5.0 Update 1. (Shipped with CA ARCserve D2D Update 6)

■ Animated CA ARCserve D2D Monitor tray icon indicates when any job is running and includes the progress completed.

   You can easily find out if a job (backup, restore, file copy, copy recovery point, catalog, or granular restore catalog) is running without logging in to CA ARCserve D2D. The job status is indicated on the CA ARCserve D2D tray monitor with an animated icon when the job starts.

■ Live Chat link added to the CA ARCserve D2D home page.

   Live Chat provides real-time monitoring and live help/support. Live Chat lets you optimize intelligent conversation between you and the CA ARCserve D2D Technical Support team, allowing you to address your concerns and questions immediately, while still maintaining access to the product. Upon completion of the chat session, you can send a transcript of the chat to your email address.

   Note: You may need to add the Live Chat link to your Trusted sites.

■ The date/time format for supported languages is displayed based on the locale.

Update 5

■ UEFI (Unified Extensible Firmware Interface) Support--UEFI is a firmware interface that Windows Vista SP2 (x64), Windows 2008 (x64), Windows 2008 R2, and Windows 7 (x64) supports. CA ARCserve D2D includes the following UEFI Support:

- Computers that adhere to the Extensible Firmware Interface (EFI) use the EFI System Partition, which is a partition on a data storage device. The EFI System partition is critical for Bare Metal Recovery (BMR). Therefore, when you select boot volume "C" on a UEFI system, the EFI System Partition is selected automatically for the backup source for BMR and an information message is displayed.

- To perform BMR for a UEFI system, you must boot the computer in UEFI mode. BMR does not support restoring a computer with different firmware.

■ Mount Recovery Point--Provides the ability to mount a recovery point to a drive letter (volume) or an NTFS folder, to view, browse, copy, or open the backup files directly in Windows Explorer.

■ Application Recovery Support--CA ARCserve D2D now supports Microsoft SQL Server 2012 Express/Web/Standard/Business Intelligence/Enterprise.

Update 4

- Addition of a Test Email feature on the Email Settings dialog (Preferences Settings).

- Email alerts for failed or crashed jobs are sent with a high importance visual indicator.

- Addition of an Advanced Backup Settings field for Reserve Space on Destination.

Update 3

- No documentation impact.

Update 2

- No documentation impact.

Update 1

- No documentation impact.

GA Release

- Rebranded to CA Technologies.

- Updated to include the following new features:

  - **Updates** - Added the capability to check for new updates to CA ARCserve D2D (manually initiated or scheduled automatically), and to download and install these updates when available.

  - **File Copy** - Added the capability to copy files (and retain or move from the source location) to help you reduce storage cost, meet compliance, and improve data protection. Lets you copy files to disk or to cloud based upon your specified policies.

  - **Encryption/Decryption** - Added the capability to encrypt and protect (with encryption passwords) your sensitive data and also decrypt the encrypted data after recovery.

  - **Exchange Granular Restore** - Added the capability to perform granular-level recovery of Microsoft Exchange objects (mailboxes, folders, or mail).

- Updated to include user feedback, enhancements, corrections, and other minor changes to help improve the usability and understanding of the product or the documentation itself.

Contents

Chapter 6: Troubleshooting CA ARCserve D2D   301

Appendix A: Frequently Asked Questions (FAQ)   325

Appendix B: Configuration Files   329

Appendix C: Files Affected During Installation/Uninstallation   335

Appendix D: Using the CA ARCserve D2D Probe for Nimsoft   349

Appendix E: Recovery Point Merge Failure May Render Recovery Point Unrecoverable   361

Index   367

Chapter 1: Understanding CA ARCserve D2D

This section contains the following topics:

Introduction

CA ARCserve D2D is a disk-based backup product designed to provide a fast, simple, and reliable way to protect and recover critical business information. CA ARCserve D2D is a light-weight solution for tracking changes on a machine at the block level and then backing up only those changed blocks in an incremental fashion. As a result, CA ARCserve D2D lets you perform frequent backups (as frequently as every 15 minutes), reducing the size of each incremental backup (as well as the backup window) and providing a more up-to-date backup. CA ARCserve D2D also provides the capability to restore files/folders, volumes, and applications, and perform bare metal recovery from a single backup. In addition, CA ARCserve D2D also lets you copy and restore backed-up data from your specified cloud storage location.

CA ARCserve D2D Documentation

The latest CA ARCserve D2D documentation can be accessed as follows:

- **User Guide:**

  The same topics contained in the CA ARCserve D2D Help system are also available as a User Guide in PDF format. The latest PDF version of this guide can be accessed from here:

  CA ARCserve D2D User Guide.

- **Release Notes:**

  The CA ARCserve D2D Release Notes contains information relating to system requirements, operating system support, application recovery support, and other information you may need to know before installation of this product. In addition, this document also contains a list of known issues that you should be aware of before you use this product. The latest version of the Release Notes can be accessed from here:

  CA ARCserve D2D Release Notes.

About this Document

This document is intended to provide you with the information to understand, install, use, and maintain CA ARCserve D2D in the most practical and efficient manner. This document is divided into the following major categories to help you easily identify and locate the specific information you are seeking.

The online help version of this document provides a link at the bottom of each topic to let you submit feedback to us about this document. We continually strive to make our documentation as complete, error free, and easy-to-read as possible. You can help by giving us feedback. Thank you in advance!

Understanding CA ARCserve D2D	This section contains an overview of the features of CA ARCserve D2D, with process-flow descriptions of how some key features work. By understanding how the features work, it should be easier to understand and perform the related tasks.
Installing CA ARCserve D2D	This section contains information about installing CA ARCserve D2D, including any pre-installation considerations you should be familiar with, the installation procedure to be performed, and instructions if you want to perform a silent installation.
Getting Started with CA ARCserve D2D	This section contains an overview of the CA ARCserve D2D user interface, and detailed information about each individual area of this interface. Before you use CA ARCserve D2D, it is important that you become familiar with the details of this interface.
Settings	This section contains information to understand and manage the various CA ARCserve D2D configuration settings.
Using CA ARCserve D2D	This section contains the step-by-step procedures for such tasks as performing ad-hoc backups, restoring from backups, copying recovery points, viewing logs, remote deploying, file copying, performing BMR, and installing any CA ARCserve D2D self-updates.
Troubleshooting CA ARCserve D2D	This section contains some fault-isolation information necessary to quickly identify and locate the source of a problem so that it can be remedied and allow CA ARCserve D2D to become fully operational again.
Appendix	The appendix section at the end of this document contains a collection of useful and supplementary information which is not necessary for proper usage of CA ARCserve D2D, but still may be of interest or use to you.

Features

CA ARCserve D2D provides the following features:

CA Support: What's New for this Release

YouTube: What's New for this Release

BACKUP

CA ARCserve D2D provides the following backup features:

- Lets you perform different types of backup jobs, such as full, incremental, or verify.

- Provides volume filtering capability to let you specify to back up only the selected volumes.

  - If the specified backup destination is on the local volume, a warning message displays notifying you this volume is not being backed up.

  - If system/boot volume is not selected for backup, a warning message displays notifying you the backup is unusable for Bare Metal Recovery (BMR).

- Protects all specified volumes of your computer (except if the volume contains the backup destination).

- Lets you encrypt and protect (with encryption passwords) your sensitive data.

- Lets you set/change backup schedules (or immediately initiate a customized backup).

- Lets you remotely manage several computers (one at a time).

- Lets you perform backups from both CA ARCserve D2D and CA ARCserve Backup simultaneously.

- Provides a system tray monitor to display status/notification information and perform quick actions.

Block Level Incremental Backups

– Only backs up the blocks on the source volumes that have changed after the last successful backup.

– Significantly reduces the amount of backup data.

If you have a large file and you only change a small portion of this file, CA ARCserve D2D backs up only the changed portion to the incremental backup. CA ARCserve D2D does not back up the whole file.

– Consumes less disk space and less time.

– Lets you perform more frequent backups, making the backup images more up-to-date (as often as every 15 minutes) for recovery.

Infinite Incremental (I^2) Snapshots

– Initially creates one full backup and then intelligently creates incremental snapshot backups forever (after the initial full backup).

– Uses less storage space, performs backups faster, and puts less load on your production servers.

– Can automatically collapse (merge) incremental changes optimizing the use of disk storage.

Application Consistent Backups

– Takes advantage of Windows Volume Shadow Copy Service (VSS) to ensure data consistency for any VSS-aware application.

– Provides recovery of both Microsoft SQL Server and Microsoft Exchange Server (without performing a full disaster recovery).

Ad-hoc Backups

An ad-hoc backup is one that is created when the situation makes it necessary, rather than being arranged in advance or being part of a plan.

– Provides you with the flexibility to perform "ad-hoc" backups outside of the scheduled backups.

For example, you have a repeat schedule for Full, Incremental, and Verify backups and you want to make major changes to your computer. You can perform an immediate backup without waiting for the next scheduled backup to occur.

– Provides you with the capability to add a customized (unscheduled) recovery point so that you can roll back to this previous point in time if necessary.

For example, you install a patch or service pack and then discover it adversely affects the performance of your computer. You can roll back to the ad-hoc backup session that does not include it.

Change Backup Destination

– Provides you with the capability to change the backup destination. When the disk space on your destination volume reaches its maximum capacity, CA ARCserve D2D lets you change the destination and you can continue with full or incremental backups.

Note: You can also configure email alert notifications for Destination Threshold so that you can be informed if it reaches the specified threshold value.

Copy Recovery Points

– Provides you with the capability to copy recovery point data and safely store it off-site for the purpose of restore in a catastrophe, or you can save your recovery points to multiple locations. In addition, if your destination is getting full you can consolidate your backups into a single recovery point which resembles the exact state at that point. When you select a recovery point to copy, you are capturing:

■ Backup blocks that were created for that specified point-in-time.

■ Whatever previous backup blocks are necessary to recreate a full and most recent backup image.

– The Copy Recovery Points feature can be launched manually (ad-hoc) or automatically based upon your specified schedule.

Mount Recovery Points

Provides the ability to mount a recovery point to a drive letter (volume) or an NTFS folder, to view, browse, copy, or open the backup files directly in Windows Explorer.

Backup Speed Throttling

Provides you with the capability to specify the maximum speed (MB/min) at which your backups are written. You can throttle the backup speed to reduce CPU or network use. However, limiting the backup speed, has an adverse effect on the backup window. As you lower the maximum backup speed, it increases the amount of time of perform the backup.

Note: By default, the Throttle Backup option is not enabled and backup speed is not being controlled.

Reserve Space on Destination

Provides you with the capability to specify a percentage of the calculated space that is necessary to perform a backup. This amount of continuous space is then reserved on the destination before the backup starts writing data and helps improve backup speed.

Backup Status Monitoring

CA ARCserve D2D provides the capability to monitor:

– Last backup status

– Recovery Points

– Destination capacity

– Protection summary

– Most recent events

– License notifications

Job Status Monitoring

CA ARCserve D2D provides the capability to monitor:

– Details about the next scheduled job

– Details about the currently running job

RESTORE

CA ARCserve D2D provides the following restore features:

■ Restore data from specific recovery points.

■ Search/browse to a specific file/folder to restore.

■ Restore from File Copy.

■ Restore a virtual machine (VM) that you previously backed up.

■ Set the restore destination to an alternate location or server.

■ Restore encrypted backup data

■ Granular-level restore of Exchange objects

Types of Restores

CA ARCserve D2D provides the following types of restores:

■ **File-Level Restore**

Restores any backed up files/folders.

■ **Recovery Point Restore**

Restores backed up data based from a specified point in time (recovery point).

■ **File Copy Restore**

Restores File Copy data from a disk or cloud.

■ **Exchange Granular-Level Restore**

Restores individual Exchange objects (mailboxes, mailbox folders, or mail).

■ **Virtual Machine (VM) Recovery**

Restores a VM that you previously backed up.

■ **Application Restore**

Restores backed up Microsoft SQL Server/Microsoft Exchange data at the database level.

■ **Explorer Integration Restore**

CA ARCserve D2D provides the capability to browse directly and restore files/folder and Exchange objects (mailboxes, mail folders, mail) from Windows Explorer by using the "Change to D2D View" option.

■ **Bare Metal Recovery (BMR)**

– Recovers a computer system from "bare metal", and includes the operating system, applications, and data components necessary to rebuild or restore the entire backed-up system. BMR is used for disaster recovery or for migration from one server to another.

– Restores to dissimilar hardware and resolves any hardware differences.

– Expands and restores to bigger disks if necessary.

– Provides the capability to perform the following types of V2P (Virtual to Physical) Bare Metal Recovery. This feature lets you perform V2P recovery from the latest state of a standby virtual machine and from any recovery point that has been previously converted from a CA ARCserve D2D backup session. This feature also helps you reduce the loss of your production computer.

– BMR from a Hyper-V server

– BMR from a VMware ESX or vCenter

Disk Resizing

– During a Bare Metal Recovery, you can restore the image to another disk and can resize the disk partitions if necessary (without losing any data that is stored on the drive).

– When restoring to another disk, the capacity of new disk must be the same size or larger than the original disk.

Note: Disk resizing if necessary is for basic disks only, and not for dynamic disks.

REMOTE DEPLOYMENT

After CA ARCserve D2D is installed on a server, you can further deploy it remotely to other servers.

ALERT NOTIFICATIONS

CA ARCserve D2D provides the following email alert notifications:

■ Missed jobs - Sends an alert notification for any scheduled job that did not run at the scheduled time.

■ Backup, Catalog, File Copy, Restore, or Copy Recovery Point job failure/crash - Sends an alert notification for all unsuccessful job attempts. This category includes all failed, incomplete, and canceled jobs, and crashed attempts.

Note: These email alerts are sent with a high importance. The email alerts that have a high importance level setting display a visual indicator of an exclamation point in their Inbox.

■ Backup, Catalog, File Copy, Restore, or Copy Recovery Point job success - Sends an alert notification for all successful job attempts.

■ Merge job stopped, skipped, failed, or crashed - Sends an alert notification for all stopped, skipped, failed, or crashed merge jobs.

■ Merge job success - Sends an alert notification for all successful merge jobs.

■ Backup destination free space is less than - Sends an email notification when the amount of unused space at the backup destination is less than a specified value.

■ New Updates Available - Sends an email notification when a new update for CA ARCserve D2D is available. Email notifications are also sent if a failure occurs during the check for updates or during the download.

■ Resource threshold alerts - Sends an alert notification when any specified resource performance threshold is reached. The monitored resource levels are CPU Usage (percentage), Memory Usage (percentage), Disk Throughput (MB/second) and Network I/O (percentage of NIC bandwidth currently using).

ENCRYPTION/DECRYPTION SUPPORT

CA ARCserve D2D provides the capability to encrypt and protect (with encryption passwords) your sensitive data and also decrypt the encrypted data after recovery.

■ Encryption support is provided for both uncompressed backup format and compressed backup format. (Uncompressed backup is no longer VHD format if encrypted).

■ Windows built-in encryption libraries are used for data encryption and decryption.

For Windows XP/2003/Vista/2008: CAPI (CryptoAPI) is used for data encryption.

For Windows 7/2008 R2: CNG (Cryptography API Next Generation) is used for data encryption.

Note: Data interoperability is supported both ways between CAPI and CNG, meaning that data that is encrypted on Windows XP/2003/Vista/2008 can be decrypted on Windows 7/2008 R2 (and vice versa). This data interoperability enables moving backups of any computer to a different computer, and to restore data from there.

■ Encryption password management provides a memory feature so that you do not need to remember encryption passwords when attempting to restore encrypted data. For every encrypted backup, the encryption password is saved in a password list file.

As long as you can log in to CA ARCserve D2D, there is no need to remember encryption passwords to restore data from current backups. (Current backups are defined as backups that were created from the same computer that you are logged in to). If you attempt to restore data from encrypted backups belonging to a different computer, you are always asked to provide the encryption password.

FILE COPY

File Copy can be used for copying critical data to secondary locations and can also be used as an archiving solution. File Copy allows you to safely and securely delete the source data after it has been copied to an off-site or secondary storage repository.

CA ARCserve D2D provides the following capabilities to copy or move files and help you reduce storage cost, meet compliance, and improve data protection.

Note: When you use the option File Copy - Delete Source, the data is moved from the source to the destination (deleted from source location). When you perform a file copy, the data is copied from the source to the destination (files remain intact on the original location).

■ Copy files to disk or to cloud based upon your specified policies.

■ Block-level file copying lets you save and store only the blocks of the source that have changed as of the last file copying. (Significantly reduces the amount of file copied data).

- Select the source to copy, which can be a specific volume, volumes, folder, or folders.

- Use filters to include or exclude files that are based upon your specific criteria or patterns.

- Specify a schedule for file copying that is based upon completion of a specified number of successful backups.

- File copy versions of the same source at the specified destination.

- Encrypt file copied data for security.

- Compress data before performing file copying process.

- Specify how long to retain file copy data.

- Specify how many versions of the data you can have on the destination.

  Note: CA ARCserve D2D does not copy application files, files with system attributes, and files with temporary attributes. Only a current backed-up source is eligible for file copying.

CA ARCserve D2D UPDATES

Provides the following capabilities for downloading and installing self- updates to CA ARCserve D2D:

- Check for new available updates to CA ARCserve D2D (manually initiated from the UI or system tray monitor or automatically as scheduled).

- Trigger automatic or manual downloading of updates.

- Specify a custom schedule to perform automatically periodic checks for updates.

- Trigger installation of updates either from the UI, the system tray monitor, or silently from the command line.

- Specify to send automatic email notifications when new updates become available (or when problems occur).

- Configure the client and or a staging server to connect to CA Support (directly or by way of a proxy server) to download available updates. (A staging server is a CA ARCserve D2D installed computer which is used as a temporary storage location for downloading an update before it is installed into a CA ARCserve D2D client computer from that staging server).

- Use staging servers for clients that have limited access to the Internet.

- Configure multiple staging servers for downloading the updates. If the primary staging server is unavailable, the download function automatically transfers to the next specified staging server.

- Remote deploy from one computer to another and let you move all updates configuration and email settings from that first computer to the deployed computer.

Note: All updates that are released for CA ARCserve D2D are cumulative. As a result, each update also includes all previously released updates to ensure that your computer is always up-to-date.

CA ARCserve D2D Videos

For those of you who believe that "a picture is worth a thousand words" CA ARCserve D2D provides various how-to videos that are designed to simplify your understanding and performance of specific tasks. Watching step-by-step videos is a great way to help you learn how to use CA ARCserve D2D features to perform essential system protection procedures.

Note: These videos are meant to supplement (and not replace) the written procedures that they are related to. Refer to the actual procedures for all detailed information (precautions, notes, examples, and so on) associated with each task.

You can access these instructional videos from the CA ARCserve D2D user interface or from within the product documentation. Simply choose the CA Support website or YouTube as the source for viewing these videos.

- To view CA ARCserve D2D videos on CA Support
- To view CA ARCserve D2D videos on YouTube

The versions of the videos from CA Support and YouTube are identical, and only the viewing source is different:

- For videos that are accessed from within the product documentation, links are provided to let you select which version you want to view.
- For videos that are accessed from the CA ARCserve D2D user interface, you can select the default source to view the version of these videos. (YouTube is the pre-selected default viewing source). For more information about setting your default video preference, see Specify General Preferences (see page 114).

The videos that are supplied are only a start, and we expect to have more created in the future. If you have any ideas for new videos, let us know. You can click the user interface link to Provide Feedback to Development, or post a comment on the Expert Advice Center. You can even send CA Technologies an email using the link at the bottom of all Online Help topics.

How CA ARCserve D2D Works

CA ARCserve D2D lets you perform frequent and periodic block level backups of your full machine. These backups can be stored on either an internal drive, an external drive, or on a remote network share. To avoid a continuous and never-ending backup cycle, the volume being backed up cannot be specified as the backup destination. CA ARCserve D2D provides the capability to perform Full, Incremental, or Verify type backups.
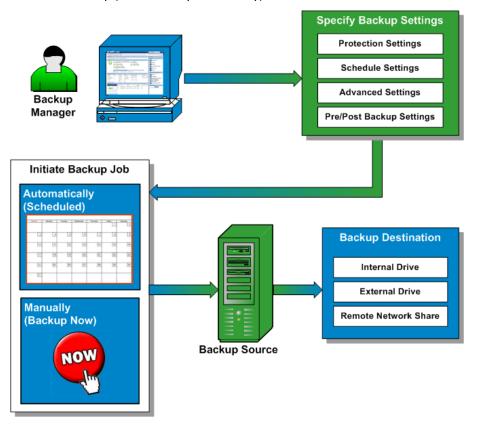
CA ARCserve D2D also provides various methods to identify and locate the backed up data and allow you to restore it if necessary. Regardless of which restore method you select, CA ARCserve D2D lets you quickly identify the data you need and retrieve it from the appropriate backup location.

How the Backup Process Works

CA ARCserve D2D lets you perform frequent and periodic block level backups of your entire machine. These backups can be stored on an internal drive, an external drive, or on a remote network share. CA ARCserve D2D provides the capability to perform Full, Incremental, or Verify type backups.
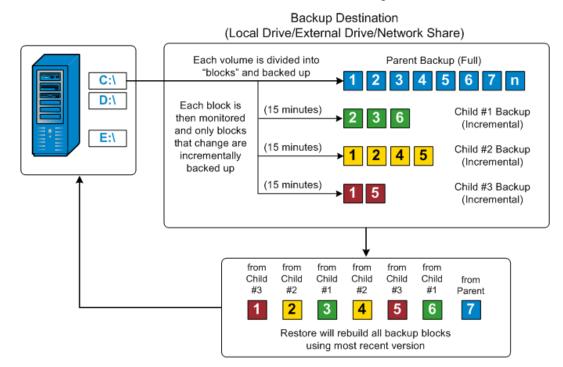
The basic process for how CA ARCserve D2D performs a backup is simple. When you initiate a backup (either as scheduled or manually launched), CA ARCserve D2D captures a full VSS snapshot, and then backs up only those blocks that have been changed since the previous successful backup. (If it is a Full backup, all blocks are backed up). This block-level incremental backup process significantly reduces the amount of backup data. For example, if you have a large file and only change a small portion of this file, CA ARCserve D2D backs up only the changed portion to the incremental backup and not back up the entire file.

During this block-level incremental backup process, CA ARCserve D2D not only captures the data, but also creates a catalog containing all information related to the operating system, installed applications (Microsoft SQL and Microsoft Exchange only), configuration settings, necessary drivers, and so on. If necessary, you can then restore this backed-up image to recover your data or your entire machine. To avoid a continuous and never-ending backup cycle, the volume being backed up cannot be specified as the backup destination.

The details of what is being backed up, how it is being backed up, when it is being backed up, and so on, are controlled by the various backup configuration settings that you specify. These settings are applied to each backup job, regardless of how you initiate the backup (automatically or manually).
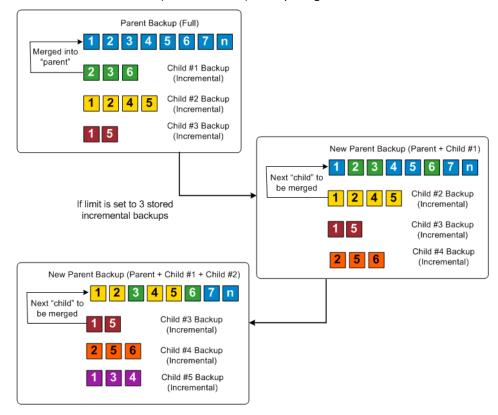

How Block-Level Incremental Backups Work

When you start a backup, the specified volume is divided into a number of subordinate data blocks that are then backed up. The initial backup is considered the "parent backup" and will be a Full Backup of the entire volume to establish the baseline blocks to be monitored. Before performing the backup, a VSS snapshot is created, then an internal monitoring driver checks each block to detect any changes. As scheduled, CA ARCserve D2D will then incrementally back up only those blocks that have changed since the previous backup. CA ARCserve D2D lets you to schedule the subsequent block-level incremental backups ("child backups") as frequently as every 15 minutes to always provide accurate, up-to-date backup images.

If you need to restore the volume information, the most recent backed up version of each block is located and the entire volume is rebuilt using these current blocks.
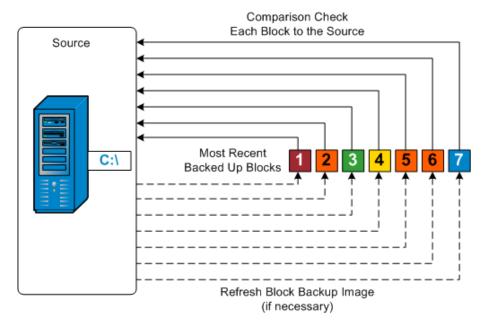

How Infinite Incremental Backups Work

If left alone, the incremental snapshots (backups) would continue, as often as 96 times each day (every 15 minutes). These periodic snapshots will accumulate a large chain of backed up blocks to be monitored each time a new backup is performed, and require added space to store these ever-growing backup images. To minimize this potential problem, CA ARCserve D2D utilizes the Infinite Incremental Backup process, which intelligently creates incremental snapshot backups forever (after the initial full backup) and uses less storage space, performs faster backups, and puts less load on your production servers. Infinite Incremental Backups allow you to set a limit for the number of incremental child backups to be stored by configuring the Recovery Points option from the Protection Settings tab on the Backup Settings dialog.

When the specified limit is exceeded, the earliest (oldest) incremental child backup is merged into the parent backup to create a new baseline image consisting of the "parent plus oldest child" blocks (unchanged blocks will remain the same). This cycle of merging the oldest child backup into the parent backup repeats for each subsequent backup, allowing you to perform Infinite Incremental (I^2) snapshot backups while maintaining the same number of stored (and monitored) backup images.
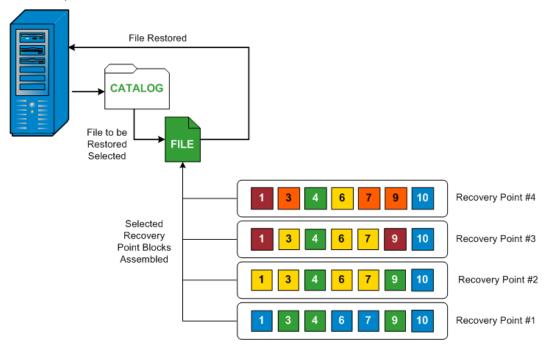
How Verify Backups Work

Every so often (as scheduled or when manually initiated), CA ARCserve D2D can perform a Verify (resynchronization) type backup to provide a confidence check of the stored backup image and resynchronize that image if necessary. A Verify type backup looks at the most recent backup of each individual block and compares the content and information to the source. This comparison verifies that the latest backed up blocks represent the corresponding information at the source. If the backup image for any block does not match the source (possibly because of changes in the system since the last backup), CA ARCserve D2D refreshes (resynchronizes) the backup of the block that does not match. A Verify backup can also be used to get the same guarantee as a full backup without taking the space of full backup. The advantage of a Verify backup is that it is small when compared to full backup because only the changed blocks (blocks that do not match the last backup) are backed up. However, a Verify backup is also slower than an Incremental backup because CA ARCserve D2D has to compare all of source disk blocks with the blocks of the last backup.

How File Level Restores Work

During a block-level backup, each backed up file is made up of a collection of blocks that define that particular file. A catalog file is created containing a list of the backed up files, along with the individual blocks that were used for each file and the available recovery points for these files. When you need to restore a particular file, you can search your backup and select the file you want to restore and the recovery point you want to restore from. CA ARCserve D2D then collects the version of the blocks that were used for the recovery point of the specified file, and reassembles and restores the file.
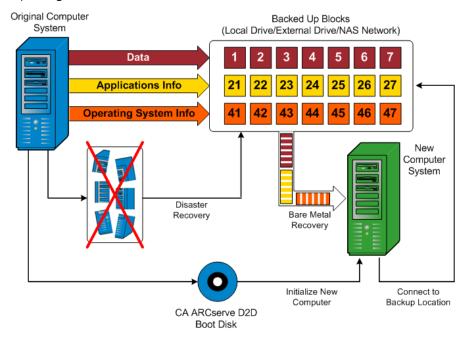
The following flow diagram shows the process of how CA ARCserve D2D restores a specific file.

How Bare Metal Recovery Works

Bare Metal Recovery is the process of restoring a computer system from "bare metal" by reinstalling the operating system and software applications, and then restoring the data and settings. The most common reasons for performing a bare metal recovery are because your hard drive either fails or becomes full and you want to upgrade (migrate) to a larger drive or migrate to newer hardware. Bare metal recovery is possible because during the block-level backup process, CA ARCserve D2D captures not only the data, but also all information related to the operating system, installed applications, configuration settings, necessary drivers, and so on. All relevant information that is necessary to perform a complete rebuild of the computer system from "bare metal" is backed up into a series of blocks and stored on the backup location.

Note: Dynamic disks are restored at disk level only. If your data is backed up to a volume on a dynamic disk, you will not be able to restore this dynamic disk (including all its volumes) during BMR.
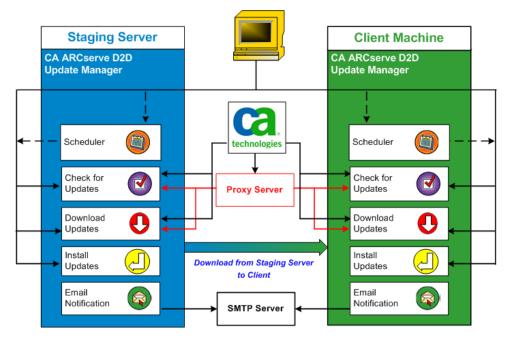

When you perform a bare metal recovery, the CA ARCserve D2D boot disk is used to initialize the new computer system and allow the bare metal recovery process to begin. When the bare metal recovery is started, CA ARCserve D2D will prompt you to select or provide a valid location to retrieve these backed up blocks from, as well as the recovery point to be restored. You may also be prompted to provide valid drivers for the new computer system if needed. When this connection and configuration information is provided, CA ARCserve D2D begins to pull the specified backup image from the backup location and restore all backed up blocks to the new computer system (empty blocks will not be restored). After the bare metal recovery image is fully restored to the new computer system, the machine will be back to the state that it was in when the last backup was performed, and CA ARCserve D2D backups will be able to continue as scheduled. (After completion of the BMR, the first backup will be a Verify Backup).

How CA ARCserve D2D Updates Works

A product update lets CA Technologies deliver product improvements to users. Updates are used to deliver bug fixes, new hardware support, and performance and security enhancements. Within CA ARCserve D2D, the Updates function simplifies this process and provides a fast, easy, and reliable solution to keep your CA ARCserve D2D installation up-to-date with the latest available updates. The Updates function is your link between CA Technologies and your CA ARCserve D2D installation.

CA ARCserve D2D Updates provide the following functions:

- Check for available updates (manual or scheduled)

- Download available updates from CA Technologies (either directly to a client machine or to a staging server first and then to a client machine)

- Install successfully downloaded updates (to be initiated manually)

- Send email notifications when a new update is available

Check for Updates

When CA Technologies Server is selected as download server, CA ARCserve D2D Updates provides the capability to connect to the CA Technologies server either directly or using a proxy server (as configured manually) to check for new and available CA ARCserve D2D updates. CA ARCserve D2D will directly connect to CA Technologies server using the proxy settings configured by browser (only applicable for IE and Chrome). This check for updates function can be triggered either manually from the user interface/tray monitor or automatically as specified by the Scheduler. (The internal Scheduler is responsible for starting at a scheduled day and time and triggering an automatic check and download of available updates).

When triggered, the update manager contacts the CA Technologies server to check the date /time stamp of a file that contains the available update information. If this available update information file has been modified since the last check, it will be downloaded from the server for comparison. The available update information is then compared to another file containing the already downloaded update information to determine if the available update is new and has not been previously downloaded. If the latest available update is not installed on your machine, CA ARCserve D2D displays an icon on the home page to inform you that a new update is available. In addition, an email notification can also be sent to inform you when a new CA ARCserve D2D update is available for downloading.

When Staging Server is selected as download server, CA ARCserve D2D downloads the available update information file from the staging server, and perform the same comparison check with the already available update information file. If the latest available update is not installed on your machine, CA ARCserve D2D will display an icon on the home page to inform you that a new update is available.

Note: All updates released for CA ARCserve D2D are cumulative. As a result, each update also includes all previously released updates to help ensure that your machine is always up-to-date. (The Help "About" dialog displays the update level installed on a machine. If necessary, you can use this information for building another server with the same configuration/patch level).

Download Updates

CA ARCserve D2D Updates provide the capability to download available CA ARCserve D2D updates either directly from the CA Technologies server (using HTTP) or from a staging server which in turn connects to the CA Technologies server. This download process is triggered automatically when the check for updates process determines that a new update is available (unless this auto-download function is disabled). You can configure CA ARCserve D2D to download an update directly (or using a proxy server) to your client machine or to a staging server. A staging server can be used as a temporary storage location for downloading an update before it is downloaded and installed into a CA ARCserve D2D client machine. You may not want to expose your client machine to the internet to download updates from the CA Technologies server. In this case, you can first download the update to a staging server and then allow other client machines to download the update from that staging server. CA ARCserve D2D provides the capability to configure multiple staging servers for downloading the updates. If for some reason the primary staging server is unavailable, the download function will automatically transfer to the next specified staging server.

Note: If you are using a staging server for your Updates downloads, CA ARCserve D2D must be installed on that staging server, but does not need to be licensed unless you are using CA ARCserve D2D to protect that staging server.

When triggered, the Updates function contacts the CA Technologies server and downloads the available update and places it in a holding directory (on either the staging server or the client machine) until directed to proceed with the subsequent installation process.

The default location for the download folder is: <Product Home>\D2DUpdates.

If for some reason, the download cannot be started, a popup message is displayed and CA ARCserve D2D waits a specified number of minutes and then attempt to download again. If after a specified number of retry attempts, the download still cannot continue, an error message will be displayed in the activity log indicating the most likely reason for the failure.

Install Updates

CA ARCserve D2D Updates provide the capability to install the available and successfully downloaded updates. This install process can only be triggered manually from the user interface/tray monitor (not automatically). When triggered, the update is installed from the holding directory to the applicable CA ARCserve D2D component directory of the client machine or the staging server. You cannot trigger the installation of the update directly from a staging server to a client machine. When you click install, the update is downloaded from the staging server to the client machine (if it has not been downloaded already), and then the installation process is triggered from the client machine.

Note: The installation only continues if no other active CA ARCserve D2D jobs are running. If another job is running, a message is displayed informing you of this condition and requesting that you try again at a later time.

If the installation is successful, the file containing the status information is updated for future use.

If the installation fails, an error message is displayed indicating the most likely reason for the failure.

Note: During the update installation CA ARCserve D2D will stop the D2D Web service and will restart this web service after successful installation of update.

Email Notifications

CA ARCserve D2D Updates provide the capability to send automatic email notifications when a new update is available. CA ARCserve D2D connects to an SMTP server (with appropriate credentials) to enable sending these email notifications over the Internet from CA Technologies to your server. (The email recipients are specified from the Preferences dialog).

In addition, email notifications are also sent if a failure occurs during the check for updates or during the download.

Chapter 2: Installing/Uninstalling CA ARCserve D2D

This section contains the following topics:

Installation Considerations

Review the following installation considerations before installing CA ARCserve D2D.

- The CA ARCserve D2D installation package is available through a web download and from the product installation CD.

- Verify that you have administrator privileges or the proper permissions to install software on the servers where you are installing CA ARCserve D2D.

- If you uninstall and install a new CA ARCserve D2D build and specify the same backup destination as the previous build, the first backup after the installation runs as a Verify backup.

- After you install CA ARCserve D2D to a server, there is a deployment link on the home page to let you deploy CA ARCserve D2D remotely. With this link, you are able to deploy CA ARCserve D2D to other servers remotely.

- If CA ARCserve D2D is being installed on a x64 Windows Core Operating System (Windows Server 2008/R2 Core edition), you should also install Windows-on-Windows 64-bit (WOW64) on the Server Core for the CA ARCserve D2D setup to work.

- By default, CA ARCserve D2D uses the Hypertext Transfer Protocol (HTTP) for communication among all of its components. If you are concerned about the security of information that is communicated between these components (including passwords), you can select this option to change the protocol being used to Hypertext Transfer Protocol Secure (HTTPS). For more information, see Change Server Communication Protocol (see page 296).

- If you previously participated in any Alpha or Beta testing for CA ARCserve D2D on the same system, you will not be able to continue performing backups to the same destination. To avoid possible merge problems, you should change your backup destination and start with a new backup set (Full Backup).

- If you are using both CA ARCserve D2D and CA ARCserve D2D On Demand within your backup environment, you should not mix backups between the two products (content from each product backed up to the same destination).

How the Installation Process Affects Operating Systems

The CA ARCserve D2D installation process updates various Windows operating system components using an installation engine named the Microsoft Installer Package (MSI). The components included in MSI let CA ARCserve D2D perform custom actions that let you install, upgrade, or uninstall CA ARCserve D2D.

The following table describes the custom actions and the affected components.

Note: All CA ARCserve D2D MSI packages call the components listed in this table when you install and uninstall CA ARCserve D2D.

Component	Description
CallAllowInstall	Lets the installation process check for conditions relating to the current CA ARCserve D2D installation.
CallPreInstall	Lets the installation process read and write MSI properties. For example, read the CA ARCserve D2D installation path from the MSI.
CallPostInstall	Lets the installation process perform various tasks relating to installation. For example, registering CA ARCserve D2D into the Windows Registry.
CallAllowUninstall	Lets the uninstallation process check for conditions relating the current CA ARCserve D2D installation.
CallPreUninstall	Lets the uninstallation process perform various tasks relating to uninstallation. For example, un-registering CA ARCserve D2D from the Windows Registry.
CallPostUninstall	Lets the uninstallation process perform various tasks after the installed files are uninstalled. For example, removing the remaining files.
ShowMsiLog	Displays the Windows Installer log file in Notepad if the end user selects the Show the Windows Installer log check box in the SetupCompleteSuccess, SetupCompleteError, or SetupInterrupted dialogs and then clicks Finish. (This works only with Windows Installer 4.0.)

Component	Description
ISPrint	Prints the contents of a ScrollableText control on a dialog.
	This is a Windows Installer .dll custom action. The name of the .dll file is SetAllUsers.dll, and its entry point is PrintScrollableText.
CheckForProductUpdates	Uses FLEXnet Connect to check for product updates.
	This custom action launches an executable file named Agent.exe, and it passes the following:
	/au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Uses FLEXnet Connect to check for product updates on reboot.
	This custom action launches an executable file named Agent.exe, and it passes the following:
	/au[ProductCode] /EndOfInstall /Reboot

Directories Updated

The installation process installs and updates CA ARCserve D2D files in the following directories by default (x86 and x64 operating systems):

> C:\Program Files\CA\ARCserve D2D

You can install CA ARCserve D2D into the default installation directory or into an alternate directory. The installation process copies various system files to the following directory:

> C:\WINDOWS\SYSTEM32

Windows Registry Keys Updated

The installation process updates the following Windows registry keys:

- Default registry keys:

  HKLM\SOFTWARE\CA\CA ARCserve D2D

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

Applications Installed

The installation process installs the following applications into your computer:

- CA Licensing

- Microsoft Visual C++ 2005 SP1 Redistributable

- Microsoft Windows Installer 3.1 Redistributable (v2) Package

- Java Runtime Environment (JRE) 1.6.0_16

- Tomcat 6.0.32

System Reboot Required by CA ARCserve D2D Installation

A system reboot is required by CA ARCserve D2D installation. One driver "ARCFlashVolDrv.sys" needs to be installed onto the target machine. This driver can only be loaded and take affect after a system reboot. Without the driver, the core functionality of CA ARCserve D2D will not work.

System Reboot Required by CA ARCserve D2D Uninstallation

A system reboot is required by CA ARCserve D2D uninstallation. One driver "ARCFlashVolDrv.sys" is installed onto the target machine while CA ARCserve D2D was installed. This driver will be loaded when the system is booted. To completely remove this driver from the machine, one system reboot after uninstallation is required.

Unsigned Binary Files

CA ARCserve D2D installs binary files that are developed by third parties, other CA Technologies products, and CA ARCserve D2D that are not signed. The following table describes these binary files.

Binary Name	Source
CALicense.msi	CA License
zlib1.dll	Zlib Compression Library
tomcat6.exe	Tomcat
tomcat6w.exe	Tomcat
awt.dll	Java Runtime Environment
cmm.dll	Java Runtime Environment
dcpr.dll	Java Runtime Environment
deploy.dll	Java Runtime Environment
deploytk.dll	Java Runtime Environment

Binary Name	Source
dt_shmem.dll	Java Runtime Environment
dt_socket.dll	Java Runtime Environment
eula.dll	Java Runtime Environment
fontmanager.dll	Java Runtime Environment
hpi.dll	Java Runtime Environment
hprof.dll	Java Runtime Environment
instrument.dll	Java Runtime Environment
ioser12.dll	Java Runtime Environment
j2pcsc.dll	Java Runtime Environment
jaas_nt.dll	Java Runtime Environment
java.dll	Java Runtime Environment
java.exe	Java Runtime Environment
java_crw_demo.dll	Java Runtime Environment
javacpl.exe	Java Runtime Environment
java-rmi.exe	Java Runtime Environment
javaw.exe	Java Runtime Environment
javaws.exe	Java Runtime Environment
jawt.dll	Java Runtime Environment
jbroker.exe	Java Runtime Environment
JdbcOdbc.dll	Java Runtime Environment
jdwp.dll	Java Runtime Environment
jli.dll	Java Runtime Environment
jp2iexp.dll	Java Runtime Environment
jp2launcher.exe	Java Runtime Environment
jp2native.dll	Java Runtime Environment
jp2ssv.dll	Java Runtime Environment
jpeg.dll	Java Runtime Environment
jsound.dll	Java Runtime Environment
jucheck.exe	Java Runtime Environment
jureg.exe	Java Runtime Environment
jusched.exe	Java Runtime Environment

Binary Name	Source
keytool.exe	Java Runtime Environment
kinit.exe	Java Runtime Environment
klist.exe	Java Runtime Environment
ktab.exe	Java Runtime Environment
management.dll	Java Runtime Environment
mlib_image.dll	Java Runtime Environment
msvcrt.dll	Java Runtime Environment
net.dll	Java Runtime Environment
npjp2.dll	Java Runtime Environment
nio.dll	Java Runtime Environment
npdeploytk.dll	Java Runtime Environment
npt.dll	Java Runtime Environment
orbd.exe	Java Runtime Environment
pack200.exe	Java Runtime Environment
policytool.exe	Java Runtime Environment
regutils.dll	Java Runtime Environment
rmi.dll	Java Runtime Environment
rmid.exe	Java Runtime Environment
rmiregistry.exe	Java Runtime Environment
jvm.dll	Java Runtime Environment
servertool.exe	Java Runtime Environment
splashscreen.dll	Java Runtime Environment
ssv.dll	Java Runtime Environment
ssvagent.exe	Java Runtime Environment
tnameserv.exe	Java Runtime Environment
unpack.dll	Java Runtime Environment
unpack200.exe	Java Runtime Environment
verify.dll	Java Runtime Environment
w2k_lsa_auth.dll	Java Runtime Environment
wsdetect.dll	Java Runtime Environment
zip.dll	Java Runtime Environment

Binary Name	Source
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft

Binary Files Containing Incorrect File Version Information

CA ARCserve D2D installs binary files that are developed by third parties, other CA products, and CA ARCserve D2D that contain incorrect file version information. The following table describes these binary files.

Binary Name	Source
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

Binary Files that Do Not Contain an Embedded Manifest

CA ARCserve D2D installs binary files that are developed by third parties, other CA Technologies products, and CA ARCserve D2D that do not contain an embedded manifest and do not contain a text manifest. The following table describes these binary files.

Binary Name	Source
CA ARCserve D2D Setup.exe	CA ARCserve D2D
ARCFlashVolDrvINSTALL.exe	CA ARCserve D2D
BaseLicInst.exe	CA License
UpdateData.exe	CA License
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft
tomcat6.exe	Tomcat
tomcat6w.exe	Tomcat

Binary Files that have a Privilege Level of Require Administrator in Manifest

CA ARCserve D2D installs binary files that are developed by third parties, other CA Technologies products, and CA ARCserve D2D that have a privilege level of Administrator or Highest Available. You must log in using an administrative account or an account with the highest available permissions to run various CA ARCserve D2D services, components, and applications. The binaries corresponding to these services, components, and applications contain CA ARCserve D2D specific functionality that is not available to a basic user account. As a result, Windows prompts you to confirm an operation by specifying your password or by using an account with administrative privileges to complete the operation.

- **Administrative Privileges** - The administrative profile or an account with administrative privileges has read, write, and execute permissions to all Windows and system resources. If you do not have Administrative privileges, you are prompted to enter user name / password of an administrator user to continue.

- **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 table describes these binary files.

Binaries	Source
afbkw.exe	CA ARCserve D2D
AFBackend.exe	CA ARCserve D2D
AgentDeployTool.exe	CA ARCserve D2D
Asremsvc.exe	CA ARCserve D2D
DeleteMe.exe	CA ARCserve D2D
MasterSetup.exe	CA ARCserve D2D
MasterSetup_Main.exe	CA ARCserve D2D
SetupFW.exe	CA ARCserve D2D
setup.exe	CA ARCserve D2D
silent.exe	CA License
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Driver Installation API for Non-WDM Driver

CA ARCserve D2D implements "SetupInstallServicesFromInfSection" API to install the non-WDM driver.

User Mode Driver Framework

CA ARCserve D2D uses the "WUDFRd.sys" driver, which is published by Microsoft and is part of UMDF (User Mode Driver Framework). This driver is not WHQL (Windows Hardware Quality Labs) signed.

Install CA ARCserve D2D

This section describes how to install CA ARCserve D2D on your local system using the InstallShield Wizard. The InstallShield Wizard is an interactive application that guides you through the installation process.

CA Support: How to: Install CA ARCserve D2D

YouTube: How to: Install CA ARCserve D2D

To install CA ARCserve D2D

1. Access the CA ARCserve D2D installation package from either the CA web site or the product CD. Select the CA ARCserve D2D Setup.exe if you are using installation package downloaded from the CA web site. Select setup.exe if you are using the product CD.

    Note: If the installation is performed using web downloaded installation package, the contents of the package are extracted to your local system.

    The License Agreement dialog opens.

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

    The Configuration dialog opens.

3. Enter the following information on the Configuration dialog:

    a. Username and password.

    b. Specify or browse to the location where CA ARCserve D2D is to be installed.

        The default location is: C:\Program Files\CA\ARCserve D2D.

        Note: During CA ARCserve D2D installation, some files will not be installed at the default location. For a complete listing of these files, see Files Installed Outside the Default Location (see page 346).

c. Port number. This port number is used to connect to the web-based UI.

The default port number is: 8014.

Note: The available port numbers for CA ARCserve D2D installation are between 1024 and 65535. You should ensure that the specified port number is free and available for use. Setup will not let you install CA ARCserve D2D for a port that is not available for use.

d. Specify if you want to use https for web communication.

By default, CA ARCserve D2D uses the Hypertext Transfer Protocol (HTTP) for communication among all of its components. If you are concerned about the security of information communicated between these components (including passwords), you can select this option to change the protocol being used to Hypertext Transfer Protocol Secure (HTTPS).

Note: You can change the communication protocol at any time after installation. For more information, see Change Server Communication Protocol (see page 296).

e. Specify if you want to install the CA ARCserve D2D change tracking driver.

By default, this option is selected.

■   Without this driver installed, CA ARCserve D2D cannot perform a local backup.

■   With this driver installed, you would still need to have a valid CA ARCserve D2D license to perform a local backup.

Note: You can install this driver at any time after the installation is complete by running the 'InstallDriver.bat' utility from the following location: "<ARCserve D2D install folder>\BIN\DRIVER"

f. Specify if you want to allow setup to register CA ARCserve D2D services and programs to Windows Firewall as exceptions.

Note: Firewall exceptions are required if you want to configure and manage CA ARCserve D2D from remote machines. (For local users, you do not need to register firewall exceptions).

4. Click Install to launch the installation process.

The Installation Progress screen is displayed indicating the status of the installation.

5. When the installation is complete, the Installation Report summary screen is displayed and automatically performs the product configuration. Click Finish.

An alert message is displayed, informing you that a system restart is required and asking if you want to reboot at this time or at a later time.

When the reboot is finished, CA ARCserve D2D is installed on your local system.

6. After installation, CA ARCserve D2D can be accessed from either the Start menu or from the CA ARCserve D2D Monitor.

7. After installation is complete, you may want to use the CA ARCserve D2D Boot Kit utility to create a BMR application USB stick if you are planning to use the created USB stick along with Windows 7/2008/2008 R2 installation media (CD/DVD) for BMR.

   When performing BMR, you will have a choice of using a Windows PE image (which is provided with the CA ARCserve D2D product) or the created USB stick along with the Windows 7/2008/2008 R2 installation media. The Boot Kit utility will also help you integrate BMR applications and third party NIC/SCSI/FC drivers to a USB stick.

   For more information about the Boot Kit utility, see Create a Boot Kit (see page 262).

Silent Install

Silent installation allows for unattended installation and does not prompt you for any input. Silent installations are used when performing similar installations on more than one computer.

The two methods for launching a CA ARCserve D2D silent installation include:

■ From the self-extracting executable file package that you installed when you downloaded CA ARCserve D2D.

■ From the CA ARCserve D2D CD (ISO) image which includes the CA ARCserve D2D setup and WinPE.

To launch the silent installation from the self-extracting executable, run the following command:

```
"CA ARCserve D2D Setup.exe" /s /a /i /AdminUser:<UserName>
/AdminPwd:<Password>
```

To launch the silent installation from the CD image, run the following command:

```
<CDROOT>\Install\MasterSetup.exe /i /AdminUser:<UserName>
/AdminPwd:<Password>
```

When configuring a silent installation, use the following syntax and arguments:

■ s - Specifies to run the executable file package using the silent mode.

■ a - Specifies any additional command line options.

■ i - Specifies to run the installation using the silent mode.

■ AdminUser - Specifies the user name.

   Note: User name must be an account that has administrative privileges.

■ AdminPwd - Specifies the corresponding password for the AdminUser.

For a silent installation, CA ARCserve D2D automatically uses all the default backup settings and the following configuration settings:

■ Install location: C:\Program Files\CA\ARCserve D2D

■ Port: 8014

Restart the target computer after the silent installation is finished.

Uninstall CA ARCserve D2D

CA ARCserve D2D can be uninstalled using the standard Add or Remove Programs application located in the Windows Control Panel.

The uninstallation routine removes all CA ARCserve D2D directories, files, and so on, from your computer, except for following directories and all of their contents:

■ **CA Licensing:**

– (x86 systems) C:\Program Files\CA\SharedComponents\CA_LIC

– (x64 systems) C:\Program Files(X86)\CA\SharedComponents\CA_LIC

Uninstall CA ARCserve D2D Using the Command Line

Windows Server 2008 Server Core is a minimal installation option for servers running Windows Server 2008. Windows Server Core contains minimal user interface functionality. The primary method of interacting with Server Core is through the command line.

Due to the lack of a user interface, situations can arise which require you to uninstall CA ARCserve D2D using the Windows command line.

The following procedure provides the steps necessary to uninstall CA ARCserve D2D from all Windows operating systems using the command line.

Follow these steps:

1. Log in to the computer where you want to uninstall CA ARCserve D2D.

   Note: Log in to the computer using an administrative account.

2. Open the Windows command line.

3. Execute the syntax that corresponds with the architecture of the computer's operating system.

   If a reboot is required after completion of the uninstall, you can specify if you want the computer to automatically reboot or to notify you that a reboot is required. You can then perform the reboot at a more convenient time:

   Note: A reboot is required If the CA ARCserve D2D driver is installed.

   ■ **Automatic Reboot**

   With this command, a reboot is performed automatically without any notification (if a reboot is required):

   – X86 operating system:

   MsiExec.exe /X{97270DB5-DB8F-467F-9C52-1AF57C55EA60} /qn

   – X64 operating system:

   MsiExec.exe /X{611E0884-4C83-4740-A3A9-9EB00D784E8D} /qn

   ■ **Manual Reboot (no notification)**

   With this command, check the return code to know if a manual reboot is required:

   Return Code:

       0 = Uninstall was successful

       3010 = Uninstall was successful, but a reboot is required

       Other = Uninstall failed

   – X86 operating system:

   MsiExec.exe /X{97270DB5-DB8F-467F-9C52-1AF57C55EA60} REBOOT=ReallySuppress /qn

   – X64 operating system:

   MsiExec.exe /X{611E0884-4C83-4740-A3A9-9EB00D784E8D} REBOOT=ReallySuppress /qn

   ■ **Manual Reboot (with notification)**

   With this command, a pop-up message displays notifying you if a manual reboot is required.

   – X86 operating system:

   MsiExec.exe /X{97270DB5-DB8F-467F-9C52-1AF57C55EA60}

   – X64 operating system:

   MsiExec.exe /X{611E0884-4C83-4740-A3A9-9EB00D784E8D}

4. After the command executes, CA ARCserve D2D is uninstalled.

Files Left Behind by the Uninstaller

Uninstallation of CA ARCserve D2D leaves behind some files such as the CA Licensing Components, Microsoft Visual C++ components installed as dependency, and driver related (wdf) files. The CA Licensing Components file is not automatically removed during uninstallation because it is a shared component with other CA products and numerous components.

If you want to manually remove these components, perform the following:

Remove CA Licensing Component manually

1. Go to " C:\Program Files (x86)\CA\SharedComponents\CA_LIC" directory.

2. Find the zip file named "lic98_uninstaller.zip" and unzip that file to some other location (for example: "C:\temp").

3. Go to the location where the files were extracted and locate two script files that are named "rmlic.exe" and "rmlicense.bat".

4. Click on "rmlicense.bat" to execute the script which uninstalls the components.

5. Manually delete the following folders

    ■   "C:\Program Files (x86)\CA "

    ■   "C:\Program Files\CA"

    ■   Folder where you extracted the zip file to.

Important! Because CA licensing is shared by all CA products, please make sure that you do not have any other CA product installed on your machine or else you may lose the licensing for all CA products installed on that machine.

Remove Microsoft Visual C++ manually

1. Access the standard Add or Remove Programs application located in the Windows Control Panel (Control Panel -> Programs and Features -> Remove Programs).

2. Select "Microsoft C++ 2005 Redistributable" and click on uninstall.

3. Select "Microsoft C++ 2005 Redistributable(x64)" and click on uninstall.

Important! Any programs that are installed after CA ARCserve D2D and depend on these removed components may not function properly.

For a complete listing of all files (path and name) that are left behind by CA ARCserve D2D uninstallation, see Files Not Removed During Uninstallation (see page 335).
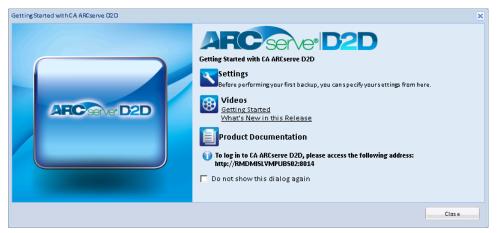
Chapter 3: Getting Started with CA ARCserve D2D

This section contains the following topics:

Getting Started

When you first access CA ARCserve D2D, the Getting Started dialog is displayed. From this dialog, you can access videos and the online help to learn more about CA ARCserve D2D. In addition, you can also access the various dialogs to specify such configuration settings as your backup source and destination, parameters, schedule, alert notifications, file copy settings, copy recovery point settings, preferences, and other related tasks. You can also select the option to not show this Getting Started dialog again.

CA ARCserve D2D User Interface

Before you use CA ARCserve D2D, become familiar with the related home page interface. The CA ARCserve D2D interface lets you perform the following tasks all from a single, easy-to-read home page:

- Manage backup servers and workstations.

- Monitor job performance.

- Obtain backup statistics.

- Initiate data protection tasks.

- Socialize with the user community.

- Get help.

The home page interface can be accessed from either the Start menu or from the CA ARCserve D2D Monitor.

| **CA Support:** | How to: Get Started with CA ARCserve D2D. |
| **YouTube:** | How to: Get Started with CA ARCserve D2D. |

The CA ARCserve D2D home page displays various icon symbols to provide a quick visual indication of the recent status and indicates the urgency of any actions you must take.

Successful
(No action is necessary)
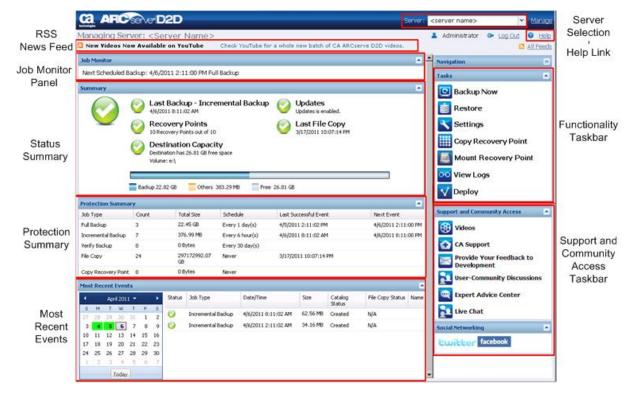
Caution
(Action may be necessary soon)

Warning
(Immediate action is necessary)

The CA ARCserve D2D home page consists of the following subsections:

- Server Selection List (see page 51)

- Job Monitor Panel (see page 52)

- Status Summary Overview (see page 54)

- Data Protection Summary (see page 57)

- Most Recent Events Summary (see page 58)

- Functionality Taskbar (see page 59)

- Support and Community Access Taskbar (see page 61)

- Help Menu Link (see page 63)

- RSS News Feeds (see page 63)

Server Selection List

From the home page, you can perform the following Server selection tasks:

- View the name of the CA ARCserve D2D server (or workstation) you are managing.

- Select a server to manage from the Server selection list.

The Server drop-down list lets you quickly and easily manage or view the status of these servers. After CA ARCserve D2D is installed on a server, you can then further deploy it to remote servers from the CA ARCserve D2D UI.

Servers are automatically added to the Server selection list when you successfully deploy CA ARCserve D2D to a remote server. In addition, you can also manually add/delete a server to/from the Server selection list using the Manage link on the home page. For more information, see Manage Server Selection List (see page 260).

Job Monitor Panel

When no jobs are currently running, the Job Monitor panel displays the date and time of the next scheduled event, with the type of event to be performed.

When a job is running, this panel expands to display information about the ongoing event such as the estimated time remaining to complete the job, the percentage and size of the job already completed, and the total size of the job when completed.

Note: When the Windows Performance Counter is disabled, the data speed of some CA ARCserve D2D jobs displayed in the job monitor may be 0 or some other abnormal value. If this occurs, see the troubleshooting section for more information.

When a job is running, you can click the Detail button to open the Backup Status Monitor and display more detailed information about the current job running. You can also click the Cancel button to stop the current job.

Note: If you want to stop the current job, click the Detail button first, to gain access to the Cancel button.

In addition to displaying more detailed information about the current job, the Backup Status Monitor also displays the throughput information for the job (actual Read and Write speed and the configured throttle speed limit).

■   If the Read/Write speed is too fast, you could enable the Throttle Backup option to adjust and limit the Write speed (and slow down the Read speed too). For more information about adjusting the Throttle Backup speed, see Specify the Protection Settings (see page 68).

   Note: Any changes made to the throttle settings does not take effect until you launch a new job.

■   If the Read/Write speed is too slow, there could be various reasons for this reduced speed such as antivirus software may be scanning the machine, or some file is being copied, or the machine is being accessed by many users.

   Note: Normally during a Verify backup job, the Read speed is much higher than Write Speed. This is because the block-by-block comparison effort (Read speed) of a Verify backup is the more active and continuous process, and because only the information that does not match the source is backed-up, the Write speed is minimized.

When a merge job is running, you can manually pause it from the CA ARCserve D2D home page Job Monitor.

If you manually pause a merge job, you must manually click resume for the merge job to continue. For more information, see Managing Merge Jobs (see page 136).

Status Summary Overview

The Status Summary section of the home page provides a quick and easy, high-level status of your backup health.

Last Backup

Displays the date and time of the last backup, with the status of that backup.

■ Green icon - Indicates that the last backup was successful and your computer is safely protected.

■ Red icon - Indicates that the last backup was not successful, your most recent backup failed, and the computer cannot be restored with that recovery point.

■ Yellow icon - Indicates that backups have not been performed for your computer and your computer is not protected.

Recovery Points/Recovery Sets

Displays the number of Recovery Points or Recovery Sets for your monitored server based on your specified retention settings.

■   Green icon - Indicates that you have reached the specified number of recovery points or recovery sets.

■   Red icon - Indicates that there are no saved recovery points or recovery sets and you have a potentially dangerous backup environment.

■   Yellow icon - Indicates that you have at least one recovery point or one recovery set, but have not reached your specified number of recovery points or recovery sets.

If you specified your retention settings based on recovery sets, the status summary overview displays the number of recovery sets already retained and the number of recovery sets in progress. In addition, click the link under Recovery Sets to display the Recovery Sets Details dialog. This dialog contains detailed information about the contents of the recovery set.

First Recovery Point	Last Recovery Point	Size	Recovery Point Count
8/26/2012 6:05:34 PM	Now	1.03 GB	1
8/24/2012 4:55:12 PM	8/24/2012 6:00:02 PM	1.03 GB	6

First Recovery Point

The date/time of the first backup in the recovery set.

Last Recovery Point

The date/time of the last backup in the recovery set. With the first/last recovery point time listed, you are able to determine the complete time range of the recovery set.

Size

The total size of the recovery set. This number can be used to calculate how much disk space is used by the recovery set.

Recovery Point Count

The number of recovery points that belong to the recovery set.

Destination Capacity

Displays the amount of free space available at your backup destination. The Destination Capacity display provides an additional indication of the amount of space that is used for the backups, the amount of space that others use, and the amount of available free space.

■ Green icon - Indicates that the amount of available free space is above the safe level.

■ Red icon - Indicates either of the following conditions:

  – The specified destination is not accessible.

  – The amount of available free space is reduced to below the predetermined safe percentage of your destination capacity. For example, if it is determined that the available free space cannot accommodate five more incremental backups the icon turns red.

    Immediately increase the free space capacity of the backup destination or change the destination to another location which has adequate space.

Note: You can set up an email alert notification when the amount of unused space at the backup destination is less than a specified value. For more information about setting up this email alert notification, see Specify Email Alert Preferences (see page 116).

Updates

Displays the status of CA ARCserve D2D updates for your computer.

■ Green icon - Indicates the CA ARCserve D2D Updates function is enabled. Your computer is able to connect to the download server, your Update Schedule is configured, and no new updates are available.

■ Yellow icon - Indicates either of the following conditions:

  – The latest available update is not installed on your computer.

    You can then click "Click here to install updates" to trigger the installation of the update.

  – Your Update Schedule has not been configured.

    For more information about configuring the Update Schedule, see Specify Updates Preferences (see page 122).

Note: All updates that are released for CA ARCserve D2D are cumulative. As a result, each update also includes all previously released updates to help ensure that your computer is always up-to-date.

■ Red icon - Indicates CA ARCserve D2D is not able to connect to the download server. When this red icon is displayed, it means that you must provide valid download server details on the Updates (see page 122) tab of the Preferences dialog.

Last File Copy

Displays the date and time of the last File Copy job, with the status of the File Copy job that was performed.

- ■ Green icon - Indicates that the last File Copy job was successful.

- ■ Red icon - Indicates that the last File Copy job was not successful.

- ■ Yellow icon - Indicates that the last File Copy job was incomplete or canceled.

In addition, the Last File Copy status indicator also displays the actual amount of space that is freed on the disk by the File Copy job. This space saved calculation is only displayed if you select to move the File Copy to a different location instead of copying the File Copy to as different location. This value is based upon the actual size of the backup that was <u>moved</u> from the computer to the specified destination. A File Copy job that does not move the copy to a different location, does not save any space.

License Failure

If a backup fails because of a license validation failure, the License Failure status is displayed indicating which license was the cause of the failure.

Data Protection Summary

The Data Protection Summary section of the home page displays status information for the available events (backups/file copy).

Protection Summary					▲
Job Type	Count	Total Size	Schedule	Last Successful Event	Next Event
Full Backup	3	22.45 GB	Every 1 day(s)	4/5/2011 2:11:02 PM	4/6/2011 2:11:00
Incremental Backup	9	422.29 MB	Every 6 hour(s)	4/6/2011 10:22:42 AM	4/6/2011 2:11:00
Verify Backup	0	0 Bytes	Every 30 day(s)		
File Copy	24	17.07 GB	Never	3/17/2011 10:07:14 PM	
Copy Recovery Point	0	0 Bytes	Never		

For each type of backup job (Full, Incremental, and Verify) and each File Copy job, this summary displays the following:

Count

For each type of event, indicates the number of successful backup/File Copy jobs that were performed (scheduled or non-scheduled).

Total Size

For each type of event, indicates the total size of the backed up/file copied data.

Schedule

For each type of job, indicates the configured schedule for automatic backup/File Copy jobs

Last Successful Event

For each type of event, indicates the date and time that the last successful event was performed.

Next Event

For each type of event, indicates the next scheduled event. If this column is blank, it indicates that you do not have a schedule for this type of event or the non-recurring schedule has been satisfied.

Most Recent Events Summary

The Most Recent Events section of the home page displays the most recent events (backup jobs), with the corresponding status, the type of event performed, the date and time of the event, the size of the data backed up, and the status of the catalog creation and corresponding File Copy job. It also includes the name of the event (if specified by the user). You can click on a specific date to display the corresponding events for that selected date.

A flag in the status column indicates that a full backup is the starting backup of a recovery set.

Note: The size field displays the backup size when the backup job is finished and then adds the catalog size to the same field when the catalog job is finished.

The calendar displays the dates of the most recent events, highlighted in corresponding status colors.

- Green - All backup attempts for that day were successful.

- Red - All backup attempts for that day were unsuccessful (failed or canceled).

- Yellow - Backup attempts for that day were not all successful or not all unsuccessful (mix of successful and unsuccessful backup attempts).

    Note: A diagonal marker in the top left corner of a date indicates that the day contains the start of a recovery set.

Functionality Taskbar

The Functionality taskbar section of the home page provides a means to initiate the various CA ARCserve D2D functions.

Backup Now

Lets you run a Full, Incremental, or Verify ad-hoc backup immediately, based on current backup settings. The backup settings are configured and defined through the Backup Settings. For more information, see Run Backup Now (see page 140).

Restore

Lets you perform a file level or application-level restores to the original location or to an alternate location. When you select this function, you then specify to which restore option you want to use to locate the backup image to be restored. For more information, see Restore Methods (see page 144).

Settings

Lets you configure/modify the following settings:

– Backup Settings (backup destination, schedule, retention count, and so on). For more information, see Manage Backup Settings (see page 67).

– File Copy (source, destination, schedule, retention count, filters, and so on). For more information, see Manage File Copy Settings (see page 89).

– Copy-Recovery Points (scheduled export of recovery points). For more information, see Specify Copy - Recovery Points Settings.

– Preferences (enable RSS news feeds and social networking, Email Alerts, and Updates). For more information, see Specify Preferences (see page 114).

Copy Recovery Point

Lets you view a list of available recovery points (successful backups) and select which recovery point you want to use to create a consolidated copy. This consolidated copy combines the blocks from the previous full and all incremental backups leading to the selected recovery point. In addition, the consolidated copy also removes any unused blocks (reducing the image size) to lets you gain more efficient use of your backup resources.

Each recovery point represents a point in time when a VSS snapshot image was captured and contains not only the data, but also all information relating to the operating system, installed applications, configuration settings, necessary drivers, and so on. For more information, see Copy Recovery Points.

View Logs
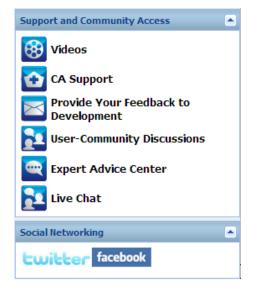
Lets you view logs of activities that are performed during operations such as backup, restore, and copy. The Activity Log displays the status of the job, including such details as the throughput, compression size, elapsed time, encryption status, and so on. For more information, see View Logs (see page 258).

Deploy

Lets you deploy CA ARCserve D2D to remote computers. For more information, see Deploy CA ARCserve D2D Remotely (see page 254).

Support and Community Access Taskbar

The Support and Community Access taskbar section of the home page provides a means to initiate the various support-related functions.

To avoid any delays in response and help ensure that your communication is routed to the proper destination, it is important to know and understand which of these sites are used for which functions.

For example:

- If you discover a bug in the product, you should select the **CA Support** link and post the problem there. By doing this, the CA Support team can directly assist you in resolving your problem in a productive and efficient manner.

- If you are seeking any product-related advice, such as the best settings to protect your environment, you should select the **User-Community Discussions** link and post the question on the CA ARCserve D2D Google Group to see if the experts in the community can provide a good answer. By doing this, you can interact with other users in similar working environments and establish an open communication for sharing ideas and advice.

- If you have a suggestion or idea for improving the product for the next release, you should select the **Provide Your Feedback to Development** link and post your idea on the Get Satisfaction site. By doing this, you can interact directly with the CA Technologies development team to work together to improve the product and help make it better for you.

- If you just want to get the latest news and information about the CA ARCserve D2D product from the CA Technologies product management team, you should select the **Expert Advice Center** link.

Videos

Provides access to view various CA ARCserve D2D-related videos. These videos are for basic CA ARCserve D2D features and procedures. You can specify the default preference for accessing and viewing these videos from either YouTube or CA Support. For more information about setting your default viewing preference, see Specify General Preferences (see page 114).

CA Support

Provides access to "One Stop Support" from where you can resolve issues and get important product information.

Provide Your Feedback to Development

Provides access to the CA ARCserve D2D Development team (using the Get Satisfaction website) from where you can view Frequently Asked Questions, ask your own questions, share ideas, and report any problems.

Note: Available in English only.

User-Community Discussions

Provides access to interact with the CA ARCserve D2D online community and be part of the CA ARCserve D2D User Group. This group allows you to share your CA ARCserve D2D experiences with other users.

Note: Available in English only.

Expert Advice Center

Provides access to the ARCserve Expert Advice Center which is a convenient landing page from where you can then access Tips and Tricks from the CA ARCserve D2D Development team (blogs), product information, group discussions, official CA Support, and other valuable CA ARCserve D2D-related information.

Live Chat

Provides real-time monitoring and live help/support. Lets you optimize intelligent conversation between you and the CA ARCserve D2D Technical Support team, allowing you to address your concerns and questions immediately, while still maintaining access to the product. Upon completion of the chat session, you can send a transcript of the chat to your email address.

Note: You may need to add the Live Chat link to your Trusted sites.

Social Networking

Provides access to Twitter and Facebook for CA ARCserve D2D-related social networking.

If you do not want to display these social network links on the home page, you can specify this preference. For more information about setting your social network display preference, see Specify General Preferences (see page 114).

Help Menu

The Help menu on the home page provides a quick and easy access to the CA ARCserve D2D Help, User Guide, and the About CA ARCserve D2D page. In addition, you can launch a manual Check for Updates from this menu.

All Feeds

CA ARCserve D2D provides an All Feeds link to let you easily subscribe to RSS feeds from related web sites. Really Simple Syndication (RSS) feeds allow you to stay informed by having relevant and up-to-date information sent to you straight from the web sites that you are interested in. With RSS feeds, you do not need to keep checking back to a particular website to see if it has been updated. All you need to do is subscribe to the RSS feed, much like you would subscribe to a magazine, but instead of it being delivered to your physical mailbox each time the magazine is published, the information is delivered to you (using an RSS feed) every time your subscribed website is updated.

To subscribe and read RSS feeds you need an RSS feed reader. There are many different programs to view RSS feeds from such as Outlook, your internet browser (Internet Explorer, Firefox), web-based readers (My Yahoo, Google Reader), and desktop-based readers (Feed Demon). After you have subscribed to a feed, the RSS feed reader is able to check for new content at specified time intervals and retrieve the updates.

When you click the All Feeds link, the All Feeds dialog opens to let you subscribe to the various CA ARCserve D2D related RSS feeds.

Unsuccessful Jobs Feed

When you subscribe to this RSS feed, you receive an update notification each time an unsuccessful backup, restore, or copy job is performed on your machine. An unsuccessful job includes all failed, incomplete, canceled, and crashed attempts.

Video

When you subscribe to this RSS feed, you receive a notification each time the CA ARCserve D2D videos are updated. This RSS feed is only applicable for the YouTube version of the videos.

Provide Your Feedback to Development

When you subscribe to this RSS feed, you receive a notification each time the Get Satisfaction website information is updated. This site provides access to the CA ARCserve D2D Development team where you can view Frequently Asked Questions, ask your own questions, share ideas, and report any problems.

User-Community Discussions
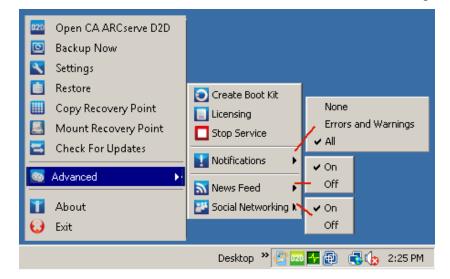
When you subscribe to this RSS feed, you receive a notification each time the CA ARCserve D2D online community website information (Google Group) is updated. This site provides access to interact with the CA ARCserve D2D online community and allows you to share your CA ARCserve D2D experiences with other users.

Expert Advice Center
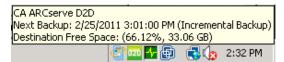
When you subscribe to this RSS feed, you receive a notification each time the ARCserve Expert Advice Center website information is updated. This site provides a convenient landing page where you can then access Tips and Tricks from the CA ARCserve D2D Development team (blogs), product information, group discussions, official CA Support, and other valuable CA ARCserve D2D-related information.

CA ARCserve D2D Monitor

From the CA ARCserve D2D Monitor, you can access many of the same task functions that you can access from the CA ARCserve D2D home page. You can launch the following tasks from the tray monitor: Open the CA ARCserve D2D home page, Backup Now, Settings, Restore, Copy Recovery Point, Mount Recovery Point, Check for Updates, and Advanced. From the Advanced option, you can access additional subordinate options such as Create Boot Kit, Licensing, Start/Stop Service, configure alert Notifications, turn on/off the News Feed, and turn on/off Social Networking.

In addition, when you hover your cursor over the CA ARCserve D2D Monitor icon, a backup status overview message is displayed. An animated icon indicates when any job is running and includes the progress completed. You can easily determine if a job (backup, restore, file copy, copy recovery point, catalog, or granular restore catalog) is running without logging in to CA ARCserve D2D.

Chapter 4: Settings

This section contains the following topics:

Manage Backup Settings

Before you perform your first backup, specify the backup settings which are applied to each backup job. These settings let you specify behaviors such as:

- Backup source and destination

- Schedule for each type of backup

- Advanced settings for your backup jobs

- Any pre or post backup operations.

These settings can be modified at any time from the CA ARCserve D2D home page.

Videos

CA Support: How to: Perform an Automatic Backup – Configuring Your Backup Settings.

YouTube: How to: Perform an Automatic Backup – Configuring Your Backup Settings.

To manage the backup settings, click the Settings link on the CA ARCserve D2D home page to display the Backup Settings dialogs and these subordinate tab options:

- Protection Settings (see page 68)

- Schedule Settings (see page 82)

- Advanced Settings (see page 84)

- Pre/Post Backup Settings (see page 88)

Specify the Protection Settings

Protection settings for the information going to be backed up ensures that the backup data is reliably protected (copied and saved) against any form of data loss.

Note: To view a video that is related to these Backup Settings, see Manage Backup Settings (see page 67).

Specify the protection settings

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the Backup Settings tab. When the Backup Settings dialog opens, select Protection.

   The Backup Settings Protection dialog opens.

2. Specify the **Backup Destination**.

   You can specify a local path (volume or folder), or remote shared folder (or mapped drive) for the backup location, or you can browse to a backup location.

   Click the green arrow icon button to verify the connection to the specified location.

   – If you entered a local path for the destination, this button is disabled.

   – If you enter a network path and click this button, you are prompted to provide the username and password.

   – If you are already connected to this path successfully, and click the arrow button you can change the username and password you used to connect.

   – If you do not click the arrow button, the destination path is verified. If needed, you are prompted for the username and password.

   a. If you want to back up to your local path (volume or folder), the specified backup destination cannot be the same location as your backup source. If you inadvertently include the source in your destination, the backup job ignores this portion of the source and it is not included in the backup.

      Example: You attempt to back up your entire local machine consisting of Volumes C, D, and E and also specify Volume E as your destination. CA ARCserve D2D only backs up Volumes C and D to Volume E. Data from Volume E is not included in the backup. If you want to back up all local volumes, specify a remote location for your destination.

      Important! Verify that your specified destination volume does not contain system information. Or else it will not be protected (backed up) and your system will fail to recover after Bare Metal Recovery (BMR) if necessary.

      Note: Dynamic disks are restored at disk-level only. If your data is backed up to a volume on a dynamic disk, you are not able to restore this dynamic disk during BMR.

   b. If you want to back up to a remote shared location, specify a location path or browse to the location. You also have to provide user credentials (Username and Password) to access the remote machine.

   c. If the backup destination has changed after the last backup was performed, select the backup type: Full Backup or Incremental Backup. These options are only enabled when you change your backup destination. The default option is Full Backup.

      Full Backup

         The next backup that is performed is going to be a Full Backup. The new backup destination does not have any dependency on the old backup destination. If you continue with a full backup, the previous location is no longer needed for backups to continue. You can select to keep the old backup for any restores or if you do not want to perform any restores from there you can delete it. The old backup will not affect future backups.

Incremental Backup

The next backup that is performed is going to be an Incremental Backup. The next incremental backup to the new destination is performed without copying all the backups from the previous destination. However, for this option, the new location is dependent on the previous location because the changes include only the incremental data (not the full backup data). Do not delete the data from the previous location. If you change the backup destination to another folder and attempt to perform an incremental backup, and the former backup destination does not exist, the backup fails.

3. Specify the **Backup Source**.

You can back up the entire machine or selected volumes.

Back up the entire machine

Lets you back up the entire machine. All volumes on the machine are backed up.

Note: If you select the full machine backup option, CA ARCserve D2D automatically discovers all disks/volumes attached to the current machine and CA ARCserve D2D includes them in the backup.

Example: If a new disk is attached to the machine after the backup setting is configured, you do not need to change the backup settings and the data on the new disk will be protected automatically.

Select individual volumes to back up

This volume filtering capability lets you specify to back up only the selected volumes. You also have the option to Select/Unselect all listed volumes.

Note: If some volumes are selected explicitly for backup, only the selected volumes are backed up. If a new disk/volume is attached to the machine, manually change the volume selection list to protect the data on the new disk/volume.

When you select this option, a listing of all available volumes display, with the corresponding volume information and notification messages.

Note: Computers that adhere to the Extensible Firmware Interface (EFI) use the EFI System Partition, which is a partition on a data storage device. The EFI System partition is critical for Bare Metal Recovery (BMR). Therefore, when you select boot volume "C" on a UEFI system, the EFI System Partition is selected automatically for the backup source for BMR and an information message is displayed.

Name	Layout	Type	File System	Contents	Total Size	Used Space	
■▭ E:	Simple	Basic	NTFS		92.79 GB	32.68 GB	▲
☐▤ F:	Simple	Basic	NTFS		596.17 GB	108.02 GB	
☐ System Reserved	Simple	Basic	NTFS	System	100.00 MB	28.19 MB	▼

Selected Volume Size: 88.58 GB

▲ **Notifications (2 warnings)**

⚠ Local backup destination volume F: will be excluded from backup source selection.

⚠ If System Volume(Usually System Reserved drive) is not in the backup source volume list, the backup cannot be used for BMR.

- **Name** – volume drive letter, mount point, volume GUID (Globally Unique Identifier) name.

- **Layout** – simple, spanned, mirror, stripped, RAID5 (backup of a RAID 5 volume on Microsoft Dynamic Disks is not supported; but backup of hardware RAID is supported).

- **Type** – basic, dynamic

- **File system** – NTFS, FAT, FAT32 (backup of FAT and FAT32 is not supported).

- **Contents** – Application (SQL/Exchange), System, Boot, Page file, Active, Removable Device, VHD, 2-TB Disk

- **Total size** – capacity of the volume

- **Used Space** – space files/folders and volume data occupies.

The notification messages display for any of the following conditions:

- **Local volume related**

  If the specified backup destination is on the local volume, a warning message displays notifying you that this volume is not backed up.

- **BMR related**

  If system/boot volume is not selected for backup, a warning message displays notifying you that the backup is not usable for BMR.

  If you select boot volume "C" on a UEFI system, the EFI System Partition is selected automatically for the backup source for BMR and an information message is displayed.

- **Application related**

  If the application data files are on a volume that is not selected for backup, the application name and database name display for reference.

4. Specify the **Retention Setting**.

   You can set the retention setting based on the number of recovery points to retain (merges sessions) or based on the number of recovery sets to retain (deletes recovery sets and disables infinite incremental backups).

   - Recovery Point – This is the recommended option. With this option selected, you can fully leverage the infinite incremental backup capabilities and save storage space.

   - Recovery Set – This option is generally used for large storage environments. With this option selected, you can create and manage backup sets that help you manage your backup window time more efficiently when you are protecting a large amount of data. You can use this option when backup time is a priority over space constraints.

   Default: Retain Recovery Points

   For more information about setting the Recovery Point and Recovery Set options, see Specify Retention Settings (see page 75).

5. Specify the type of **Compression**.

   Specifies the type of compression that is used for backups.

   Compression is often selected to decrease disk space usage, but also has an inverse impact on your backup speed due to the increased CPU usage.

The available options are:

■ **No Compression**

No compression is performed. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

■ **Standard Compression**

Some compression is performed. This option provides a good balance between CPU usage and disk space usage. Standard compression is the default setting.

■ **Maximum Compression**

Maximum compression is performed. This option provides the highest CPU usage (lowest speed), but also has the lowest disk space usage for your backup image.

Notes:

■ If your backup image contains uncompressible data (such as JPG images or ZIP files), you can allocate additional storage space to handle such data. As a result, if you select any compression option and you have uncompressible data in your backup, it can result in an increase in disk space usage.

■ If you change the compression level from No Compression to either Standard Compression or Maximum Compression, or if you change from either Standard Compression or Maximum Compression to No Compression, the first backup that is performed after this compression level change is automatically a Full Backup. After the Full Backup is performed, all future backups (Full, Incremental, or Verify) will be performed as scheduled.

■ If your destination does not have sufficient free space, you can consider increasing the Compression setting of the backup.

6. Specify the **Encryption** settings.

   a. Select the type of encryption algorithm that is used for backups.

   Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. CA ARCserve D2D data protection uses secure, AES (Advanced Encryption Standard) encryption algorithms to achieve maximum security and privacy of your specified data.

   The available format options are No Encryption, AES-128, AES-192, and AES-256. (To disable encryption, select No Encryption).

   ■ A full backup and all its related incremental and verify backups must use the same encryption algorithm.

   ■ If the encryption algorithm for an incremental or verify backup is changed, a full backup must be performed. This means after changing encryption algorithm, the first backup will be full, despite the original backup type.

   For example, if you change the algorithm format and you submit a customized incremental or verify backup manually, it is automatically converted to a full backup.

b. When an encryption algorithm is selected, provide (and confirm) an encryption password.

  ■ The encryption password is limited to a maximum of 23 characters.

  ■ A full backup and all its related incremental and verify backups must use the same password to encrypt data.

  ■ If the encryption password for an incremental or verify backup is changed, a full backup must be performed. This means after changing encryption password, the first backup will be full, despite the original backup type.

    For example, if you change the encryption password and you submit a customized incremental or verify backup manually, it is automatically converted to a full backup.

c. CA ARCserve D2D provides encryption password management so that you do not need to remember encryption passwords.

  ■ Password is also encrypted.

  ■ Password is remembered and not required (if you restore to the same machine).

  ■ Password is required if you restore to a different machine.

  ■ Password is not required if you are attempting to export a recovery point that contains encrypted data and the recovery point belongs to backups performed on the current machine.

  ■ Password is always required if you are attempting to recover encrypted data from an exported recovery point.

  ■ Password is not required to browse to an encrypted recovery point.

  ■ Password is required to perform a BMR.

d. When encryption is enabled, the activity log is updated.

  ■ A message is recorded in the activity log to describe the selected encryption algorithm for every backup.

  ■ A message is recorded in the activity log to indicate why an incremental or verify backup was converted to a full backup (password change or algorithm change).

Note: Encryption settings do not have to remain the same for your backups. You can change these settings at any time, including after several backups of the same data.

7. Specify the **Throttle Backup**.

You can specify the maximum speed (MB/min) at which backups are written. You can throttle the backup speed to reduce CPU or network use. However, limiting the backup speed, has an adverse effect on the backup window. As you lower the maximum backup speed, it increases the amount of time of perform the backup. For a backup job, the Job Monitor on the CA ARCserve D2D home page displays the average Read and Write speed of the job in progress and the configured throttle speed limit.

Note: By default, the Throttle Backup option is not enabled and backup speed is not being controlled.

8. Calculate the **Estimated Backup Size**.

Displays the estimated usage of the destination volume.

For more information about using these estimated backup calculations, see Estimate Future Backup Space Requirements (see page 80).

9. Click Save Settings.

Your backup protection settings are saved.

Specify Retention Settings

Retain Recovery Points

Select this option to set your retention setting based on the number of recovery points to retain instead of on the number of recovery sets to retain.

Specify the number of recovery points to retain

Specifies the number of recovery points (full, incremental, and verify backup images) retained. When the number of recovery points present on the destination exceeds the specified limit, the earliest (oldest) incremental backups beyond the retention count are merged into the parent backup to generate a new baseline image consisting of the "parent plus oldest childs" blocks. If there are multiple sessions available for merge, the oldest child backups will be merged into the parent backup in a single pass, if the backups are compressed. If the backups are not compressed, then only the oldest child backup will be merged into the parent backup and this cycle repeats for each subsequent child backup to be merged.

Specifying the number of recovery points to retain allows you to perform infinite incremental backups, while maintaining the same retention count. For more information, see Merge Job Guidelines.

Note: If your destination does not have sufficient free space, you can consider reducing the number of saved recovery points.

Default: 31

Minimum: 1

Maximum: 1344

Note: The CA ARCserve D2D home page Summary section indicates how many recovery points are retained out of the number specified. For more information, see Status Summary Overview (see page 54) in the online help.

Run the merge job:

As soon as possible

Select this option to run the merge job at any time.

Each day during the following time range

Select this option to run the merge job each day only within the specified time range. Setting a time range helps to avoid the merge job introducing too many I/O operations to the production server if the merge job runs for a long time.

Note: When setting the time range to run the merge job, ensure that you specify a time range that will allow the related backup jobs to complete prior to the start of the merge.

Retain Recovery Sets

> Select this option to set your retention setting based on the number of recovery sets to retain instead of on the number of recovery points to retain. With this setting you can disable infinite incremental backups, without merging any sessions. Using recovery sets helps reduce the amount of time it takes to complete merge jobs.

Specify the number of recovery sets to retain

> Specifies the number of recovery sets retained. A recovery set is a series of backups, starting with a full backup, and then followed by a number of incremental, verify, or full backups.

> **Example Set 1:**
>
> ■ Full
>
> ■ Incremental
>
> ■ Incremental
>
> ■ Verify
>
> ■ Incremental

Example Set 2:

- Full

- Incremental

- Full

- Incremental

A full backup is required to start a new recovery set. The backup that starts the set will be automatically converted to a full backup, even if there is no full backup configured or scheduled to be performed at that time. A flag in the status column on the CA ARCserve D2D home page Most Recent Events section indicates that a full backup is the starting backup of a recovery set. After the recovery set setting is changed (for example, changing the recovery set starting point from the first backup of Monday to the first backup of Thursday), the starting point of existing recovery sets will not be changed.

Note: An incomplete recovery set is not counted when calculating an existing recovery set. A recovery set is considered complete only when the starting backup of the next recovery set is created.

When the specified limit is exceeded, the oldest recovery set is deleted (instead of merged).

Default: 2

Minimum: 1

Maximum: 100

Note: If you want to delete a recovery set to save backup storage space, reduce the number of retained sets and CA ARCserve D2D automatically deletes the oldest recovery set. Do not attempt to delete the recovery set manually.

Example 1 - Retain 1 Recovery Set:

- Specify the number of recovery sets to retain as 1.

CA ARCserve D2D always keeps two sets in order to keep one complete set before starting the next recovery set.

Example 2 - Retain 2 Recovery Sets:

- Specify the number of recovery sets to retain as 2.

CA ARCserve D2D will delete the first recovery set when the fourth recovery set is about to start. This ensures that when the first backup is deleted and the fourth is starting, you still have two recovery sets (recovery set 2 and recovery set 3) available on disk.

Note: Even if you choose to retain only one recovery set, you will need space for at least two full backups.

Example 3 - Retain 3 Recovery Sets:

■ The backup start time is 6:00 AM, August 20, 2012.

■ An incremental backup runs every 12 hours.

■ A new recovery set starts at the last backup on Friday.

■ You want to retain 3 recovery sets.

With the above configuration, an incremental backup will run at 6:00 AM and 6:00 PM every day. The first recovery set is created when the first backup (must be a full backup) is taken. Then the first full backup is marked as the starting backup of the recovery set. When the backup scheduled at 6:00 PM on Friday is run, it will be converted to a full backup and marked as the starting backup of the recovery set.

Start a new recovery set on every:

Selected day of the week

Specifies the day of the week selected to start a new recovery set.

Selected day of the month

Specifies the day of the month selected to start a new recovery set. Specify 1 through 30. Or, since a given month may have 28, 29, 30, or 31 days, you can specify the last day of the month as the day to create the recovery set.

Start a new recovery set with:

First backup on the selected day

Indicates you want to start a new recovery set with the first scheduled backup on the specified day.

Last backup on the selected day

Indicates you want to start a new recovery set with the last scheduled backup on the specified day. If the last backup is selected to start the set and for any reason the last backup did not run, then the next scheduled backup will start the set by converting it to a full backup. If the next backup is run ad-hoc (for example an emergency situation requires a quick incremental backup), you can decide if you want to run a full backup to start the recovery set or run an incremental backup so that the next backup starts the recovery set.

Note: The last backup may not be the last backup of the day if you run an ad-hoc backup.

The CA ARCserve D2D home page Summary section indicates how many recovery sets are retained (or in progress) out of the number specified. Click the link under Recovery Sets to display the Recovery Sets Details dialog. This dialog contains detailed information about the contents of the recovery set. For more information about this dialog, see <u>Status Summary Overview</u> (see page 54) in the online help.

Estimate Future Backup Space Requirements

CA ARCserve D2D provides you with this tool to calculate the estimated amount of available free space that you will need for backups. The calculations are based on your estimate of future data change and on the space that is occupied from previous backups.

To use this estimating tool

1. Select the backup source. This can be your entire machine or selected volumes within your machine.

   The actual size of the selected backup source is displayed in the Total Source Size field.

2. Estimate the anticipated Change Rate for future backups.

   Base this estimate upon past performance of how much your total backup size has changed for each subsequent incremental backup.

   With the Estimated Values defined, CA ARCserve D2D calculates and displays the estimated backup size required based on the configuration of the backup destination and the recovery points. The pie chart also displays the amount of used space and free space.

3. Estimate the Space Saved After Compression percentage value.

Estimated Values

You can use estimated values to calculate the approximate overall backup size that is based on the number of recovery points. Base this estimate upon past performance of your backups with different Compression settings applied. As you change this value, you will see the corresponding size impact for your backup sizes.

Note: If necessary, you can perform some Full Backups, each with a different Compression setting (No Compression, Standard Compression, and Maximum Compression) to establish past performance values and help you to better calculate the percent of space saving that each setting produces for your backup.

■ **Space Saved After Compression**

This value indicates how much disk space is saved after compression.

Example: If the data size of a volume is 1000 MB and after backup the compressed data size is 800 MB, then the Space Saved After Compression is estimated to be 200 MB (20%).

■ **Change Rate**

This value indicates the typical data size of an incremental backup.

Example: If an incremental backup data size is 100 MB and the full backup data size is 1000 MB, the change rate is estimated to be 10%.

Estimated Backup Size

Displays the estimated values for Total Source Size, Compressed Full Backup Size, Compressed Incremental Backup Size, and Estimated Total Backup Size.

■ The Compressed Full Backup Size field displays a calculated value that is based upon:

– Size of the backup source

– Specified compression percentage.

■ The Compressed Incremental Backup Size field displays a calculated value that is based upon:

– Estimated Change Rate

– Number of recovery points to be saved

– Specified compression percentage

■ The Estimated Total Backup Size field will display the anticipated space that you will need for future backups and is based upon:

– Amount of space that is required for one Full Backup plus

– Amount of space that is required for the number of Incremental Backups needed to satisfy the specified number of saved recovery points.

4. From this Estimated Total Backup Size value, you should be able to determine if your backup destination has sufficient space to fit your backup.

   If your destination does not have sufficient free space, you can consider the following corrective actions:

   ■ Reduce the number of saved recovery points.

   ■ Increase the available free space at the backup destination.

   ■ Change the backup destination to a larger capacity.

   ■ Reduce the size of the backup source (maybe eliminate unnecessary volumes from the backup).

   ■ Increase the Compression setting of the backup.

Specify the Backup Schedule

CA ARCserve D2D lets you specify the schedule for your backups.

Note: To view a video related to these Backup Settings, see Manage Backup Settings (see page 67).

Specify the backup schedule

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the Backup Settings tab. When the Backup Settings dialog opens, select Schedule.

   The Backup Settings Schedule dialog opens.

2. Specify your backup schedule options.

Set start date and time

> The start date and start time for your scheduled backups.
>
> **Note:** When setting the interval between repeat backup jobs, ensure that you leave enough time to allow the previous job and any related merge jobs to complete before the next backup job starts. This amount of time can be estimated based on your own specific backup environment and history.

Incremental Backup

> Determines the backup schedule for Incremental Backups.
>
> As scheduled, CA ARCserve D2D incrementally backs up only those blocks that have changed since the last successful backup. The advantages of Incremental Backups are that it is a fast backup and it produces a small backup image. This is the most optimal way to perform backups and you should use this by default.
>
> The available options are Repeat and Never. If you select the Repeat option, you must also specify the elapsed time period (in minutes, hours, or days) between backup attempts. The minimum setting for Incremental backups is every 15 minutes.
>
> By default the schedule for Incremental backups is to repeat every 1 day.

Full Backup

> Determines the backup schedule for Full Backups.
>
> As scheduled, CA ARCserve D2D performs a Full backup of all used blocks from the source machine. The available options are Repeat and Never. If you select the Repeat option, you must also specify the elapsed time period (in minutes, hours, or days) between backup attempts. The minimum setting for Full backups is every 15 minutes.
>
> By default the schedule for Full backups is Never (no scheduled repeat).

Verify Backup

> Determines the backup schedule for Verify Backups.
>
> As scheduled, CA ARCserve D2D verifies that the protected data is valid and complete by performing a confidence check of the stored backup image to the original backup source. If necessary, the image is resynchronized. A Verify Backup looks at the most recent backup of each individual block and compares the content and information to the source. This comparison verifies that the latest backed up blocks represent the corresponding information at the source. If the backup image for any block does not match the source (possibly because of changes in the system since the last backup), CA ARCserve D2D refreshes (resynchronizes) the backup of the block that does not match. You can also use a Verify Backup (very infrequently) to get the guarantee of full backup without using the space required for a full backup.

Advantages: Produces a small backup image when compared to full backup because only the changed blocks (blocks that do not match the last backup) are backed up.

Disadvantages: Backup time is long because all source blocks are compared with the blocks of the last backup.

The available options are Repeat and Never. If you select the Repeat option, you must also specify the elapsed time period (in minutes, hours, or days) between backup attempts. The minimum setting for Verify backups is every 15 minutes.

By default the schedule for Verify backups is Never (no scheduled repeat).

3. Click Save Settings.

   Your backup schedule settings are saved.

Note: If at a given time there are more than one type of backup scheduled to be performed simultaneously, the type of backup that will be performed is based upon the following priorities:

■ Priority 1 - Full backup

■ Priority 2 - Verify backup

■ Priority 3 - Incremental backup

■ For example, if you schedule all three types of backups to be performed at the same time, CA ARCserve D2D will perform the Full Backup. If there is no Full Backup scheduled, but you scheduled a Verify Backup and Incremental Backup to be performed at the same time, CA ARCserve D2D will perform the Verify Backup. A scheduled Incremental Backup is performed only if there is no conflict with any other type of backup.

Specify the Advanced Backup Settings

CA ARCserve D2D lets you specify the Advanced Settings for your backups.

Note: To view a video that is related to these Backup Settings, see Manage Backup Settings .

Follow these steps:

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the Backup Settings tab. When the Backup Settings dialog opens, select Advanced.

   The Advanced dialog opens.

2. Specify your advanced backup settings options.

   Truncate Log

   Truncates the accumulated transaction log files for the selected applications after the next successful backup.

   CA ARCserve D2D backups consist of a snapshot image and the transaction log files that were created for it. At some point in time, the older (committed) transaction log files are no longer needed and can be purged to make space for new log files. The process of purging these log files is truncating the log. This option enables truncating of committed transaction log files, which conserves disk space.

   The available options are SQL Server and Exchange Server. You can select either, both, or none of these applications. If you select any of these applications, you can also specify a scheduled time period (Daily, Weekly, or Monthly) for automatic log truncation:

Note: The transaction log files cannot be truncated without performing a successful backup.

- **Daily** - Each day after the backup completes successfully, the committed transaction logs will be purged immediately.

- **Weekly** - After seven days, the committed transaction logs will be purged immediately after the backup completes successfully.

- **Monthly** - After 30 days, the committed transaction logs will be purged immediately after the backup completes successfully.

If a backup job is already running at the same time the purging is scheduled to be performed, the purging operation is moved to the next scheduled job.

Example:

You scheduled an Incremental Backup to run automatically every day at 5:00 pm, and then started a Full Backup manually at 4:55 pm. You assume that the backup successfully finishes at 5:10 pm.

In this case, the Incremental Backup that is scheduled for 5:00 pm is skipped because the ad-hoc Full Backup is still in progress. Now the committed transaction log files are purged after the next successful backup job and be performed on the next day after the scheduled Incremental Backup completes successfully at 5:00 pm.

Reserve Space on Destination

This value indicates a percentage of the calculated space that is necessary to perform a backup. This amount of continuous space is then immediately reserved on the destination before the backup starts writing data and helps improve backup speed.

Default: 10%.

Example: Set the value to 10% and the current backup has 50 GB of data to back up. Before the backup starts writing data, it first reserves 5 GB of disk space. After the 5 GB of disk space is used up, it then reserves the next 5 GB of disk space. If the data remaining for the backup is less than 5 GB (suppose 2 GB are remaining to back up), then the remaining GB (in this example 2 GB) are reserved.

Exchange Granular Restore Catalog

Enables automatic generation of the Exchange Granular Restore catalogs after each backup.

An Exchange Granular Restore backup captures information about the mail message, the mail folder, and the mailbox levels of Exchange in a single pass backup through the Exchange database. With this option enabled, you can then perform granular recoveries of the Exchange database by selecting from a list of objects inside Exchange and specifying exactly what you want to recover without first having to recover or dump the Exchange database to an alternate location.

– Advantages: With an Exchange Granular Restore catalog, there is no need to wait a long time to perform a restore browse.

– Disadvantages: When you generate an Exchange Granular Restore catalog during each backup, it results in an increased backup window (additional time to complete the backup job) and an increased workload. CA ARCserve D2D must go to each mailbox, authenticate, and build the granular information, which considering the number of mailboxes and size of data, could be a time consuming task.

– If you disable this option, CA ARCserve D2D only saves the general information for Exchange. Before restore you have an opportunity to generate an Exchange Granular Restore catalog at that time.

Administrator Account

Specifies the User Name and Password with access rights to perform the backup. CA ARCserve D2D verifies that the name and password are valid and the user belongs to an administrator group.

Important! If the Administrator Account credential information for the CA ARCserve D2D server is changed (User Name/Password), you must also reconfigure/update the Administrator Account information in this dialog.

Note: To specify a domain account, the format for the user name is a fully qualified domain user name in the form of "*<domain name>\<user name>*".

Recover Backup Destination Connection

Lets you update (resynchronize) the connection information to your backup destination.

You can use this option if you are performing periodic backups to a remote share computer and then you can change the access credentials (user name/password) for that remote computer. In this case, typically your next backup would fail because the access credentials configured at your local computer do not match the new credentials at the remote computer.

Note: When you click the Update Connection button and the resynchronize process begins, you cannot cancel it.

Before you click this Update button, perform the following tasks:

■ Log in to the remote destination computer and use the following net session command to disconnect the connection between the local CA ARCserve D2D computer and the remote computer:

net session \\<computer name or IP address> /d

■ Return to the CA ARCserve D2D computer, and click the Update Connection button.

■ Enter new password for destination.

■ CA ARCserve D2D updates your configured credentials to match the new credential information at the remote share destination. A pop-up confirmation screen appears informing you that the credentials have been updated.

3. Click Save Settings.

Your advanced backup settings are saved.

Specify Pre/Post Backup Settings

CA ARCserve D2D lets you specify the Pre/Post Backup settings.

Note: To view a video that is related to these Backup Settings, see <u>Manage Backup Settings</u> (see page 67).

Specify the Pre/Post Backup Settings

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the Backup Settings tab. When the Backup Settings dialog opens, select Pre/Post Backup.

The Pre/Post Backup Settings dialog opens.

2. Specify your pre/post backup setting options.

   Actions

   Runs script commands for actions to take before the start of the backup, after the snapshot image is captured, and/or upon the completion of the backup. You can also trigger the script command based upon specific exit codes and select the action to be taken (run job or fail job) when that exit code is returned.

   ■ A "run job" action directs CA ARCserve D2D to continue to run the job if the specified exit code is returned.

   ■ A "fail job" action directs CA ARCserve D2D to cancel the job if the specified exit code is returned.

3. Click Save Settings.

   Your pre/post backup settings are saved.

Manage File Copy Settings

CA ARCserve D2D lets you copy selected source files (copy or move) from a backup session to a destination (disk or cloud) based upon your specified file copy and retention criteria. File Copy can be used for copying critical data to secondary locations and can also be used as an archiving solution. File Copy allows you to safely and securely delete the source data after it has been copied to an off-site or secondary storage repository.

The advantages of copying files are:

■ **Improve Efficiency** - Helps you to speed backup and recovery processes by copying and moving unchanged data and reduce the amount of real data being backed up and stored to tape or disk.

■ **Meet Regulatory Compliance** - Helps you to preserve important documents, emails, and other critical data, as necessary to comply with internal rules and external regulations.

■ **Reduce Storage Cost** - Helps you to reclaim storage capacity by migrating older or infrequently accessed data from your primary systems to more cost-effective archival storage locations.

■ **Maintain Multiple File Versions** - Helps you to roll back to previous versions of backed-up files (if necessary) or maintain multiple versions of the same files at different destinations.

Before you perform your first File Copy job, specify the File Copy settings and policies. These configurations allow you to specify behaviors such as the source of your file copy data, destination for your copied files, the schedule for each file copy job, and the settings and filters applied to your file copy jobs. These settings can be modified at any time from the CA ARCserve D2D home page.

Note: To improve the performance (upload speed and server load), File Copy can upload the data to the specified destination in parallel chunks. To configure the number of chunks that are simultaneously sent to the destination, see Configure File Copy Chunk Value (see page 106).

Note: The File Copy job always applies the policies that were defined at the time of catalog generation for that session, and not the policies that were defined at the time of backup.

CA Support:	How to: Perform a File Copy Job
YouTube:	How to: Perform a File Copy Job

To manage the File Copy settings, click the Settings link on the CA ARCserve D2D home page and select the File Copy Settings tab. The File Copy Settings dialogs consist of the following subordinate tab options:

- Source (see page 90)

- Destination (see page 98)

- Schedule (see page 107)

Specify the File Copy Source

CA ARCserve D2D lets you specify the source settings for your information to be file copied.

Note: To view a video that is related to the File Copy Settings, see Manage File Copy Settings (see page 89).

Follow these steps:

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the File Copy Settings tab. When the File Copy Settings dialog opens, select Source.

   The File Copy Source dialog opens.

2. Specify your file copy source settings.

   Enable File Copy

   Enables the scheduled copying of files after the specified number of backups. If this option is not selected (File Copy disabled), no scheduled file copying is performed and any changes to the File Copy settings are not validated and saved.

   File Copy Sources

   Displays a selectable listing of all sources, with the corresponding policy (filters) and type of file copy (copy and retain or copy and move) to be performed after each successful CA ARCserve D2D backup. These File Copy Sources can be added, removed, or modified.

   Note: CA ARCserve D2D does not copy application files, files with system attributes, and files with temporary attributes.

   Note: If a symbolic link is selected when specifying the File Copy source folder, it is replaced with the actual path it points to when saving the settings. From the File Copy Restore user interface, the actual path displays instead of the symbolic link.

■ **Add Source**

When clicked, the Policy type dialog opens to let you initially select the type of file copy job to perform (copy and retain or copy and move). After you select the policy type, the corresponding File Copy Policy dialog opens to let you add a source to copy and specify the corresponding policies for that source. For more information, see Specify File Copy Policies (see page 92).

Note: The File Copy source can only be chosen from a volume that is currently selected in Backup Settings.

■ **Remove**

When clicked removes the selected source from this displayed list.

■ **Modify**
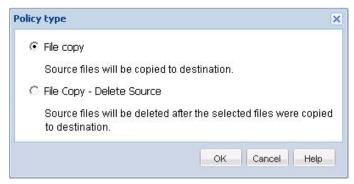
When clicked, the File Copy Policies dialog opens to let you change the policy settings for the selected source. For more information, see Specify File Copy Policies (see page 92).

3. Click Save Settings.

Your File Copy settings are saved.

Specify File Copy Policies

When you click the Add Source option for File Copy, the Policy type dialog opens to let you initially select the type of File Copy job to be performed.

The available types are File Copy and File Copy - Delete Source.

File Copy

Data is copied from the source to the destination (remains on source location) and provides multiple stored versions on the destination.

File Copy - Delete Source

Data is <u>moved</u> from the source to the destination (deleted from source location) and provides more available free space at your source.

When you select File Copy - Delete Source, a warning message is immediately displayed alerting you that your specified file copied data will be moved (deleted) from and no longer available at the original source location. Click OK to continue to the File Copy Policies dialog.

For files copied using the File Copy - Delete Source option, CA ARCserve D2D leaves a stub file with the "D2DARC" extension. The stub file contains information about the destination where the files were moved. If a file is restored to the original location and then gets moved again to the specified destination, then the stub file is updated with this move information. If necessary, these file copy stub files can be safely disabled or deleted without any negative impact. (Existing stub files are not deleted when the registry key is changed to no longer create stub files).

If you want to disable stub file creation, access/create the registry key "HKLM\SOFTWARE\CA\CA ARCserve D2D\AFArchiveDLL" and then create a DWORD named "CreateStubFile" with the value set to 0.

Note: If you disable or delete the file copy stub files, you can no longer track the status and location of moved files.

If you want to Add a new File Copy source or you want to Modify an existing File Copy source, the File Copy Policies dialog lets you specify the details.

Depending upon the policy type that is selected, a different File Copy Policies dialog opens; however, the selections are similar.

File Copy Selected:

File Copy - Delete Source Selected:

File Copy - Source Selection

Lets you specify the file copy source. You can specify or browse to a source volume or folder.

Source Filters

Filters let you limit the objects to be file copied by certain specified types and values.

For more information about these filters, see How File Copy Source Filters Work (see page 97).

Filter Type

There are two types of filters: Include and Exclude.

An Include filter copies only those objects from the file copy source that match the specified value.

An Exclude filter copies all objects from the file copy source except those that match the specified value.

You can specify multiple filters within the same file copy request by separating each filter value with a comma.

– If you specify multiple Include filters, the data is included in the file copy if any one of those Include filters matches.

– If you specify multiple Exclude filters, the data is excluded from the file copy if any one of those Exclude filters matches.

– You can mix both Include and Exclude filters in the same file copy request.

Note: When the specified parameters of Exclude and Include filters conflict, the Exclude filter is always a higher priority and is enforced. An Include filter can never file copy an object that was also Excluded.

Filter Variable (Pattern)

There are two types of variable pattern filters: File Pattern and Folder Pattern.

You can use a File Pattern filter or Folder Pattern filter to include or exclude certain objects from the file copy.

Filter Value

The filter value lets you limit the information that is file copied by selecting only the parameter information that you specify, such as .txt files.

CA ARCserve D2D supports the use of wildcard characters to help select multiple objects to file copy with a single request. A wildcard character is a special character that can be used as a substitute to represent either a single character or a string of text.

The wildcard characters asterisk and question mark are supported in the Value field. If you do not know the complete file/folder pattern value, you can simplify the results of the filter by specifying a wildcard character.

–   "*" - Use the asterisk to substitute zero or more characters in the value.

–   "?" - Use the question mark to substitute a single character in the value.

For example, you can enter *.txt to exclude all files with a .txt extension if you do not know the specific file name. You can provide as much of the file name as you know, then use wildcards to fill in the blanks.

Note: When you select File Pattern as the filter type, a drop-down list of predefined filters for many commonly used files is available (MS-Office files, Image files, Executable files, Temp files, etc.). After choosing any of the predefined filters, you can still append or modify the corresponding values.

File Size Filter (File Copy - Delete Source Jobs Only)

This filter only applies to File Copy - Delete Source jobs (not File Copy jobs).

File size filters let you limit the source objects to be file copied based upon the size of the file. When you enable the file size filter, the parameters that you specify become the filter for which objects will and will not be included in the file copy. You can select the range (Equal to or Greater Than, Equal to or Less Than, or Between) and then enter a value for the size.

For example, if you specify Equal to or Greater Than 10MB, then CA ARCserve D2D only file copies objects that meet this criteria. All other objects that do not meet this file size criteria are not file copied.

File Age Filter (File Copy - Delete Source Jobs Only)

This filter only applies to File Copy - Delete Source jobs (not File Copy jobs).

File age filters let you automatically include source objects to be file copied based upon certain dates for the file. You can select a parameter (Files not accessed in, Files not modified in, and/or Files not created in) and then enter a value for the number of days, months, or years for the file age filter. You can select multiple file age filters for automatic file copying.

For example, if you specify Files not modified in 180 days, then CA ARCserve D2D automatically file copies all files that meet this criteria (have not been modified during the last 180 days).

Important! If you specify both File Size and File Age filters (or multiple File Age filters), then only the files which meet <u>all</u> of the specified filter parameters are file copied. Files which do not meet any one of these specified parameters are not file copied.

How File Copy Filters Work

The File Copy source filters for files and folders work as follows:

- File with "d2darc" and "ASBUARC" extensions are always skipped.

- Files with system and temporary attributes are always skipped.

- Windows, Program Files, and D2D installation folders (for both File Copy and File Copy - delete source policies) are always skipped.

- The following precedence order is used for filtering (with the highest precedence listed first):

  - Exclude directory filters

  - Exclude file filters

  - Include directory filters

  - Include file filters

  - Include Criteria

  - Exclude system and application files (Exchange and SQL only) present in any location. (This filter is only applicable for File Copy - Delete Source policies).

- A file is copied only if the Include Folder or the Include File filter matches, it does not need to satisfy both filter requirements.

- The File filter works only on the file name, and does not depend on the path.

  For example, if you have the three files "Test.txt", "Hellotest.txt", and "TestHello.txt" these filters produce the following results:

  - Test*.txt filter matches only Test.txt and TestHello.txt

  - Test* filter matches Test.txt and TestHello.txt

  - Test filter does not match anything

  - *.txt filter matches all of them

  - *test filter does not match anything

■ A Folder filter works on the policy source level.

For example, if you have the following directory structure:

```
C:
->Z99
-> ->A00
-> -> ->B01
-> -> ->C01
-> -> ->D01
```

- If you configure your File Copy Source as "C:\Z99\A00" and you apply an Include Folder **b*** filter, then all files under c:\Z99\A00\B01 are copied.

  In this example, the Source includes the parent folder and the asterisk is located after the "b". As a result all files in any folder subordinate to "A00" that starts with "b" are copied.

- If you configure your File Copy Source as "C:\Z99 and you apply an Include Folder **b*** filter, then this filter does not match any folder and no files are copied.

  In this example, the Source does includes the"Z99" grandparent folder, but not the "A00" parent folder. As a result, there are no "b" folders directly subordinate to "Z99" and no files are copied.

- However if you specify a ***b*** filter, it now matches any subordinate folder that starts with "b" and all files within these "b" folders are then copied.

  In this example, the asterisk is now located before the "b". As a result, all files in any folder subordinate to "C:\Z99" (regardless of the root level) that starts with "b" are copied.

- If you configure your File Copy Source as "C:\Z99" and you apply an Include Folder ***01** filter, then all subordinate folders containing "01" (B01, C01, and D01) are copied.

  In this example, the asterisk is located before the "01". As a result, all files in any subordinate folders (regardless of the root level) that contains "01" are copied.

Note: Folder filters are always relative to the source folder path specified in the policy.

Specify the File Copy Destination

CA ARCserve D2D lets you specify the destination settings for your information to be file copied.

Note: To view a video that is related to File Copy Settings, see Manage File Copy Settings (see page 89).

Specify the file copy destination

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the File Copy Settings tab. When the File Copy Settings dialog opens, select Destination.

   The File Copy Settings Destination dialog opens.

2. Specify your File Copy destination settings.

Destination

Specifies the destination location for the file copy job. You can only select one destination.

CA ARCserve D2D lets you specify the settings for file copying your backed-up files to a disk or to the cloud. For file copying, you can specify to perform a copy and retain or a copy and move of your backed-up data. The two processes are similar, with the exception that when you perform a copy and move, the data is moved from the source to the destination (deleted from source location) and provides more available free space at your source. When you perform a copy and retain, the data is copied from the source to the destination (remains on source destination) and provides multiple stored versions.

- ■ **File Copy to a local or network drive**

    When selected, lets you specify the full path of the location where you want to move or copy the source files/folders. The destination can be any local volume or folder or a file share accessible by any uniform naming convention (UNC) path. You can browse to this destination location. Clicking the green arrow icon lets you validate the connection to the specified destination.

- ■ **File Copy to Cloud**

    When selected, lets you specify the cloud location where you want to move or copy the source files/folders. CA ARCserve D2D currently supports file copying to multiple cloud vendors, such as Amazon S3 (Simple Storage Service), Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus. These cloud vendors are publicly available web services which let you safely and securely store and retrieve any amount of data, at any time, from anywhere on the Web.

    You can click the Configure button to display the Cloud Configuration dialog. For more information, see Specify Cloud Configuration for File Copy (see page 103).

    Note: To eliminate any potential clock skew error when attempting to connect to the cloud, verify that your machine has the correct time zone set and the clock is in sync with the global time. You should always check the time of your machine against the GMT time. If the time of your machine is not synchronized with the correct global clock time (within 5 to 10 minutes), your cloud connection may not work. If necessary, reset the correct time for your machine and rerun your file copy job.

For either destination option, if the connection to the specified destination is lost or broken, CA ARCserve D2D makes several attempts to continue the file copy job. If these reattempts are not successful, a makeup job is then performed from the point where the failure occurred. In addition, the activity log is updated with a corresponding error message and an email notification is sent (if configured).

Compression

Specifies the type of compression that is used for File Copy jobs.

Compression is performed to decrease your storage space at the File Copy destination, but also has an inverse impact on your file copy speed due to the increased CPU usage.

Note: For a compressed File Copy job, the Activity log displays only the uncompressed size.

The available options are:

- **No Compression**

  No compression is performed. This option has the lowest CPU usage (fastest speed), but also has the largest storage space requirement for your file copy.

- **Standard Compression**

  Some compression is performed. This option provides a good balance between CPU usage and storage space requirement. This is the default setting.

- **Maximum Compression**

  Maximum compression is performed. This option provides the highest CPU usage (lowest speed), but also has the lowest storage space requirement for your file copy.

Encryption

Specifies to use encryption for file copying.

Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. CA ARCserve D2D data protection uses secure, AES-256 (Advanced Encryption Standard) encryption algorithms to achieve maximum security and privacy of your specified data.

When an encryption is selected, you must provide (and confirm) an encryption password.

Retention Time

This setting only applies to file copied data that is moved (not file copy data that is retained).

Specifies the amount of time (years, months, weeks, days) that the stored data is retained at the destination location. At the end of the specified retention time period, the stored data is purged from the destination.

The retention time calculations are based upon a month being 30 days and a year being 365 days. For example: If you specify a retention time of 2 years, 2 months, and 5 days, then the total retention time for your file copied data is 795 days (365 + 365 + 30 + 30 + 5).

Important! Because this retention time setting only applies to data that has been copied and moved from the source to the destination (and not copied and retained), it is important to understand that at the end of the specified retention time when the data is purged from the destination, all of this moved data is no longer stored or saved.

Note: The Retention Time purge process is only triggered if the File Copy Schedule option is enabled.

File Versions

This setting only applies to copied data that is retained (not copied data that is moved).

Specifies the number of copies retained and stored at the destination location (cloud or disk). After this number is exceeded, the earliest (oldest) version will be discarded. This cycle of discarding the oldest stored version repeats as newer versions are added to the destination, allowing you to always maintain the specified number of stored versions.

For example, if your specified File Versions retention count is set to 5 and you perform five file copies at times t1, t2, t3, t4, and t5, these file copies become the five file copy versions retained and available to recover. After the sixth file copy is performed (new version is saved), CA ARCserve D2D will remove the t1 copy and the five available versions to recover are now t2, t3, t4, t5, and t6.

By default, the number of copies retained at the destination location before discarding is 15.

3. Click Save Settings.

    Your File Copy settings are saved.

Specify Cloud Configuration for File Copy

From the File Copy Settings Destination dialog, you can click the Configure button to display the Cloud Configuration dialog.

From this dialog you can use the drop-down menu to select which cloud vendor type you want to use for storage of your file copies. The available options are Amazon S3, Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus. (Amazon S3 is the default vendor). For more information about Fujitsu Cloud (Windows Azure), see the Overview and Registration.

Note: If you are using Eucalyptus-Walrus as your file copy cloud vendor, you will not be able to copy files whose entire path length is greater than 170 characters.

The configuration options for each cloud vendor are similar (with some different terminology), and any differences are described.

1. Specify the Connection Settings:

    Vendor URL

    Identifies the URL address of the cloud provider.

    (For Amazon S3, Windows Azure, and Fujitsu Cloud (Windows Azure), the Vendor URL is automatically pre-populated. For Eucalyptus-Walrus, the Vendor URL must be manually entered using the specified format).

    Access Key ID/Account Name/Query ID

    Identifies the user who is requesting access this location.

    (For this field, Amazon S3 uses Access Key ID, Windows Azure and Fujitsu Cloud (Windows Azure) use Account Name, and Eucalyptus-Walrus uses Query ID).

    Secret Access Key/Secret Key

    Because your Access Key is not encrypted, this Secret Access Key is a password that is used to verify the authenticity of the request to access this location.

    Important! This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials in a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

    (For this field, Amazon S3 uses Secret Access Key. Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus use Secret Key).

    Enable Proxy

    If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections. You can also select this option if your proxy server requires authentication. You then must provide the corresponding authentication information (Username and Password) that is required to use the proxy server.

    (Proxy capability is not available for Eucalyptus-Walrus).

2. Specify the Advanced Settings:

Bucket Name/Container

All files and folders moved or copied to the cloud vendor are stored and organized in your buckets (or containers). Buckets are like a container for your files and are used to group and organize objects together. Every object stored at the cloud vendor is placed in a bucket.

(For this field, Amazon S3 and Eucalyptus-Walrus use Bucket Name. Windows Azure and Fujitsu Cloud (Windows Azure) use Container).

Note: For the remainder of this step, all references to Buckets can also be applied to Containers unless specified.

You can either select a bucket name from the drop-down list, or you can add a new bucket name. If necessary, you can click the refresh button to update the list of available buckets.

To add a new bucket name:

a. Click the Add button next to the Bucket Name field to display the Add New Bucket dialog.

b. Add your new Bucket Name. The Bucket Name is automatically prefixed with name "d2dfilecopy-<hostname>-<user given name>". This is the format for the Bucket Name you create and is used as your File Copy destination.

A bucket name should be unique, easily identifiable, and compliant with internet domain naming rules. No two buckets can have the same name. It is important to understand valid syntax for bucket names.

For Amazon S3 and Eucalyptus-Walrus, refer to the Amazon S3 documentation for more information about bucket naming requirements.

For Windows Azure and Fujitsu Cloud (Windows Azure), refer to the Microsoft documentation for more information about container naming requirements.

c. For Amazon S3 only, select an available region from the drop-down menu. By default, all available regions are included in the drop-down menu and you can select the region where you want the new bucket to be created.

Regions allow you to select the geographical region where Amazon S3 stores the buckets that you create. You should select a Region that provides you with fast access to your data and allows you to optimize latency, minimize costs, or address regulatory requirements.

(For Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus, the region is not selectable).

d. After you have specified your values, click OK. The Bucket name is validated and created at the cloud.

e. After you successfully create the new bucket, the main Cloud Configuration dialog is displayed again, with the new bucket information (name and region) included in the Advanced Settings fields.

Enable Reduced Redundancy Storage

For Amazon S3 only, this option lets you select to enable Reduced Redundancy Storage (RRS). RRS is a storage option within Amazon S3 that helps you reduce cost by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. Both the standard and reduced redundancy storage options store data in multiple facilities and on multiple devices, but with RRS the data is replicated fewer times, so the cost is less. You should expect the same latency and throughput using either the Amazon S3 standard storage or RRS. By default this option is not selected (Amazon S3 uses the standard storage option).

3. Click Test Connection to verify the connection to the specified cloud location.

4. Click OK to exit the Cloud Configuration dialog.

Configure File Copy Chunk Value

To improve the performance (upload speed and server load), File Copy can upload data to the specified destination in parallel chunks. CA ARCserve D2D lets you set the number of 1-MB chunks that will be simultaneously sent to the destination. By increasing the number of parallel chunks, you will decrease the time to complete the job, but will also have an adverse affect on server performance. You should configure this value as necessary to obtain optimal performance.

For example, if you are performing File Copy for a 10-MB file and set the number of 1-MB chunks to 2, then File Copy will write 10 chunks, two at a time. If you see that this is taking too long to complete the job, you can change this value to 4. The time to complete the job will then decrease because File Copy will now be writing 10 chunks, four at a time, but the load on your server will increase.

To configure the number of chunks, set the corresponding DWORD value as follows:

1. Start edit registry.

2. Locate key:

   "HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AfArchiveDll"

3. Manually create a DWORD value for "ArchMultChunkIO"

4. Assign a DWORD value:

   The available range for the number of chunks is 1 - 4 chunks (default value is 4 chunks).

Specify the File Copy Schedule

CA ARCserve D2D lets you specify the schedule settings for your information to be file copied.

Note: To view a video that is related to the File Copy Settings, see Manage File Copy Settings (see page 89).

Follow these steps:

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the File Copy Settings tab. When the File Copy Settings dialog opens, select Schedule.

   The File Copy Settings Schedule dialog opens.

2. Specify your File Copy schedule settings.

   Schedule

   Enables the file copying of data after the specified number of backups.

   The file copy process will be launched automatically after the specified number of successful backups (Full, Incremental, and Verify) and will be based on your selected File Copy policies.

   You can use this setting to control how many times a File Copy job is triggered each day. For example, if you specify to run a backup job every 15 minutes, then if you specify to run a File Copy job after every 4 backups, there will be 24 File Copy jobs performed each day (1 each hour).

   The number of backups that can be specified before the File Copy job runs must be in the range 1 - 700. By default, the schedule for file copying is after every five successful backups are completed.

3. Click Save Settings.

   Your File Copy settings are saved.

Configure the Copy Recovery Point Settings

CA ARCserve D2D lets you specify the recovery point copy settings. Before you copy a recovery point, configure the copy recovery point settings. For a better understanding about how the options on this dialog can be used to configure your recovery point copy schedule, see Copy Recovery Points - Example Scenarios (see page 112).

Note: The recovery point copy process is a copy and paste operation only and not a cut and paste operation. As a result, whenever a scheduled copy recovery point job is performed CA ARCserve D2D creates an additional copy of the recovery point to the specified copy destination, while still retaining the original copy of the recovery point at the backup destination that was specified in Backup Settings.

Follow these steps:

1. On the CA ARCserve D2D home page, select Settings from the taskbar.

   The Settings dialog opens.

2. Click the Copy Recovery Points tab.

   The Copy Recovery Points dialog opens.

3. Select Enable Copy Recovery Points.

   When selected, enables the copying of recovery points.

   Note: If you do not select this option, no scheduled copying of recovery points is performed.

4. Specify the following recovery point copy schedule settings:

Destination

Specifies the storage location for the copy of the selected recovery point. (Optional) You can click the green arrow button to verify the connection to the specified location.

Note: The maximum length for the specified destination path is 158 characters.

Copy Recovery Points job will be run after the specified number of backups are performed

Specifies when the scheduled recovery point copy process is automatically launched. This process is launched based on your selected copy policies and specified number of successful backups (Full, Incremental, and Verify).

You can use this setting to control how many times a recovery point copy process is triggered each day. For example, if you schedule to run a backup job every 15 minutes, and copy job after every 4 backups, then it performs 24 recovery point copy jobs each day (1 each hour).

Default: 8

Minimum: 1

Maximum: 1344

Important! If you schedule backup and copy jobs to run at regular intervals and if the copy job is currently running (in active state) when the scheduled time for the backup job time arrives, the backup job fails. (The next backup job will run as scheduled and should be successful if it does not conflict with another copy job). Because the copy operation takes almost same amount of time as performing a full backup, the best practice is not to set a frequent schedule for your recovery point copy jobs.

Specify the number of recovery points to keep

Specifies the number of recovery points that are retained and stored at the specified copy destination. Discards the oldest recovery point, when this number is exceeded.

Note: If you do not have sufficient free space at the target destination, reduce the number of saved recovery points.

Default: 1

Maximum: 1344

5. Select the Compression level.

Compression is typically performed to decrease your disk space usage, but also has an inverse impact on your backup speed due to the increased CPU usage.

The available options are:

- **No Compression** - Compression is not performed. Files are pure VHD. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

- **No Compression - VHD** - Compression is not performed. Files are converted to .vhd format directly, without the need for manual operations. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

- **Standard Compression** - Some compression is performed. This option provides a good balance between CPU usage and disk space usage. This setting is the default setting.

- **Maximum Compression** - Maximum compression is performed. This option provides the highest CPU usage (lowest speed), but also has the lowest disk space usage for your backup image.

Note: If your backup image contains uncompressible data (such as JPG images or ZIP files), additional storage space can be allocated to handle such data. As a result, if you select any compression option and you have uncompressible data in your backup, it can actually result in an increase in your disk space usage.

6. If you also want the copied recovery point to be encrypted, specify the following information:

Encryption Algorithm

Specifies the type of encryption algorithm that is used for the recovery point copies.

The available format options are No Encryption, AES-128, AES-192, and AES-256.

Encryption Password

Lets you specify and confirm the encryption password being used to encrypt the destination session.

7. Click Save Settings.

Your recovery point copy settings are saved.

The copy recovery point settings are successfully configured.

Copy Recovery Points - Example Scenarios

The following example scenarios are provided to give you a better understanding of how the various options can affect your scheduled copying of recovery points.

For this example, assume that you configured your CA ARCserve D2D backup schedule as follows:

- Full Backup - Every 7 days

- Incremental Backup - Every 1 hour

- Verify Backup - Every 3 days

and assume:

- First backup is on Day #1 at 5:00PM (by default, the first backup is always a Full Backup)

- First Incremental Backup will be on Day #1 at 6:00PM (and every hour after)

- Recovery Points retention count is set to 31 (default number)

- Location "D" is configured as the copy destination

Scenario #1

For this scenario, the Copy Recovery Point settings are as follows:

- Copy after 4 backups

- Retain 1 recovery point

  Result:

  – At 8:00PM (after the 4th backup), the scheduled copy job will run and consolidate all 4 recovery points into a single recovery point and store it at destination D.

  – At 12:00 midnight (after the 8th backup), the next scheduled copy job will run and consolidate all 8 recovery points into a single recovery point and store it at destination D.

  The previous recovery point is removed from destination D because the setting is to retain only 1 recovery point at the destination.

Scenario #2

For this scenario, the Copy Recovery Point settings are as follows:

- Copy after 4 backups
- Retain 4 recovery points

   Result:

   – At 8:00PM (after the 4th backup), the scheduled copy job will run and consolidate all 4 recovery points into a single recovery point (Recovery Point #1) and store it at destination D.

   – At 12:00 midnight (after the 8th backup), the next scheduled copy job will run to create Recovery Point #2 and store it at destination D.

   – At 4:00AM on Day #2 (after the 12th backup), the next scheduled copy job will run to create Recovery Point #3 and store it at destination D.

   – At 8:00AM on Day #2 (after the 16th backup), the next scheduled copy job will run to create Recovery Point #4 and store it at destination D.

   – At 12:00 noon on Day #2 (after the 20th backup), the next scheduled copy job will run. A new recovery point will be created and the first recovery point (created after the 8:00PM backup on previous day) is removed from destination D, because the setting is to retain only 4 recovery points at the destination.

Scenario #3

For this scenario, the Copy Recovery Point settings are as follows:

- Copy after 1 backup
- Retain 4 recovery points

   Result:

   – At 5:00PM (after the 1st backup), the scheduled copy job will run to create a single recovery point (Recovery Point #1) and store it at destination D.

   – At 6:00PM (after the 2nd backup), the next scheduled copy job will run to create Recovery Point #2 and store it at destination D.

   – At 7:00PM (after the 3rd backup), the next scheduled copy job will run to create Recovery Point #3 and store it at destination D.

   – At 8:00PM (after the 4th backup), the next scheduled copy job will run to create Recovery Point #4 and store it at destination D.

   – At 9:00PM (after the 5th backup), the next scheduled copy job will run. A new recovery point will be created and the first recovery point (created after the 5:00PM backup) is removed from destination D, because the setting is to retain only 4 recovery points at the destination.

Specify Preferences

The Preferences dialog page provides a quick and easy way to specify various options for the behavior of your CA ARCserve D2D. When clicked, the Preferences dialog opens with the following subordinate tabs:

■ General (see page 114)

■ Email Alerts

■ Updates (see page 122)

Specify General Preferences

CA ARCserve D2D lets you specify your General preferences:

Specify the General Preferences

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the Preferences tab. When the Preferences dialog opens, select General.

   The General preferences dialog opens.

2. Specify your General preference settings.

News Feed

When checked, enables RSS feeds of the latest CA ARCserve D2D related news and product information (from the Expert Advice Center) to be displayed on the home page.

Social Networking

When checked, displays icons on the home page for access to Twitter and Facebook for CA ARCserve D2D-related social networking. These selections will take affect only after refreshing the home page.

Tray Notifications

Select the type of Alert notifications you want to display. The available options are None, All, and Errors and Warnings.

Videos

Select the source for viewing CA ARCserve D2D instructional videos when accessed from either the Getting Started (see page 49) screen or the Support and Community Access (see page 61) taskbar. The available options for viewing these "how-to videos" are Use CA Support Videos and Use YouTube Videos. (The content of the videos are the same at each source).

Note: This selection does not affect the video viewing options available on the related of the Help topics.

3. Click Save Settings.

Your General preference settings are saved.

Specify Email Preferences

CA ARCserve D2D lets you specify the following Email Alert preferences:

Specify the Email Alerts Preferences

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the Preferences tab. When the Preferences dialog opens, select Email Alerts.

   The Email Alerts preferences dialog opens.

2. Specify your Email Alerts notification settings.

   Automatic email alert notifications are sent upon the completion of selected events. You can select any or all of the available options.

   Note: If you do not need specific notifications for successful jobs, you can configure CA ARCserve D2D to only send email alerts for failed and missed jobs. This configuration could help you reduce the amount of email notifications and also monitor any failures.

The available options are to send an alert notification for the following events:

Missed jobs

Sends an email alert notification for all missed jobs. A missed job is any scheduled job that did not run at the scheduled time. A missed job could happen when some other job of the same type is running or previous job that started earlier did not finish yet.

CA ARCserve D2D allows different types of jobs to be run in parallel; however, only one job of each type can be run at the same time. For example, if a copy job is still running at the scheduled time for another copy job then the scheduled copy job is missed, but another backup job can still run.

Backup, Catalog, File Copy, Restore, or Copy Recovery Point job failure/crash

Sends an alert notification for all unsuccessful backup, catalog, file copy, restore, or copy recovery point job attempts. This category includes all failed, incomplete, and canceled jobs, and crashed attempts.

Note: These email alerts are sent with a high importance. The email alerts that have a high importance level setting display a visual indicator of an exclamation point in their Inbox.

Backup, Catalog, File Copy, Restore, or Copy Recovery Point job success

Sends an alert notification for all successful backup, catalog, file copy, restore, or copy recovery point job attempts.

Merge job stopped, skipped, failed, or crashed

Sends an alert notification for all stopped, skipped, failed, or crashed merge jobs. If you enable this alert, you are informed once a merge job is unsuccessful.

A merge failure can occur for the following reasons:

■   The session is mounted.

    To solve the problem, you can dismount the session.

■   The session is locked by a catalog job.

    The next backup job automatically merges this session.

■   The session is locked due to other reasons.

If you disable this alert, you only know when a merge was unsuccessful from the balloon message in the tray monitor or the Recovery Points Summary on the CA ARCserve D2D Home Page.

Merge job success

Sends an alert notification for all successful merge jobs.

Backup Destination free space is less than

Sends an email alert notification when the amount of unused space at the backup destination is less than a specified value. For this option, you can further select either a percentage of the total capacity or a specific value (in MB) for the threshold level of when the alert notification is sent.

New Updates Available

Sends an email notification when a new update for CA ARCserve D2D is available. Email notifications are also sent if a failure occurs during the check for updates or during the download.

Enable Resource Alerts

Sends an email notification when any specified resource threshold level is reached. To ensure that your server is efficient and reliable, continually be aware of the performance to identify possible problems and quickly address bottleneck situations.

Defining threshold levels for these resource indicators is strictly up to you and your knowledge of your server. You cannot specify right or wrong settings and could base these alert notifications upon "normal" and acceptable performance. For example, if your system typically runs at an 80 percent CPU load, then setting a CPU Usage threshold at 75 percent would not be useful or efficient.

Each of these resource parameters can be separately configured to send an alert notification when the corresponding threshold level is reached. The maximum number that each resource alert email is sent is 5 per day.

– **CPU Usage**

The specified CPU Usage alert threshold indicates the percentage of CPU usage for your CA ARCserve D2D protected server. You can use this alert notification to ensure that your server does not become overloaded too often.

If your CPU usage is too high, your server response time can become slow or unresponsive. Therefore, consider spreading out (balancing) your load.

– **Disk Throughput**

The specified Disk Throughput alert threshold indicates the disk throughput (MB/second) for your CA ARCserve D2D protected server. You can use this alert notification to ensure that you are maximizing the capability of your disk.

If your disk throughput is close to the maximum value your disk can handle, consider upgrading to a disk that better matches your needs. Generally a faster disk leads to better performance.

– **Memory Usage**

The specified Memory Usage alert threshold indicates the percentage of memory in use on your CA ARCserve D2D protected server. Utilization is how much of your memory capacity you are using. The higher the percentage the worse your server performance is going to be.

If your memory use continually becomes too high, determine the process causing this high usage. You can use this indicator setting to alert you of when an application or server upgrade can be necessary.

– **Network I/O**

The specified Network I/O alert threshold indicates the percentage of NIC bandwidth you are currently using on your CA ARCserve D2D protected server. Utilization is how much of your network interface card (or NIC) capacity you are using. The higher the percentage the worse your network performance is going to be.

If your network use continually becomes too high, determine the process causing this high usage and remedy the problem. In addition, if based on your specific network capacity the percentage of your network use is too high during backup time, you can upgrade your NIC card to handle the higher throughput requirements.

3. Click Save Settings.

Your Email Alerts preference settings are saved.

After you select to send an email notification, you can then click Email Settings to display the related dialog.

Specify Email Settings

From the Email Settings dialog, you can specify email settings such as the:

- Mail server
- Subject title
- Who the email is coming from
- Email recipients

You can also enable and define your proxy settings. These settings apply to all email alert notifications and can be modified at any time.

After you establish your email settings, you can test the settings using the Test Email button. After a job runs successfully or fails, it is too late to receive an email alert for having the wrong settings. Therefore, testing the email information that is provided validates the settings and tries to send an email using the specified settings. If the email settings are valid, you receive an email indicating so. If the email settings are invalid, you receive a failure message.

Service

The email provider service to use for sending the alert notifications. The available options are Google Mail, Yahoo Mail, Live Mail, and Other.

■   If you select Other, identify the mail server and corresponding port number used.

■   If you select Google Mail, Yahoo Mail, or Live Mail the mail server and port number fields are automatically populated.

Default: Other

Mail Server

The host name of the SMTP mail server that CA ARCserve D2D can use to send the email alerts.

Port

The output port number for the mail server.

Requires Authentication

Specifies if this mail server requires authentication when attempting to send an email by way of the Internet. When this option is selected, provide the corresponding user Account Name and Password.

Subject

Subject description for the email alert notifications that CA ARCserve D2D sends.

Default: "CA ARCserve D2D Alert"

From

The email address that CA ARCserve D2D uses to send the email alert notifications.

Recipients

Email address for the recipients of the email alert notifications sent.

Note: To enter multiple email addresses, separate each address with a semi-colon character.

Use SSL

Email server requires an SSL (Secure Sockets Layer) connection to transmit data securely by way of the Internet.

Send STARTTLS

Email server requires a STARTTLS (Start TLS extension) command that is issued to initiate a secure SMTP connection between servers.

Use HTML format

Email alert notifications are sent as HTML. If this option is not selected, the alerts are sent as plain text. By default, this option is selected.

Enable Proxy Settings

Specifies if you want to connect to a proxy server for sending your email alert notifications. When this option is selected, provide the corresponding name of the proxy server and port number.

Specify Update Preferences

CA ARCserve D2D lets you specify the following Updates preferences:

Specify Updates Preferences

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Settings from the taskbar and then select the Preferences tab. When the Preferences dialog opens, select Updates.

   The Updates preferences dialog opens.

2. Specify your Updates preference settings.

   Download Server

   Specifies the source server from where your CA ARCserve D2D server will connect to and download available updates.

   ■ **CA Server**

   You can use this option to specify that CA ARCserve D2D updates will be downloaded from the CA Technologies server directly to your local server.

   This is the default setting.

■ **Staging Server**

You can use this option to specify the server that will be used as a staging server.
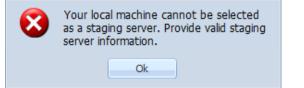
If you specify more than one staging server, the first listed server will be designated as the primary staging server. CA ARCserve D2D will initially attempt to connect to the primary staging server. If for any reason the first listed server is not available, then the next listed server will become the primary staging server. The same sequence will be continued until the last listed server becomes the primary staging server. (The Staging Server list is limited to the maximum of 5 servers).

– You can use the Move Up and Move Down buttons to change the staging server sequence.

– You can use the Delete button to remove a server from this listing.

– You can use the Add Server button to add a new server to this listing. When you click the Add Server button, the Staging Server dialog opens, allowing you to specify the name of the added staging server.

Staging Server

Name: |

Port: 8014

OK   Cancel

CA ARCserve D2D updates will be downloaded from the CA Technologies server directly to the specified staging server location. After the updates are downloaded to this staging server, you can then further download the updates from the staging server to a client server. If you select the Staging Server location, you must also specify the host name or IP address for the staging server, along with the corresponding port number.

You cannot specify your same local client server as this staging server. This is an invalid configuration because the staging server cannot connect to itself to get and download the available updates from. If you attempt to use your local client server as the staging server, an error message will be displayed.

Your local machine cannot be selected as a staging server. Provide valid staging server information.

Ok

Note: You cannot download CA ARCserve D2D updates from a staging server if HTTPS is enabled on it for web communication.

■ **Proxy Settings**

Note: This Proxy Server option is only available when you select CA Technologies Server as the download server.

Select Proxy Settings to specify if you want the CA ARCserve D2D updates to be downloaded via a proxy server. A proxy server acts as an intermediary between your download server (staging or client) and the CA Technologies server to ensure security, increased performance, and administrative control. This will be the connection to the CA Technologies server from which your download server will get the updates.

When you select this option the Proxy Settings dialog opens.

– **Use browser proxy settings**

This selection is only applicable to Windows Internet Explorer (IE) and Google Chrome.

When selected, directs CA ARCserve D2D to automatically detect and use the same proxy settings that are applied to the browser to connect to the CA Technologies server for CA ARCserve D2D update information.

– **Configure proxy settings**

When selected enables the specified proxy server to connect to the CA Technologies server for CA ARCserve D2D update information. If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections.

In addition, you can also specify if your proxy server will require authentication. When selected, specifies that authentication information (User ID and Password) are required to use the proxy server.

Note: The format for user name should be a fully qualified domain user name in the form of "<domain name>\<user name>".

Test Connection

Lets you test the following connections and display a status message when completed:

– If you selected "CA Technologies Server" as the download server, tests the connection between the machine and the CA Technologies server through the specified proxy server.

– If you selected "Staging Server" as the download server, tests the connection between the machine and the specified staging server. The test connection button is used to test the availability of each listed staging server, and a corresponding status is displayed in the Connection Status field. If none of the configured staging servers are available, a red icon is displayed on the status Summary section home page to provide a visual alert of this condition.

Note: The test connection is automatically performed when you launch the Preferences Updates dialog from the home page. When this auto test is performed it will check the latest connection status of the previously configured download server (either CA Technologies Server or Staging Server(s), whichever is selected). If you previously configured more than one staging server, then this auto test will be performed on all staging servers to get the latest connection status.

Update Schedule

Specifies when to check for (and download) new CA ARCserve D2D updates.

– With this option selected, specifies to automatically check for new and available CA ARCserve D2D updates. When you select this option, you then have drop-down menu capabilities to specify when to perform this function (every day or weekly on a specified day) and the time of the day that it will be performed.

Note: The default setting for the day or hour that these checks will be automatically performed is randomly assigned by CA ARCserve D2D at the time of installation. After installation, you can use this Update Schedule setting to change the day and time for these checks.

By default, if this check determines that a new update is available, CA ARCserve D2D will also automatically download the update. If you do not want this automatic download to be performed, you can disable this function from the D2DPMSettings.INI file. For more information, see D2DPMSettings.INI file (see page 329) in Appendix B.

– With this option not selected, specifies to disable all automatic check and download functions (and its status is displayed under status Summary section of the home page). With this option not selected, these update functions can only be triggered manually.

Note: If configured you will get an email notification if the scheduled check for updates discovers that a new update is available. In addition, email notifications will also be sent if a failure occurs during the check for updates or during the download.

3. Click Save Settings.

Your Updates preference settings are saved.

Chapter 5: Using CA ARCserve D2D

This section contains the following topics:

Perform a Backup

Before you perform your first backup, specify the backup settings to be applied to and control all subsequent backup jobs. These settings are applied to each backup job, regardless of how you initiate the backup. For more information, see Manage Backup Settings (see page 67).

A backup job can be initiated either automatically (based upon your schedule settings) or manually (immediate ad-hoc backup).

Run a Scheduled Backup (see page 139)

Run a Backup Now (see page 140)

Backup Considerations

Before you perform a CA ARCserve D2D backup, review the following backup considerations:

- **Destination available free space**

  If your destination does not have sufficient free space, you can consider the following corrective actions:

  - Reduce the number of saved recovery points.

  - Increase the available free space at the backup destination.

  - Change the backup destination to a larger capacity.

  - Reduce the size of the backup source (maybe eliminate unnecessary volumes from the backup).

  - Increase the Compression setting of the backup.

- **Ensure that you have proper licensing**

  - When using CA ARCserve D2D to perform backups (especially for Microsoft SQL Server and Microsoft Exchange Server), it is important to verify that you have the proper licenses.

  - CA ARCserve D2D uses all the VSS writers during backup to ensure consistent backups. The only exceptions are Microsoft SQL Server, Microsoft Exchange, and Hyper-V writers which are only included when they are properly licensed.

- **Backup disk size**

  A volume is skipped from a backup if it is on a disk larger than 2 TB and the compression option is disabled. However, there is no size limitation if compression is enabled (which is the default setting). As a result, if you want to back up source volumes larger than 2 TB, you must keep the compression option enabled.

- **Ensure that you are using a supported disk**

  Different types of disks are supported as CA ARCserve D2D backup source disks and destination disks.

  For more information, see Disks Supported by CA ARCserve D2D (see page 134).

- **Selecting your backup frequency and retention count**

  If your scheduled backups are occurring more frequently than the amount of time it takes to generate a file system catalog for previous backup jobs, your recovery point retention count may be exceeded before the file system catalog being generated for the oldest session is completed. If this happens there may be no catalog generated for the backup sessions. To avoid this problem, you can either increase the schedule interval time for your incremental backups or increase the retention count.

- **Backup destination folder manual operations**

  Manual operations (such as copy, cut, paste, or drag-and-drop) for the backup destination folder are not successful if a job is active or a user is browsing recovery points using the ARCserve D2D View. Verify that no active jobs are running or browsing of recovery points (using ARCserve D2D View) is being performed before attempting any of these manual operations.

- **Proper drivers installed**

  Verify that you have latest drivers/firmware installed for all the devices.

- **Ensure your machine is properly shutdown.**

  Even when backup jobs are not running, CA ARCserve D2D is constantly monitoring changes that are related to the operating system and data. Any detected changes are then compiled and saved in a list to include as an Incremental Backup after the next machine start-up. If your machine was not properly shut down and all of the changed information was not saved, CA ARCserve D2D may perform a more lengthy Verify Backup for the next backup, even if a Verify Backup was not scheduled.

- **How running backup jobs on a Hyper-V server affects the tasks that can be performed**

  When the CA ARCserve D2D backup job runs on a Hyper-V server, the status of the VMs is "Backing up" and the following tasks cannot be performed:

  - Power on

  - Power off

  - Save

  - Pause

  - Reset

  - Snapshot

  - Move

  - Rename

  - Enable replication

- **How changing the machine host name can affect saving your settings**

  When you enter a backup path, CA ARCserve D2D appends the host name to that path to use as the destination and this host name is also displayed in the settings dialog. When the name of the machine is changed, you must also change the destination path (backup, file copy, copy recovery point) by removing the old host name from the path before you attempt to save the settings.

  For example: If your host name is "Host_A" and your backup destination is X:\ and you change your host name to "Host_B", any changes that are made to your backup settings are not saved unless you first change the backup destination from x:\Host_A to x:\ again.

  If you do not change the backup destination host name and attempt to save the settings, CA ARCserve D2D thinks the backup destination "x:\Host_A" is already in use by Host_A and that Host_A is another machine and does not accept any changes to the settings.

- **How changing your backup destination can affect saved recovery points**

  When you continue performing Incremental Backups to the changed destination and the specified number of saved recovery points is reached, CA ARCserve D2D merges the earliest backup sessions to the first destination to maintain the specified number of recovery points. As this merging process repeats, the number of recovery points that are saved to the first destination decreases, and at the same time the number of recovery points for the changed destination increases. Eventually, there are no recovery points for the first destination and all of the sessions are merged to the changed destination.

- **How changing backup destinations can affect continued backups**

  If you configure and perform a Full Backup (and maybe some Incremental Backups) to a destination and then you decide to change your backups to a different destination, you can reconfigure your backup settings and continue performing Incremental Backups to the new destination without any problems.

If you later decide to change your backup destination again, you can simply reconfigure your backup settings again and continue performing Incremental Backups to the new destination without any problems.

For example:

– If you have a machine and it is configured to back up to Folder A on your local/remote volume, and after you perform a Full Backup and some Incremental backups, your destination is getting full and you want to change to a different destination (Folder B). You can reconfigure the backup settings to the Folder B destination and CA ARCserve D2D continues performing Incremental backups to that new destination. As a result, you have your Full Backup and some Incremental Backups on the original Folder A destination, and you have some Incremental Backups on the new Folder B destination.

– If after performing some Incremental Backups to Folder B, you decide to reconfigure to another new destination (Folder C), CA ARCserve D2D will continue performing Incremental Backups to the Folder C destination because the link to the original Full Backup location (Folder A) has been maintained.

If you configure and perform a Full Backup (and maybe some Incremental Backups) to a destination and then you decide to change your backups to a different destination, you can copy or move the contents from the original destination to the new destination, and then reconfigure your backup settings and continue performing Incremental Backups to the new destination without any problems.

However, if you have Full Backups in one location and Incremental Backups in a second location and then move the contents from the second location to a third location and attempt to continue performing Incremental Backups, then these backups fail because the link to the first location has been lost.

For example:

– If you have a machine and it is configured to back up to Folder A on your local/remote volume, and after you perform a Full Backup and some Incremental Backups, your destination is getting full and you want to change to a different destination (Folder B). You can move the contents of Folder A to Folder B and reconfigure the backup settings to the new Folder B destination. CA ARCserve D2D continues performing Incremental Backups to that new Folder B destination. As a result, you have your Full Backup and Incremental Backups all on the new Folder B destination.

– However, if your first destination is in Folder A (which now contains a Full Backup and some Incremental Backups) and you change the destination to Folder B using CA ARCserve D2D backup settings and continue to perform Incremental Backups, in this scenario, Folder B now only contains Incremental Backups. Then, if you move the contents from Folder B to another new destination in Folder C (moving only the Incremental Backups from Folder B without a Full Backup included), in this scenario, if you continue to perform Incremental Backups to Folder C, these Incremental Backups fails because the link to the original Full Backup location (Folder A) has been lost.

■ **How your Retention Settings can affect your merge performance**

Previously the CA ARCserve D2D merge process took a long time to complete and while the merge job was running, you could not submit any other jobs. The merge happened inside the backup job (at the end) and in a catalog job (in the beginning).

> For example, if each incremental backup generates about 100 GB of data. Merging the 100 GB of data to the full session takes more than 15 hours to complete and during this time nothing can be done.

CA ARCserve D2D now allows the merge job to merge multiple sessions at the same time. In addition, the merge job can be started/stopped and paused/resumed on demand and does not affect any other jobs. This merge process avoids multiple reads and writes because it only merges the latest change for each block. The merge process ignores all the changes that have occurred to the same block during any intermediate incremental backups. Merging multiple sessions at the same time is faster than merging them individually.

Slow merge performance is generally caused by the following reasons:

– Merge operation reads data from incremental sessions, and writes to a full session, in single data blocks (1 - 64 KB).

– Too many I/O operations for a small amount of data.

To resolve this slow merge issue, consider retaining Recovery Sets instead of Recovery Points. You can configure how many recovery sets to retain, starting with a full backup, and when the number of recovery sets exceeds the user-specified one, the oldest recovery set will be deleted, instead of merged. For more information, see Merge Job Guidelines (see page 136) and Specify Retention Settings (see page 75).

■ **How volume defragmentation can affect continued backups**

Volume defragmentation by Windows native tool affects the size of the block-level backups because CA ARCserve D2D will continue to incrementally back up all changed blocks. This means that blocks that shifted during defragmentation will also be included in the backup, even if no data has changed in the files. As a result, the backup size may increase. This is expected behavior. If you do not want the increased backup size and the added backup time is a problem, you can exclude volumes from defragmentation or stop any schedules for defragmentation.

■ **How to configure backups of replicated volumes**

If you are backing up volumes that were replicated using CA ARCserve Replication and High Availability, you should verify that the spool has been created on a separate volume and configure your backup settings to exclude the spool volume. This helps to avoid the backing up of unnecessary temp spool data.

■ **Restrictions for a Microsoft SQL Server Backup**

Due to Microsoft SQL Server VSS writer restrictions, some Microsoft SQL Server databases with a special status are automatically skipped and not backed up. These databases include:

– Database with 'Restoring' status. This status indicates that the database may be the log shipping secondary database, the mirror database, or the database waiting for more backed-up data to be restored.

– Database with 'Offline' status. This status indicates that the database is not available for general use.

– If your database is configured in one volume and the logs are configured in another volume and you select only one volume to back up, the Microsoft SQL application backup is skipped for that particular database.

– If you install Microsoft SQL Server after CA ARCserve D2D has been installed, and no backup has been performed yet, the Microsoft SQL Server may not be detected. As a result if you unselect a volume that has that application installed you may not get a warning notification that you are missing that application from the backup. This condition will be automatically remedied after you stop and start the D2D services or perform the next backup.

■ **Restrictions for a Microsoft Exchange Server Backup**

– If your database is configured in one volume and the logs are configured in another volume and you select only one volume to back up, the Microsoft Exchange application backup is skipped for that particular database.

– Any database in a dismounted state is skipped from Microsoft Exchange application backup.

– If you install Microsoft Exchange after CA ARCserve D2D has been installed, and no backup has been performed yet, the Microsoft Exchange server may not be detected. As a result if you unselect a volume that has that application installed you may not get a warning notification that you are missing that application from the backup. This condition will be automatically remedied after you stop and start the D2D services or perform the next backup.

■ **Restrictions for VSS Writers**

CA ARCserve D2D uses all the VSS writers during backup to ensure consistent backups. The only exceptions are Microsoft SQL Server, Microsoft Exchange, and Hyper-V writers which are only included when they are properly licensed.

■ **VHD Restrictions for Compression and Encryption**

If both compression and encryption are disabled, then CA ARCserve D2D can only back up the files in .VHD format. CA ARCserve D2D cannot back up the files in .VHDX format.

Disks Supported by CA ARCserve D2D

Different types of disks are supported for CA ARCserve D2D backup source and destination disks. The following matrix lists the types of disks that are supported for each function.

Disk (Volume) Type	As Backup/File Copy Source	As Backup Destination
System Reserved Partition (Windows 2008 R2 Boot Manager)	Yes	Not applicable
Mounted Volume (No drive letter/NTFS formatted)	Yes	Yes
RAW Volume (No drive letter/Not formatted)	No	No
VHD Mounted Volume (Windows 2008 R2)	No	Yes
GPT Disk:		
GPT (GUID Partition Table) Data Disk	Yes	Yes
GPT (GUI Partition Table) Boot Disk	Yes – R16 Update 5 or higher required	Yes – Not recommended to put CA ARCserve D2D backups on boot disk
Dynamic Disk:		
■ No RAID	Yes	Yes
■ Software RAID (RAID-0 (Stripe)	Yes	Yes
■ Software RAID (RAID-1 (Mirrored)	Yes	Yes
■ Software RAID-5	No	Yes
Hardware RAID (include Embedded RAID)	Yes	Yes

Disk (Volume) Type	As Backup/File Copy Source	As Backup Destination
File System:		
■ FAT/FAT32	No	Yes*
■ NTFS	Yes	Yes
■ REFS	Backup: Yes File Copy: No	Yes
■ Deduplication-enabled NTFS	Backup: Yes File Copy: No	Yes
Shared Volume:		
■ Windows Shared Volume	No	Yes
■ Linux Shared Volume (samba shared)	No	Yes
Device Type:		
■ Removable Disk (Ex. Memory Stick, RDX)	No	Yes

Notes:

- Any non-removable disk that appears as a local drive to a server protected by CA ARCserve D2D will also be protected. This includes any Fibre Channel (FC) attached Storage Area Network (SAN) disks, or iSCSI disks. For iSCSI disks, CA ARCserve D2D can protect system and data disks; however, iSCSI system disks are not supported for BMR. Therefore, you should only use iSCSI for data disks.

- Supported file copy destinations include Amazon S3, Windows Azure, Eucalyptus-Walrus, and NTFS local or network volumes (could be on iSCSI).

* FAT/FAT32 cannot hold a single file larger than 4 GB. If after compression the CA ARCserve D2D file is larger than 4 GB (because the source is very large), the backup will fail.

Merge Job Guidelines

Review the following merge job guidelines:

- A merge job has the lowest priority. When a merge job is running, if any other job comes in, the merge job will be stopped. After that job completes, the merge will be resumed/restarted.

- You can manually stop/pause the merge job when it is running. If the merge job is manually stopped/paused, you must manually start/resume it from the CA ARCserve D2D home page. It will not be resumed/restarted automatically. As a result, the launching of all scheduled merge jobs will be suspended until you manually resume them.

- If the merge job is automatically stopped it will be automatically started when no other job is running.

- When a merge job is resumed, CA ARCserve D2D will know exactly where to start the process. If the merge job crashed or the machine was abruptly shut down, the job is resumed from the previous merge state.

  Example 1: When a merge job is started and crashed at 20%, the next time when the job is restarted, it will start to merge sessions again from 0%.

  Example 2: When a merge job is started and paused at 10%, the next time when the job is restarted, it will start to merge sessions from the 10% point. If it crashes at 20%, then the merge job will be restarted from the 10% point.

- When a merge job is resumed/restarted, if the list of sessions being merged is not changed since the time it was paused, the merge is resumed. This means it resumes and continues the merge from the point where it was paused.

- When a merge job is resumed/restarted, if the list of sessions being merged is changed since the time it was paused, the original merge is resumed without any added/modified sessions. This means the original merge resumes and continues the merge from the point where it was paused. When the original merge is completed, a new merge of the added/modified sessions will then be performed.

  Example: The original merge job contains 4 backup sessions and is paused when it completes 90% of the merge. When the merge is resumed, CA ARCserve D2D will complete the remaining 10% of the original merge and then a new merge will be performed for the added/modified sessions.

- The CA ARCserve D2D home page Job Monitor indicates the merge job status. It shows the percentage complete and displays more details if needed. For more information, see Job Monitor Panel (see page 52).

- If there are multiple sessions to be merged, they will be merged at once. The time spent for merging 10 sessions may be very close to the time spent for merging a single session.

  Example: If the merge job is stopped while merging session 1,2 and after some time when the merge job is resumed, it detects that session 3,4 should be merged as well. The merge job will merge 1,2,3,4 from the very beginning and the original merge process of 1,2 will be discarded.

Example: Set the retention count to 7. You have 10 recovery points (from session 1-10, 1 is the full backup and 2-9 are incremental backups). If the merge job starts, session 1,2,3 should be purged and session 4 will be the full session after the merge.

■ The merge process must be able to keep the recovery point in a consistent state. You can restore a file from any visible session even if the session is partially merged. If there is a session merge not completed, the merge job will run in the background to merge the session.

CA ARCserve D2D in a Microsoft Hyper-V Environment

CA ARCserve D2D provides both host-level and virtual machine (VM) level protection for Microsoft Hyper-V environments. The following scenarios describe situations that you can encounter and offer protection solutions using CA ARCserve D2D.

Note: Verify that you apply the appropriate license for each of these scenarios.

■ **Scenario 1 - You want to protect your Hyper-V host server:**

1. Install CA ARCserve D2D on the Hyper-V Host server.

2. Verify that you back up the system and boot volume (if you are choosing volume filtering).

3. If the Hyper-V host server goes down, follow the standard Bare Metal Recovery procedure in CA ARCserve D2D to recover your Hyper-V host server.

4. If you want to restore selected files, use the standard CA ARCserve D2D restore procedure.

■ **Scenario 2 - You want to protect your Hyper-V host server and the Virtual Machines which are hosted on that server:**

1. Install CA ARCserve D2D on the Hyper-V host server.

2. Verify that you back up the entire machine to provide complete protection of both the host server and VMs.

3. Submit the backup jobs.

4. To restore a VM from a CA ARCserve D2D backup, there are two possible solutions:

   a. **Restore the VM to original location:**

      – From the restore window in CA ARCserve D2D, select the VM files (".vhd", ".avhd", configuration files, and so on).

      – Select "Restore to original location" as the destination and select the "Overwrite existing files" option for resolving conflicts.

      – Submit the restore job.

      Note: The recommendation is to turn off the VM before submitting the restore job because if the older file is active, it will be overwritten by CA ARCserve D2D only after you reboot the Hyper-V host server to complete the restore process.

      – When the restore job has finished, open the Hyper-V Manager and start the VM.

      – If the VM is not yet registered in the Hyper-V Manager, create a VM. During the VM creation process, point the path of VM's configuration and vhd file to the same path of destination location where the restore was performed.

   b. **Restore the VM to alternate location on the same Hyper-V Host server:**

      – From the restore window in CA ARCserve D2D, select the VM files (".vhd", ".avhd", configuration files, and so on).

      – Select "Restore to alternate location" as the destination and provide a destination path.

      – Submit the restore job.

      – When the restore job has finished, open the Hyper-V Manager and create a VM. During VM creation process, point the path of VM's configuration and vhd file to the same path of destination location where the restore was performed.

      – When the VM is created, start the VM.

      Note: See the Microsoft Hyper-V documentation for more detailed information for restoring Hyper-V Virtual Machines.

■ **Scenario 3 - You want to protect your Hyper-V Virtual Machines:**

To protect your Hyper-V Virtual Machines (VM) using CA ARCserve D2D, there are two possible solutions:

a. **Install CA ARCserve D2D on the Hyper-V host server**

– Using the CA ARCserve D2D Backup Settings, select the volume where the VM files (".vhd", ".avhd", configuration files, and so on) are located.

– Submit a backup job.

– To restore a Hyper-V Virtual Machine from a CA ARCserve D2D backup, follow the steps for either of the restore solutions provided in Scenario 2.

b. **Install CA ARCserve D2D inside the Windows Virtual Machine**

Follow the standard backup and restore procedure to protect the VM, the same as a physical machine.

Note: For scenarios 2 and 3a, if you attached/mounted an iSCSI LUN directly inside the VM, the data inside the LUN is not backed up using CA ARCserve D2D Hyper-V host level backups. You can overcome this limitation by using the same approach as the "Install CA ARCserve D2D inside the Windows Virtual Machine" solution in scenario 3b.

Run a Backup Automatically

Automatic backup jobs are the same as manual backup jobs, except they are triggered at pre-configured days and times. You can configure automatic backup jobs using the Backup Schedule dialog. For more information, see Specify the Backup Schedule (see page 82).

CA Support:	How to: Perform an Automatic Backup – Configuring Your Backup Settings.
YouTube:	How to: Perform an Automatic Backup – Configuring Your Backup Settings.

The process for scheduling an automatic backup is as follows:

1. Based upon the configured time settings, CA ARCserve D2D triggers the launching of each type of scheduled backup job (Full, Incremental, and Verify).

2. Configuration settings specified in the Backup Settings dialogs are applied to the job.

3. If configured, an email notification is sent to the recipients informing them when the backup job is completed (or if a problem occurred that prevented the scheduled backup job from being completed).

Run a Backup Now

Typically, backups are performed automatically and are controlled by the schedule settings. However, there can be times when you have to perform an ad-hoc backup (Full, Incremental, or Verify) immediately.

An ad-hoc backup is need-based, rather than being scheduled in advance as part of a backup plan. For example, if you have a repeat schedule for Full, Incremental, and Verify backups and you want to make major changes to your machine, you should perform an immediate ad-hoc backup without waiting for the next scheduled backup to occur.

An ad-hoc backup also allows you to add a customized (unscheduled) recovery point so that you can roll back to this previous point in time if necessary. For example, if you install a patch or service pack and then discover that it adversely affects the performance of your machine, you may want to roll back to the ad-hoc backup session that does not include the patch or service pack.

CA Support: How to Perform a Manual (Ad-Hoc) Backup.

YouTube: How to Perform a Manual (Ad-Hoc) Backup.

Run a backup now

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), click Backup Now.

    The Run a backup now dialog opens.

2. Select the type of backup you want to perform.

    The available options are Full, Incremental, or Verify.

    Full Backup

    Initiates a Full Backup of your entire machine or the selected volumes.

Incremental Backup

Initiates an Incremental Backup of your machine. An Incremental Backup backs up only those blocks that have changed after the previous backup.

The advantages of Incremental Backups are that it is a fast backup and it produces a small backup image. This is the most optimal way to perform backups.

Verify Backup

Initiates a Verify Backup of your machine by examining the most recent backup of each individual block and comparing the content and information to the original source. This comparison verifies that the latest backed up blocks represent the corresponding information at the source. If the backup image for any block does not match the source, CA ARCserve D2D refreshes (resynchronizes) the backup of the block that does not match.

Advantages: A very small backup image is produced when compared to a Full Backup because only the changed blocks (blocks that do not match the last backup) are backed up.

Disadvantages: The backup time is slow because all of source disk blocks are compared with the blocks of the last backup..

Note: If you add a new volume to the backup source, the newly added volume is fully backed up regardless of the overall backup method selected.

3. If necessary, specify a backup name and click OK. If no backup name is specified, it is automatically named Customized Full/Incremental/Verify Backup by default.

A confirmation screen appears, and the selected type of backup is launched immediately.

All configuration settings specified in the Backup Settings dialogs are applied to the job.

Note: Only one job can be run at a time. If you manually attempt to launch a backup job now and another job is currently running, an alert message informs you that another job is running and request that you try again at a later time.

Note: If a custom (ad-hoc) backup job fails, no makeup job is created. A makeup job is only created for a failed scheduled job.

Perform File Copy to Disk/Cloud

CA ARCserve D2D provides the capability to copy/move files to and from the cloud or disk, which is based on your specified File Copy and retention policies. File Copy can be used for copying critical data to secondary locations and can also be used as an archiving solution. File Copy allows you to safely and securely delete the source data after it has been copied to an off-site or secondary storage repository.

The process of file copying CA ARCserve D2D backup information lets you specify the file copy source, destination, and corresponding policies for the type of File Copy job performed. The available types are File Copy and File Copy - Delete Source. The two processes are similar, with the exception that when you perform a File Copy - Delete Source job, the data is <u>moved</u> from the source to the destination (deleted from source location) and provides more available free space at your source. When you perform a File Copy job, the data is <u>copied</u> from the source to the destination (remains on source destination) and provides multiple stored versions. For more information about configuring the File Copy settings and polices, see Manage File Copy Settings (see page 89).

The File Copy process can only be launched automatically as scheduled. For more information about configuring the schedule settings, see Specify the File Copy Schedule (see page 107).

Note: For a compressed File Copy job, the activity log displays only the uncompressed size.

CA Support:	How to: Perform a File Copy Job
YouTube:	How to: Perform a File Copy Job

Perform a Restore

CA ARCserve D2D provides you with various tools and options that you can use to restore data. 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. Each restore job requires a source and destination.

Restore Considerations

Before you perform a CA ARCserve D2D restore, review the following restore considerations:

- **Restore Considerations for a remote destination**

  If all the drive letters (A - Z) are occupied, the restore to a remote path will not succeed because CA ARCserve D2D needs to use one drive letter to mount the remote destination path.

- **Restore Considerations for Hyper-V servers**

  On a Hyper-V server (even if you have the proper VM license), you must manually restore VHD files of VM and then re-register them with Hyper-V Manager.

  Note: After the VHDs are restored they are not directly registered with Hyper-V Manager. You can either attach them to existing VM or create a new VM and attach those to them.

- **Restore Considerations for a Microsoft SQL Server 2008 database with FILESTREAM data**

  Both the database and its related FILESTREAM BLOB data can be automatically backed-up by CA ARCserve D2D, but the FILESTREAM BLOB data cannot be restored automatically with the database. This is because FILESTREAM feature is not supported by the latest SQL Server Writer. As a result, when one database with FILESTREAM BLOB data is restored, just restoring the database is no longer enough, and the folder of FILESTREAM BLOB data also needs to be restored.

  Note: FILESTREAM is a feature introduced by Microsoft SQL Server 2008, which provides the capability of storing binary large object (BLOB) data (MP3, Word, Excel, PDF, etc.) in the NTFS file system, rather than in a database file.

- **Restore Considerations for session dismount time**

  When you browse the volume of one recovery point which does not have a catalog, the volume will be mounted. After the volume is mounted, the volume status is queried every 10 minutes to check if it is used. If it is not used, it will be dismounted.

  To change the default session dismount time of 10 minutes, modify the Registry Key, using the following information:

  - **Registry key path:** CA ARCserve D2D Installation path

  - **Registry key name:** SessionDismountTime

  - **Registry key type:** String

  - **Registry key value unit:** second

  For example: If you set the registry value to 60, the mounted volume status is queried every 60 seconds and if it is not used for the last 60 seconds, it will be dismounted.

Restore Methods

The goal of running a successful restore job is to identify quickly the data you need and to retrieve it from the appropriate backup location. CA ARCserve D2D provides various methods to identify and locate the backed up data and allow you to restore it. Regardless of the restore method you select, CA ARCserve D2D uses visual indicators (restore markers) of the objects that are or are not selected for restore. For more information, see Restore Markers (see page 145).

Note: CA ARCserve D2D only allows one restore job to run at the same time. If you attempt to launch manually a restore job now, and during that time another restore job is currently running an alert message opens. The alert message informs you that another job is running and requests that you try again at a later time.

Restore data

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog opens.

2. Select the type of restore you want to perform.

   The available options are Browse Recovery Points, Browse File Copies, Find Files/Folders to Restore, Recover VM, and Restore Exchange Mails.

   Note: Use the Browse Recovery Points if you want to restore any applications.

   Browse Recovery Points

   Lets you browse the available recovery points (successful backups) from a calendar view. The calendar dates that contain valid recovery points are highlighted in green. When you select a recovery date, all the associated recovery points for that date are displayed. You can then browse and select the backup content (including applications) to be restored.

   Browse File Copies

   Lets you browse the available File Copy locations (local disk/network drive or cloud) to locate the specific file or folder that is going to be restored.

   Find Files/Folders to Restore

   Lets you search for a file name pattern in a specific location and or the file version that is going to be restored.

   Recover VM

   Lets you browse the available virtual machine recovery points from a calendar view. The calendar dates that contain valid recovery points are highlighted in green. When you select a recovery date, all the associated virtual machine recovery points for that date are displayed. You can then browse and select the virtual machine content that is going to be restored.

   Restore Exchange Mails

   Lets you browse and select individual objects within an Exchange database to perform a granular-level restore.

Restore Markers

Regardless of which restore method you select, when you navigate to a specific volume, folder, or file to restore, each object displayed in the restore window has a green or gray box to its left called a marker. These markers are visual indicators of the objects that are or are not selected for restore.

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.
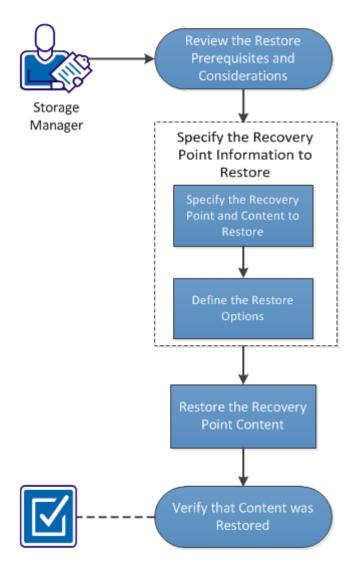
■ If all the markers at the lower levels are completely filled, then the marker at the higher level is also automatically completely filled.

■ 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.

How to Restore From a Recovery Point

Each time CA ARCserve D2D performs a successful backup, a point-in-time snapshot image of your backup is created (recovery point). This collection of recovery points allows you to locate and specify exactly which backup image you want to restore. If at some later time, you suspect any of the backed up information is missing, corrupted, or not reliable, you can then locate and restore from a previous known good version.

The following diagram illustrates the process to restore from a recovery point:

How to Restore from a Recovery Point

Storage Manager

Review the Restore Prerequisites and Considerations

Specify the Recovery Point Information to Restore

Specify the Recovery Point and Content to Restore

Define the Restore Options

Restore the Recovery Point Content

Verify that Content was Restored

Perform the following tasks to restore from a recovery point:

1. Review the Restore Prerequisites and Considerations (see page 148)
2. Specify the Recovery Point Information to Restore (see page 150)
    a. Specify the Recovery Point and Content to Restore (see page 150)
    b. Define the Restore Options (see page 152)
3. Restore the Recovery Point Content (see page 155)
4. Verify that Content was Restored (see page 156)

SUPPLEMENTAL VIDEO

This procedure contains a supplemental instructional video. Select either CA Support or YouTube as the source for viewing this video. The versions of the video from CA Support and YouTube are identical, and only the viewing source is different.

CA Support: How to Restore from a Recovery Point

YouTube: How to Restore from a Recovery Point

Review the Restore Prerequisites and Considerations

Verify that the following prerequisites exist before performing a restore:

- You have at least one recovery point available to restore.

- You have a valid and accessible recovery point destination to restore the recovery point content from.

- You have a valid and accessible target location to restore the recovery point content to.

Review the following restore considerations:

- CA ARCserve D2D only allows one restore job to run at the same time. If you attempt to launch a restore job manually, while another restore job is running, an alert message opens informing you another job is running and requests you to try again later.

- If the restore is to a remote destination and if all the drive letters (A - Z) are occupied, the restore to a remote path will not succeed. CA ARCserve D2D needs to use one drive letter to mount the remote destination path.

- (Optional) Understand how the restore process works. For more information, see How File Level Restores Work (see page 28).

- When you attempt to restore an optimized backup session to a non-empty volume (unoptimized restore), the restore job may take more time than the estimated time displayed in the job monitor. The amount of data that is processed and the elapsed time may increase based on the data that is optimized on the volume.

  Example:

  The backup volume size is 100 GB and after optimization the volume size is reduced to 50 GB.
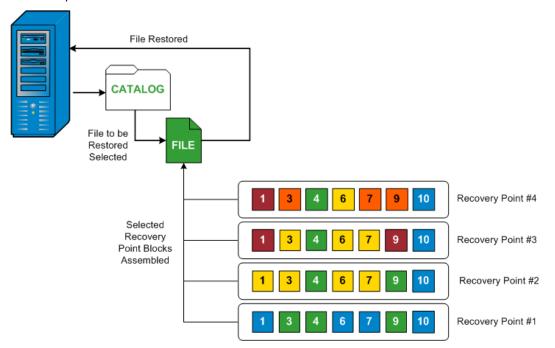
  When you perform an unoptimized restore of this volume the restore job monitor displays 100% after restoring 50 GB, but it will take more time to restore the entire 100 GB.

- The following Activity log message will be displayed when restoring a catalog enabled session or a catalog-less session, and the file has attribute FILE_ATTRIBUTE_SYSTEM (for example, System Volume Information or Recycle Bin folder) or it is under the %SystemDrive%\Windows directory:

  "System files were skipped. If necessary, you can use the Bare Metal Recovery (BMR) option to restore them."

How File Level Restores Work

During a block-level backup, each backed up file is made up of a collection of blocks that define that particular file. A catalog file is created containing a list of the backed up files, along with the individual blocks that were used for each file and the available recovery points for these files. When you need to restore a particular file, you can search your backup and select the file you want to restore and the recovery point you want to restore from. CA ARCserve D2D then collects the version of the blocks that were used for the recovery point of the specified file, and reassembles and restores the file.

The following flow diagram shows the process of how CA ARCserve D2D restores a specific file.

Specify the Recovery Point Information to Restore

CA ARCserve D2D provides you with an option to restore data from a recovery point. The goal of running a successful restore job is to identify quickly the data you need and to retrieve it from the appropriate backup location. Each restore job requires a source and destination.

The process involved in restoring from a recovery point is as follows:

1. Specify the Recovery Point and Content to Restore (see page 150)

2. Define the Restore Options (see page 152)

Specify the Recovery Point and Content to Restore

Use the Browse Recovery Points option to restore from a recovery point. When you select a recovery date, all the associated recovery points for that date are displayed. You can then browse and select the backup content (including applications) to be restored.

Follow these steps:

1. On the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog opens.

2. Click the Browse Recovery Points option.

   The Browse Recovery Points dialog opens.

3. Specify or browse to the location where your backup images are stored and select the appropriate backup source.

   You can click the green arrow button to verify the connection to the specified location. If necessary, enter the Username and Password credentials to gain access to that source location.

   The calendar view appears and all the dates containing recovery points for the specified backup source are highlighted in green.

4. Select the calendar date for the backup image to restore.

   The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed (Full, Incremental, or Verify), and the name of the backup.

5. Select a recovery point to restore.

   The backup content (including any applications) for the selected recovery point displays.

   Note: A clock icon with a lock symbol indicates the recovery point contains encrypted information and may require a password for restore.

6. Select the content to restore.

   ■ For a volume-level restore, you can specify to restore the entire volume or selected files/folders within the volume.

   ■ For an application-level restore, you can specify to restore the entire application or selected components, databases, instances, and so on, within the application.

7. Click Next.

   The Restore Options dialog Opens.

   The recovery point and content to restore is specified.

Define the Restore Options

After you specify a recovery point and content to restore, define the copy options for the selected recovery point.

Follow these steps:

1. On the Restore Options dialog, select the restore destination.

The available destination options are:

Restore to Original Location

Restores to the original location from where the backup image was captured.

Restore to

Restores to the specified location. You can click the green arrow button to verify the connection to the specified location. If necessary, enter the Username and Password credentials to gain access to that location.

2. Specify the Resolving Conflicts option that CA ARCserve D2D performs if conflicts are encountered during the restore process.

The available options are:

Overwrite existing files

Overwrites (replaces) any existing files, which are at the restore destination. All objects are restored from the backup files regardless of their current presence on your computer.

Replace active files

Replaces any active files upon reboot. If during the restore attempt CA ARCserve D2D discovers that the existing file is currently in use or being accessed, it will not immediately replace that file, but instead to avoid any problems will delay the replacement of the active files until the next time the machine is rebooted. (The restore occurs immediately, but the replacement of any active files is done during the next reboot).

This option is only available if you select the "Overwrite existing files" option.

Note: If you do not select this option, any active file is skipped from the restore.

Rename files

Creates a new file if the file name already exists. Selecting this option copies the source file to the destination with the same filename but a different extension. Data is then restored to the new file.

Skip existing files

Skips over and not overwrite (replace) any existing files that are located at the restore destination. Only objects that are not currently existing on your machine are restored from the backup files.

Default: Skip existing files.

3. Specify the Directory Structure to create a root directory during restore.

   Create root directory

   Specifies that if a root directory structure exists in the captured backup image, CA ARCserve D2D recreates that same root directory structure on the restore destination path.

   With this option not selected, the file or folder is restored directly to the destination folder.

   For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt" and "C:\Folder1\SubFolder2\B.txt" and during the restore you specified to the restore destination as "D:\Restore".

   - If you select to restore the "A.txt" and "B.txt" files individually, the destination for the restored files will be "D:\Restore\A.txt" and "D:\Restore\B.txt" (the root directory above the specified file level will not be recreated).

   - If you select to restore from the "SubFolder2" level, the destination for the restored files will be "D:\Restore\SubFolder2\A.txt" and "D:\Restore\SubFolder2\B.txt" (the root directory above the specified folder level will not be recreated).

   With this option selected, the entire root directory path for the files/folders (including the volume name) is recreated to the destination folder. If the files/folders to be restored are from the same volume name, then the destination root directory path does not include that volume name. However, if the files/folders to be restored are from different volume names, then the destination root directory path does include the volume name.

   For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", and also E:\Folder3\SubFolder4\C.txt" and during the restore you specified to the restore destination as "D:\Restore".

   - If you select to restore just the "A.txt" file, the destination for the restored file will be "D:\Restore\ Folder1\SubFolder2\A.txt" (the entire root directory without the volume name will be recreated).

   - If you select to restore both the "A.txt" and "C.txt" files, the destination for the restored files will be "D:\Restore\C\Folder1\SubFolder2\A.txt" and "D:\Restore\E\Folder3\SubFolder4\C.txt" (the entire root directory with the volume name will be recreated).

4. If necessary, specify the Backup Encryption Password, if the data you are trying to restore is encrypted.

   A password is not required if you are attempting to restore from the same CA ARCserve D2D computer from where the encrypted backup was performed. However, if you are attempting to restore from a different CA ARCserve D2D computer, a password is required.

   Note: A clock icon with a lock symbol indicates the recovery point contains encrypted information and may require a password for restore.

5. Click Next.

   The Restore Summary dialog opens.

The restore options are defined to restore from a recovery point.

Restore the Recovery Point Content

After you define the restore options, verify that your settings are correct and confirm the restore process. Restore Summary helps you to review all the restore options that you defined and modify them if necessary.

Follow these steps:

1. On the Restore Summary dialog, review the displayed information to verify that all the restore options and settings are correct.

- If the summary information is incorrect, click Previous and go back to the applicable dialog to change the incorrect setting.

- If the summary information is correct, click Finish to launch the restore process.

The recovery point content is restored.

Verify that Content was Restored

After the completion of the restore process, verify that content was restored to the specified destination.

Follow these steps:

1. Navigate to the CA ARCserve D2D restore destination you specified.

    A list of folders appears.

2. Locate the file to which you have restored the content.

    For example, If you select to restore the "A.txt'' file to the restore destination as "D:\Restore, then navigate to the following location:

    D:\Restore\A.txt.

3. Verify the content to confirm the restore job.

The restored content is successfully verified.

How to Restore From a File Copy

Each time CA ARCserve D2D performs a successful file copy job, it backs up all files that have changed since the last successful file copy job. This restore method allows you to browse the file copied data and specify exactly which file you want to restore.

The following diagram illustrates the process to restore from a file copy:

How to Restore from a File Copy

Storage
Manager

Review the Restore
Prerequisites and
Considerations

Specify the File Copy
Information to Restore

Specify the File Copy
and Content to Restore

Cloud

Local or
Network
Drive

Specify Cloud
Configuration
For Restore

Define the Restore
Options

Restore the File Copy
Content

Verify that Content was
Restored

Perform the following tasks to restore from a File Copy:

1. Review the Restore Prerequisites and Considerations (see page 158)

2. Specify the File Copy Information to Restore (see page 159)

   a. Specify the File Copy and Content to Restore (see page 159)

      ■ Specify Cloud Configuration for Restore (see page 162)

   b. Define the Restore Options (see page 164)

3. Restore the Recovery Point Content (see page 167)

4. Verify that Content was Restored (see page 168)

SUPPLEMENTAL VIDEO

This procedure contains a supplemental instructional video. Select either CA Support or YouTube as the source for viewing this video. The versions of the video from CA Support and YouTube are identical, and only the viewing source is different.

CA Support: How to Restore from a File Copy

YouTube: How to Restore from a File Copy

Review the Restore Prerequisites and Considerations

Verify that the following prerequisites exist before performing a restore:

■ You have at least one file copy available to restore.

■ You have a valid and accessible file copy destination to restore the file copy content from.

■ You have a valid and accessible target location to restore the file copy content to.

Review the following restore considerations:

■ CA ARCserve D2D only allows one restore job to run at the same time. If you attempt to launch a restore job manually, while another restore job is running, an alert message opens informing you another job is running and requests you to try again later.

■ If the restore is to a remote destination and if all the drive letters (A - Z) are occupied, the restore to a remote path will not succeed. CA ARCserve D2D needs to use one drive letter to mount the remote destination path.

■ (Optional) Understand how the restore process works. For more information, see How File Level Restores Work (see page 159).

How File Level Restores Work

During a File Copy, each backed up file is made up of a collection of blocks that define that particular file. A catalog file is created for every version of the backed up file, along with the individual blocks that were used for these files. When you need to restore a particular file, you can browse and select the file you want to restore and the file copy versions you want to restore from. CA ARCserve D2D then collects the version of the blocks that were used for the file copy of the specified file, which reassembles and restores the file.

The following flow diagram shows the process of how CA ARCserve D2D restores a specific file.

File Restored

CATALOG

File to be Restored Selected

FILE

Selected File Copy Blocks Assembled

1 2 3 4 5 6 7 File Copy (Version 4)

1 2 3 4 5 6 7 File Copy (Version 3)

1 2 3 4 5 6 7 File Copy (Version 2)

1 2 3 4 5 6 7 File Copy (Version 1)

Specify the File Copy Information to Restore

CA ARCserve D2D provides you with an option to restore data from a file copy. The goal of running a successful restore job is to identify quickly the data you need and to retrieve it from the appropriate backup location. Each restore job requires a source and destination.

The process involved in restoring from a file copy is as follows:

1. Specify the File Copy and Content to Restore

2. Define the Restore Options (see page 164)

Specify the File Copy and Content to Restore

Use the Browse File Copies option to restore from a file copy. This restore method allows you to browse the file copied data and specify exactly which file you want to restore.

Follow these steps:

1. On the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

    The restore methods selection dialog opens.

2. Click the Browse File Copies option.

    The Restore dialog opens. The destination that is currently showing in the Restore From field is the configured default File Copy destination.

3. If necessary, you can click Change to browse to an alternate location where your file copy images are stored.

    A dialog opens displaying the available alternate destination options.

Local or network drive

The Select a Backup Location dialog opens, allowing you to browse to and select an alternate local or network drive location.

Cloud

The Cloud Configuration dialog opens, allowing you to access and select an alternate cloud location. For more information about this dialog, see Specify Cloud Configuration for Restore. (see page 162)

4. Regardless of whether you selected to restore from Local or network drive or from Cloud, when you change the destination to an alternate location a pop-up dialog will appear, asking you if you want to perform a new catalog synchronization or read from the existing catalog.

If it is the first time you are performing a catalog synchronization, the "Browse Existing" button will be disabled because there is no existing file copy catalog locally.

If a catalog synchronization has been previously performed, this dialog will display details about the last time the catalog was synchronized from this destination. If there were more file copy jobs run since that displayed time, your catalog may not be currently synchronized and you can select the "Sync" option to ensure your file copy catalog is up-to-date.

a. Click "Sync" to download the file copy catalog from the specified file copy destination to your local machine to provide faster browsing.

b. Click "Browse Existing" to use the file copy catalog that is available locally and not download/sync it again.

5. On the left pane, specify the file copy data to be restored. You can select file copied folders or files to be restored.

When you select an individual file to be restored, all file copied versions of that file are displayed in the right pane. If multiple versions are available, you must select which file copied version you want to restore.

6. After selecting the file copied folder or file version to restore, click Next.

The Restore Options dialog opens.

The File Copy and Content to restore is specified.

Specify Cloud Configuration for Restore

Note: The following procedure only applies if you are restoring a file/folder from a file copy cloud location.

From the Browse File Copies option or the Find Files/Folders to Restore option, click the Configure button to display the Cloud Configuration dialog.

Follow these steps:

1. From the Cloud Configuration dialog, use the drop-down menu to select which cloud vendor type you want to restore from. The available options are Amazon S3, Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus. (Amazon S3 is the default vendor). For more information about Fujitsu Cloud (Windows Azure), see the Overview and Registration.

    Note: If you are using Eucalyptus-Walrus as your file copy cloud vendor, you will not be able to copy files whose entire path length is greater than 170 characters.

2. Specify the Configuration Options.

    The configuration options for each cloud vendor are similar (with some different terminology), and any differences are described.

    a. Specify the Connection Settings:

        Vendor URL

            Identifies the URL address of the cloud provider.

            (For Amazon S3, Windows Azure, and Fujitsu Cloud (Windows Azure), the Vendor URL is automatically pre-populated. For Eucalyptus-Walrus, the Vendor URL must be manually entered using the specified format).

        Access Key ID/Account Name/Query ID

            Identifies the user who is requesting access this location.

            (For this field, Amazon S3 uses Access Key ID, Windows Azure and Fujitsu Cloud (Windows Azure) use Account Name, and Eucalyptus-Walrus uses Query ID).

        Secret Access Key/Secret Key

            Because your Access Key is not encrypted, this Secret Access Key is a password that is used to verify the authenticity of the request to access this location.

            Important! This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials in a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

            (For this field, Amazon S3 uses Secret Access Key. Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus use Secret Key).

Enable Proxy

If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections. You can also select this option if your proxy server requires authentication. You then must provide the corresponding authentication information (Username and Password) that is required to use the proxy server.

(Proxy capability is not available for Eucalyptus-Walrus).

b. Specify the Advanced Settings:

Bucket Name/Container

All files and folders moved or copied to the cloud vendor are stored and organized in your buckets (or containers). Buckets are like a container for your files and are used to group and organize objects together. Every object stored at the cloud vendor is placed in a bucket.

Select a bucket name from the drop-down list. If necessary, you can click the refresh button to update the list of available buckets.

(For this field, Amazon S3 and Eucalyptus-Walrus use Bucket Name. Windows Azure and Fujitsu Cloud (Windows Azure) use Container).

Bucket Region

For Amazon S3 only, the available region for the specified bucket is displayed in this field.

(For Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus, the region is not displayed).

Enable Reduced Redundancy Storage

For Amazon S3 only, this option lets you select to enable Reduced Redundancy Storage (RRS). RRS is a storage option within Amazon S3 that helps you reduce cost by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. Both the standard and reduced redundancy storage options store data in multiple facilities and on multiple devices, but with RRS the data is replicated fewer times, so the cost is less. You should expect the same latency and throughput using either the Amazon S3 standard storage or RRS. By default this option is not selected (Amazon S3 uses the standard storage option).

3. Click Test Connection to verify the connection to the specified cloud location.

4. Click OK to exit the Cloud Configuration dialog.

Define the Restore Options

After you specify the file copy information to restore, define the copy options for the selected file copy and content.

Follow these steps:

1. On the Restore Options dialog, select the restore destination.

   The available destination options are:

   Restore to Original Location

   Restores to the original location from where the backup image was captured.

   Restore to

   Restores to the specified location. You can click the green arrow button to verify the connection to the specified location. If necessary, enter the Username and Password credentials to gain access to that location.

2. Specify the Resolving Conflicts option that CA ARCserve D2D performs if conflicts are encountered during the restore process.

   The available options are:

   Overwrite existing files

   Overwrites (replaces) any existing files, which are at the restore destination. All objects are restored from the backup files regardless of their current presence on your computer.

Replace active files

Replaces any active files upon reboot. If during the restore attempt CA ARCserve D2D discovers that the existing file is currently in use or being accessed, it will not immediately replace that file, but instead to avoid any problems will delay the replacement of the active files until the next time the machine is rebooted. (The restore occurs immediately, but the replacement of any active files is done during the next reboot).

This option is only available if you select the "Overwrite existing files" option.

Note: If you do not select this option, any active file is skipped from the restore.

Rename files

Creates a new file if the file name already exists. Selecting this option copies the source file to the destination with the same filename but a different extension. Data is then restored to the new file.

Skip existing files

Skips over and not overwrite (replace) any existing files that are located at the restore destination. Only objects that are not currently existing on your machine are restored from the backup files.

Default: Skip existing files.

3. Specify the Directory Structure to create a root directory during restore.

Create root directory

Specifies that if a root directory structure exists in the captured backup image, CA ARCserve D2D recreates that same root directory structure on the restore destination path.

With this option not selected, the file or folder is restored directly to the destination folder.

For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt" and "C:\Folder1\SubFolder2\B.txt" and during the restore you specified to the restore destination as "D:\Restore".

■ If you select to restore the "A.txt" and "B.txt" files individually, the destination for the restored files will be "D:\Restore\A.txt" and "D:\Restore\B.txt" (the root directory above the specified file level will not be recreated).

■ If you select to restore from the "SubFolder2" level, the destination for the restored files will be "D:\Restore\SubFolder2\A.txt" and "D:\Restore\SubFolder2\B.txt" (the root directory above the specified folder level will not be recreated).

With this option selected, the entire root directory path for the files/folders (including the volume name) is recreated to the destination folder. If the files/folders to be restored are from the same volume name, then the destination root directory path does not include that volume name. However, if the files/folders to be restored are from different volume names, then the destination root directory path does include the volume name.

For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", and also E:\Folder3\SubFolder4\C.txt" and during the restore you specified to the restore destination as "D:\Restore".

- If you select to restore just the "A.txt" file, the destination for the restored file will be "D:\Restore\ Folder1\SubFolder2\A.txt" (the entire root directory without the volume name will be recreated).

- If you select to restore both the "A.txt" and "C.txt" files, the destination for the restored files will be "D:\Restore\C\Folder1\SubFolder2\A.txt" and "D:\Restore\E\Folder3\SubFolder4\C.txt" (the entire root directory with the volume name will be recreated).

4. The Encryption Password for file copy destination is loaded automatically. If you select an alternate destination for the restore, you will need to enter the encryption password manually.

5. Click Next.

The Restore Summary dialog opens.

The restore options are defined to restore from a file copy.

Restore the File Copy Content

After you define the restore options, verify that your settings are correct and confirm the restore process. Restore Summary helps you to review all the restore options that you defined and modify them if necessary.

Follow these steps:

1. On the Restore Summary dialog, review the displayed information to verify that all the restore options and settings are correct.

- If the summary information is incorrect, click Previous and go back to the applicable dialog to change the incorrect setting.

- If the summary information is correct, click Finish to launch the restore process.

The file copy content is restored.

Verify that Content was Restored

After the completion of the restore process, verify that content was restored to the specified destination.

Follow these steps:

1. Navigate to the CA ARCserve D2D restore destination you specified.

A list of folders appears.

2. Locate the file to which you have restored the content.

For example, If you select to restore the "A.txt'' file to the restore destination as "D:\Restore, then navigate to the following location:

D:\Restore\A.txt.

3. Verify the content to confirm the restore job.

The restored content is successfully verified.

How to Restore Files/Folders

Each time CA ARCserve D2D performs a successful backup, all backed up files/folders are included in the snapshot image of your backup. This restore method allows you to specify exactly which file/folder you want to restore.

The following diagram illustrates the process to restore specific files/folders:

How to Restore Files/Folders

Perform the following tasks to restore files/folders:

1. Review the Restore Prerequisites and Considerations (see page 171)

2. Specify the File/Folder Information to Restore (see page 173)

   a. Specify the File/Folder Location (see page 173)

      ■ Specify Cloud Configuration for Restore (see page 162)

   b. Specify the File/Folder to Restore (see page 179)

   c. Define the Restore Options (see page 180)

3. Restore the File/Folder (see page 183)

4. Verify that the File/Folder was Restored (see page 184)

SUPPLEMENTAL VIDEO

This procedure contains a supplemental instructional video. Select either CA Support or YouTube as the source for viewing this video. The versions of the video from CA Support and YouTube are identical, and only the viewing source is different.

CA Support: How to Restore Files/Folders

YouTube: How to Restore Files/Folders

Review the Restore Prerequisites and Considerations

Verify that the following prerequisites exist before performing a restore:

■ You have at least one backup or file copy version available to restore.

■ You have a valid and accessible backup or file copy destination to restore the backup or file copy content from.

■ You have a valid and accessible target location to restore the backup or file copy content to.

Review the following restore considerations:

■ CA ARCserve D2D only allows one restore job to run at the same time. If you attempt to launch a restore job manually, while another restore job is running, an alert message opens informing you another job is running and requests you to try again later.

■ If the restore is to a remote destination and if all the drive letters (A - Z) are occupied, the restore to a remote path will not succeed. CA ARCserve D2D needs to use one drive letter to mount the remote destination path.

■ (Optional) Understand how the restore process works. For more information, see How File Level Restores Work (see page 28).

Note: The process for restoring from a file copy location is similar to restoring from a backup location.

How File Level Restores Work

During a block-level backup, each backed up file is made up of a collection of blocks that define that particular file. A catalog file is created containing a list of the backed up files, along with the individual blocks that were used for each file and the available recovery points for these files. When you need to restore a particular file, you can search your backup and select the file you want to restore and the recovery point you want to restore from. CA ARCserve D2D then collects the version of the blocks that were used for the recovery point of the specified file, and reassembles and restores the file.

The following flow diagram shows the process of how CA ARCserve D2D restores a specific file.

Specify the File/Folder Information to Restore

CA ARCserve D2D provides you with an option to find and restore a specific file or folder. The goal of running a successful restore job is to identify quickly the data you need and to retrieve it from the appropriate backup location. Each restore job requires a source and destination.

The process involved in restoring by find files/folders is as follows:

1. Specify the File/Folder Location (see page 173)

   ■   Specify Cloud Configuration for Restore (see page 162)

2. Specify the File/Folder to Restore (see page 179)

3. Define the Restore Options (see page 180)

Specify the File/Folder Location

Use the Find Files/Folders option to restore files and folders. This restore method allows you to specify exactly which file or folder you want to restore.

Follow these steps:

1. On the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog opens.

2. Click the Find Files/Folders to Restore option.

   The Find Files/Folders to Restore dialog opens.

3. Specify where to search (Backup Location and/or File Copy Location).

   Note: By default, the Backup Location and File Copy Location fields display the corresponding path used for the most recent backup/file copy destinations.

   a. Select Backup Location and then either specify or browse to the location where your backup images are stored.

      You can click green arrow validate icon to verify proper access to the source location.

   b. Select File Copy Location or click the Change button to change the search location to the destination where your file copy images are stored.

      If you click the Change button, the Destination dialog opens and you can select Local or network drive or Cloud.

   ■ If you select Local or network drive, you can either specify a location or browse to the location where your file copy images are stored.

      You can click green arrow validate icon to verify proper access to the source location.

   ■ If you select Cloud, you can either specify a cloud location or click the Configure button to display the Cloud Configuration dialog. For more information, see Specify Cloud Configuration for Restore (see page 162).

4. Regardless of whether you selected to restore from Local or network drive or from Cloud, when you change the destination to an alternate location a pop-up dialog will appear, asking you if you want to perform a new catalog synchronization or read from the existing catalog.

   If it is the first time you are performing a catalog synchronization, the "Browse Existing" button will be disabled because there is no existing file copy catalog locally.

If a catalog synchronization has been previously performed, this dialog will display details about the last time the catalog was synchronized from this destination. If there were more file copy jobs run since that displayed time, your catalog may not be currently synchronized and you can select the "Sync" option to ensure your file copy catalog is up-to-date.

a. Click "Sync" to download the file copy catalog from the specified file copy destination to your local machine to provide faster browsing.

b. Click "Browse Existing" to use the file copy catalog that is available locally and not download/sync it again.

The Backup or File Copy location is specified.

Specify Cloud Configuration for Restore

Note: The following procedure only applies if you are restoring a file/folder from a file copy cloud location.

From the Browse File Copies option or the Find Files/Folders to Restore option, click the Configure button to display the Cloud Configuration dialog.

Perform a Restore

Follow these steps:

1. From the Cloud Configuration dialog, use the drop-down menu to select which cloud vendor type you want to restore from. The available options are Amazon S3, Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus. (Amazon S3 is the default vendor). For more information about Fujitsu Cloud (Windows Azure), see the Overview and Registration.

   Note: If you are using Eucalyptus-Walrus as your file copy cloud vendor, you will not be able to copy files whose entire path length is greater than 170 characters.

2. Specify the Configuration Options.

   The configuration options for each cloud vendor are similar (with some different terminology), and any differences are described.

   a. Specify the Connection Settings:

      Vendor URL

      Identifies the URL address of the cloud provider.

      (For Amazon S3, Windows Azure, and Fujitsu Cloud (Windows Azure), the Vendor URL is automatically pre-populated. For Eucalyptus-Walrus, the Vendor URL must be manually entered using the specified format).

      Access Key ID/Account Name/Query ID

      Identifies the user who is requesting access this location.

      (For this field, Amazon S3 uses Access Key ID, Windows Azure and Fujitsu Cloud (Windows Azure) use Account Name, and Eucalyptus-Walrus uses Query ID).

      Secret Access Key/Secret Key

      Because your Access Key is not encrypted, this Secret Access Key is a password that is used to verify the authenticity of the request to access this location.

      Important! This Secret Access Key is crucial for maintaining the security of your accounts. You should keep your keys and your account credentials in a secure location. Do not embed your Secret Access Key in a web page or other publicly accessible source code and do not transmit it over insecure channels.

      (For this field, Amazon S3 uses Secret Access Key. Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus use Secret Key).

178 User Guide

Enable Proxy

If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections. You can also select this option if your proxy server requires authentication. You then must provide the corresponding authentication information (Username and Password) that is required to use the proxy server.

(Proxy capability is not available for Eucalyptus-Walrus).

b. Specify the Advanced Settings:

Bucket Name/Container

All files and folders moved or copied to the cloud vendor are stored and organized in your buckets (or containers). Buckets are like a container for your files and are used to group and organize objects together. Every object stored at the cloud vendor is placed in a bucket.

Select a bucket name from the drop-down list. If necessary, you can click the refresh button to update the list of available buckets.

(For this field, Amazon S3 and Eucalyptus-Walrus use Bucket Name. Windows Azure and Fujitsu Cloud (Windows Azure) use Container).

Bucket Region

For Amazon S3 only, the available region for the specified bucket is displayed in this field.

(For Windows Azure, Fujitsu Cloud (Windows Azure), and Eucalyptus-Walrus, the region is not displayed).

Enable Reduced Redundancy Storage

For Amazon S3 only, this option lets you select to enable Reduced Redundancy Storage (RRS). RRS is a storage option within Amazon S3 that helps you reduce cost by storing non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage. Both the standard and reduced redundancy storage options store data in multiple facilities and on multiple devices, but with RRS the data is replicated fewer times, so the cost is less. You should expect the same latency and throughput using either the Amazon S3 standard storage or RRS. By default this option is not selected (Amazon S3 uses the standard storage option).

3. Click Test Connection to verify the connection to the specified cloud location.

4. Click OK to exit the Cloud Configuration dialog.

Specify the File/Folder to Restore

After you specify the backup or file copy location, search for the file or folder name to restore. If a file has multiple file copy versions, all versions are listed and sorted by date (with the most recent listed first).

Follow these steps:

1. From the Find Files/Folders to Restore dialog, specify what to search for (file or folder name to restore).

    Note: The File Name field supports full name searching and wildcard searching. 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 File Name field.

    The wildcard characters supported for the file or folder name are as follows:

    - Use the asterisk to substitute zero or more characters in a file or folder name.

    - Use the question mark to substitute a single character in a file or folder name.

    For example, if you specify *.txt, all files with a .txt file extension appear in the search results.

2. (Optional) Specify a path to further filter your search and select whether to include or not include any subdirectories.

3. Click Find to launch search results.

    The search results are displayed. If the searched file has multiple file copy versions, all versions will be listed, sorted by date (with the most recent listed first). It also indicates if the searched file was backed up or file copied.

4. Select the version (occurrence) of the file/folder that you want to restore and click Next.

    The Restore Options dialog opens.

    The file/folder name to be restored is specified.

Define the Restore Options

After you specify the file or folder to restore, define the restore options for the selected file or folder.

Follow these steps:

1. From the Restore Options dialog, select the restore destination.

The available destination options are:

Restore to Original Location

Restores to the original location from where the backup image was captured.

Restore to

Restores to the specified location. You can click the green arrow button to verify the connection to the specified location. If necessary, enter the Username and Password credentials to gain access to that location.

2. Specify the Resolving Conflicts option that CA ARCserve D2D performs if conflicts are encountered during the restore process.

The available options are:

Overwrite existing files

Overwrites (replaces) any existing files, which are at the restore destination. All objects are restored from the backup files regardless of their current presence on your computer.

Replace active files

Replaces any active files upon reboot. If during the restore attempt CA ARCserve D2D discovers that the existing file is currently in use or being accessed, it will not immediately replace that file, but instead to avoid any problems will delay the replacement of the active files until the next time the machine is rebooted. (The restore occurs immediately, but the replacement of any active files is done during the next reboot).

This option is only available if you select the "Overwrite existing files" option.

Note: If you do not select this option, any active file is skipped from the restore.

Rename files

Creates a new file if the file name already exists. Selecting this option copies the source file to the destination with the same filename but a different extension. Data is then restored to the new file.

Skip existing files

Skips over and not overwrite (replace) any existing files that are located at the restore destination. Only objects that are not currently existing on your machine are restored from the backup files.

Default: Skip existing files.

3. Specify the Directory Structure to create a root directory during restore.

Create root directory

Specifies that if a root directory structure exists in the captured backup image, CA ARCserve D2D recreates that same root directory structure on the restore destination path.

With this option not selected, the file or folder is restored directly to the destination folder.

For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt" and "C:\Folder1\SubFolder2\B.txt" and during the restore you specified to the restore destination as "D:\Restore".

■   If you select to restore the "A.txt" and "B.txt" files individually, the destination for the restored files will be "D:\Restore\A.txt" and "D:\Restore\B.txt" (the root directory above the specified file level will not be recreated).

■   If you select to restore from the "SubFolder2" level, the destination for the restored files will be "D:\Restore\SubFolder2\A.txt" and "D:\Restore\SubFolder2\B.txt" (the root directory above the specified folder level will not be recreated).

With this option selected, the entire root directory path for the files/folders (including the volume name) is recreated to the destination folder. If the files/folders to be restored are from the same volume name, then the destination root directory path does not include that volume name. However, if the files/folders to be restored are from different volume names, then the destination root directory path does include the volume name.

For example, if during the backup you captured the files "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", and also E:\Folder3\SubFolder4\C.txt" and during the restore you specified to the restore destination as "D:\Restore".

■ If you select to restore just the "A.txt" file, the destination for the restored file will be "D:\Restore\ Folder1\SubFolder2\A.txt" (the entire root directory without the volume name will be recreated).

■ If you select to restore both the "A.txt" and "C.txt" files, the destination for the restored files will be "D:\Restore\C\Folder1\SubFolder2\A.txt" and "D:\Restore\E\Folder3\SubFolder4\C.txt" (the entire root directory with the volume name will be recreated).

4. The Encryption Password for file copy destination is loaded automatically. If you select an alternate destination for the restore, you will need to enter the password manually.

5. Click Next.

The Restore Summary dialog opens.

The restore options are defined to restore the specified file/folder.

Restore the File/Folder

The Restore Summary helps you to review all the restore options that you previously defined and lets you modify them if necessary.

Follow these steps:

1. From the Restore Summary dialog, review the displayed information to verify that all the restore options and settings are correct.

- If the summary information is incorrect, click Previous and go back to the applicable dialog to change the incorrect setting.
- If the summary information is correct, click Finish to launch the restore process.

The specified file/folder is restored.

Verify that the File/Folder was Restored

After the completion of the restore process, verify that the file/folder was restored to the specified destination.

Follow these steps:

1. Navigate to the CA ARCserve D2D restore destination you specified.

   A list of folders appears.

2. Locate the file to which you have restored the content.

   For example, If you select to restore the "A.txt'' file to the restore destination as "D:\Restore, then navigate to the following location:

   D:\Restore\A.txt.
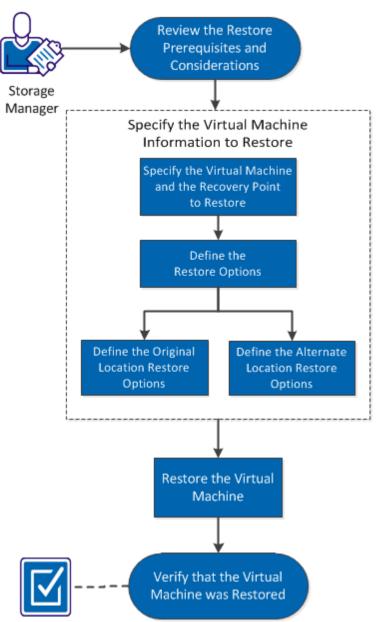
3. Verify the content of the restored file/folder.

The restored content is successfully verified.

How to Restore a Virtual Machine

CA ARCserve D2D lets you use the Recover VM option to restore a virtual machine (VM) that you previously backed up using CA ARCserve Central Host-Based VM Backup. This method can be used to restore the entire virtual machine to the original or to an alternate ESX location (as long as the recovery point data was created by CA ARCserve Central Host-Based VM Backup is available). You can browse the available virtual machine recovery points from a calendar view and select which recovery point you want to restore.

Note: This option can be used to recover a virtual machine from a backup session that was created using CA ARCserve Central Host-Based VM Backup without having to use that product.

The following diagram illustrates the process to restore from a virtual machine:

How to Restore a Virtual Machine

Perform the following tasks to restore a virtual machine:

1. Review the Restore Prerequisites and Considerations (see page 187)

2. Specify the Virtual Machine Information to Restore (see page 188)

    a. Specify the Virtual Machine and the Recovery Point to Restore (see page 188)

    b. Define the Restore Options (see page 191)

        ■ Define the Original Location Restore Options (see page 193)

        ■ Define the Alternate Location Restore Options (see page 194)

3. Restore the Virtual Machine (see page 199)

4. Verify that the Virtual Machine was Restored (see page 200)

SUPPLEMENTAL VIDEO

This procedure contains a supplemental instructional video. Select either CA Support or YouTube as the source for viewing this video. The versions of the video from CA Support and YouTube are identical, and only the viewing source is different.

CA Support: How to Restore a Virtual Machine

YouTube: How to Restore a Virtual Machine

Review the Restore Prerequisites and Considerations

Verify that the following prerequisites exist before performing a restore:

■ You have at least one CA ARCserve Central Host-Based VM Backup recovery point available to restore from.

■ You have a valid and accessible target Virtual Center or ESX server to recover the virtual machine.

Review the following restore considerations:

■ CA ARCserve D2D only allows one restore job to run at the same time. If you attempt to launch a restore job manually, while another restore job is running, an alert message opens informing you another job is running and requests you to try again later.

Specify the Virtual Machine Information to Restore

You can recover an entire virtual machine from a CA ARCserve Central Host-Based VM Backup recovery point. This Recover VM method is similar to performing a bare metal recovery (BMR). However a BMR is performed to restore a virtual machine that was backed up using CA ARCserve D2D, while a Recover VM is performed to restore a virtual machine that was backed up using CA ARCserve Central Host-Based VM Backup.

The process involved in restoring virtual machine is as follows:

1. Specify the Virtual Machine and the Recovery Point to Restore (see page 188)

2. Define the Restore Options (see page 191)

   ■ Define the Original Location Restore Options (see page 193)

   ■ Define the Alternate Location Restore Options (see page 194)

Specify the Virtual Machine and the Recovery Point to Restore
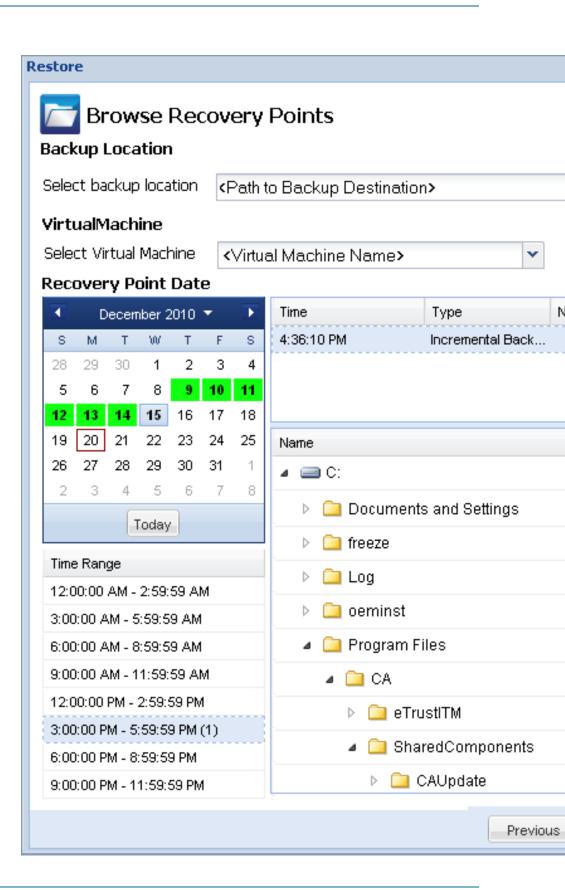
Use the Recover VM option to restore a virtual machine that you previously backed up. This method quickly and consistently creates a virtual machine from a CA ARCserve Central Host-Based VM Backup recovery point on an ESX server. The recovered virtual machine can then simply be started to complete the recovery process.

Follow these steps:

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog is displayed.

2. Click the Recover VM option.

   The Browse Recovery Points dialog is displayed.

3. Specify or browse to the location where your backup images are stored and select the appropriate backup source.

   You can click the green arrow button to verify the connection to the specified location. If necessary, enter the Username and Password credentials to gain access to that source location.

4. From the drop-down menu, select the virtual machine to recover. The drop-down menu includes all virtual machines at the specified backup location.

   The calendar view appears and all the dates containing recovery points for the specified backup source are highlighted in green.

5. Select the calendar date for the virtual machine image to restore.

   The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed, and the name of the backup.

6. Select a recovery point to restore.

   The backup content (including any applications) for the selected recovery point is displayed. When restoring a virtual machine, the entire system is restored. As a result, you can view, but not select individual volumes, folders, or files from within the selected virtual machine.

   Note: A clock icon with a lock symbol indicates that the recovery point contains encrypted information and can require a password for restore.

7. Click Next.

   The Restore Options dialog Opens.

The virtual machine and the recovery point to restore are specified.

Define the Restore Options

After you specify the virtual machine and the recovery point to restore, define the restore options for the selected virtual machine image.

Follow these steps:

1. From the Restore Options dialog, select the restore destination

The available destination options are:

Restore to Original Location

Restores the virtual machine to the original location from where the backup image was captured. By default, this option is selected.

For more information, see Define the Original Location Restore Options (see page 193).

Restore to an Alternative Location

Restores to the virtual machine to a different location from where the backup image was captured.

For more information, see Define the Alternate Location Restore Options (see page 194).

2. Specify the Resolving Conflicts options that CA ARCserve D2D will perform if conflicts are encountered during the restore process

   The available option is whether to overwrite the existing virtual machine. By default, this overwrite option is not selected.

   - If you select this option, the restore process overwrites (replaces) any existing images of this virtual machine that are at the specified restore destination. The virtual machine image is restored from the backup files regardless of its current presence on your restore destination.

   - If you do not select this option, the restore process creates a separate image of this virtual machine and the restore process does not overwrite any existing images that are at the specified restore destination.

3. Specify the Post Recovery option.

   Select whether power is applied to the virtual machine at the end of the restore process. By default, this option is not selected.

   The restore options are defined to restore a virtual machine.

Define the Original Location Restore Options

During the Recover VM configuration process, you are required to select the option of where you want to restore the virtual machine to. The available selections are Restore to the Original Location and Restore to an Alternative Location.

This procedure explains how to restore a virtual machine to the original location.

Follow these steps:

1. From the Restore Options dialog, after specifying the Resolve Conflicts and Post Recovery options, select Restore to Original Location and click Next.

   The Set Credential for Source vCenter/ESX Server dialog is displayed.

2. Specify the credentials for accessing the virtual machine.

vCenter/ESX Server

Displays the host name or IP address for the destination vCenter Server or ESX Server system.

Note: You cannot edit this field. You can only view the details.

VM Name

Displays the host name of the virtual machine that you are restoring.

Note: You cannot edit this field. You can only view the details.

Protocol

Specifies the protocol that you want to use for communication with the destination server. The available selections are HTTP and HTTPS.

Port Number

Specifies the port that you want to use for data transfer between the source server and the destination.

Default: 443.

User Name

Specifies the user name that has access rights to log in to the vCenter/ESX server where you plan to restore the virtual machine.

Password

Specifies the corresponding password for the User Name.

3. Click OK.

The Restore Summary dialog opens.

The restore options for original location are defined.

Define the Alternate Location Restore Options

During the Restore VM configuration process, specify where the recovered virtual machine is stored. The available selections are Restore to the Original Location and Restore to an Alternative Location.

This procedure explains how to restore a virtual machine to alternate location or different data store.

Follow these steps:

1. From the Restore Options dialog, after specifying the Resolve Conflicts and Post Recovery options, select Restore to an Alternative Location.

   The Restore Options dialog expands to display additional restore to alternative options.

2. Specify the vCenter/ESX Server Information.

   vCenter/ESX Server

   Specifies the host name or IP address for the destination vCenter or ESX server system.

   Username

   Specifies the user name that has access rights to log in to the vCenter/ESX server where you plan to restore the virtual machine.

   Password

   Specifies the corresponding password for the User Name.

   Protocol

   Specifies the protocol that you want to use for communication with the destination server. The available selections are HTTP and HTTPS.

   Default: HTTP.

   Port Number

   Specifies the port that you want to use for data transfer between the source server and the destination.

   Default: 443.

3. When the vCenter/ESX Server Information is specified, click the Connect to this vCenter/ESX Server button.

   If the alternative server access credential information is correct, the Other Information fields become enabled.

4. Specify the Other Information.

   VM Name

   Specifies the host name of the virtual machine that you are restoring.

   ESX Server

   Specifies the destination ESX server. The drop-down menu contains a listing of all ESX servers that are associated with a vCenter server.
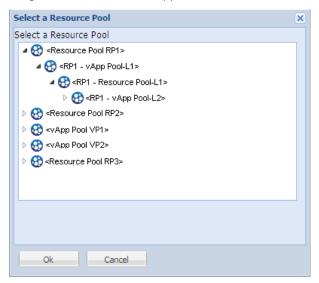
   Resource Pool

   Selects the Resource Pool or vApp Pool you want to use for the virtual machine recovery.

   Note: A Resource Pool is a configured collection of CPU and memory resources. A vApp Pool is a collection of one or more virtual machines that can be managed as a single object.

   Default: empty.

Click the Browse Resource Pool button to display the Select a Resource Pool dialog. This dialog contains a listing of all Resource Pools and vApp Pools available for the destination ESX server. Select the pool to use for the virtual machine recovery. You can leave this field blank when you do not want to assign a Resource Pool or vApp Pool to this virtual machine recovery.

VM DataStore

Specify the destination VM DataStore for the virtual machine recovery or each virtual disk within the virtual machine.

A virtual machine can have multiple virtual disks and you can specify a different data store for each virtual disk.

For example:

■   Disk0 can be restored to Datastore1.

■   Disk1 can be restored to Datastore1.

■   Disk2 can be restored to Datastore2.

Important! For VM DataStore, this field only populates if the user has full VMware system administrator permissions. If the user does not have proper administrator permissions, CA ARCserve D2D will not continue the restore process after you connect to the vCenter/ESX Server.

5.   Click OK.

The Restore Summary dialog opens.

The restore options for alternate location are defined.

Restore the Virtual Machine

The Restore Summary helps you to review all the restore options that you defined and modify them if necessary.

Follow these steps:

1. On the Restore Summary dialog, review the displayed information to verify that all the restore options and settings are correct.

    Restore Summary for Original Location:

Restore Summary for Alternate Location:

- If the summary information is incorrect, click Previous and go back to the applicable dialog to change the incorrect setting.

- If the summary information is correct, click Finish to launch the restore process.

The virtual machine is restored.

Verify that the Virtual Machine was Restored

After the completion of the restore process, verify that the virtual machine was restored to the specified destination.

Follow these steps:

1. Navigate to the CA ARCserve D2D restore destination you specified.

    For example, if you select to restore the virtual machine to the restore destination as original location, then login to the original ESX server and check if the virtual machine exists.
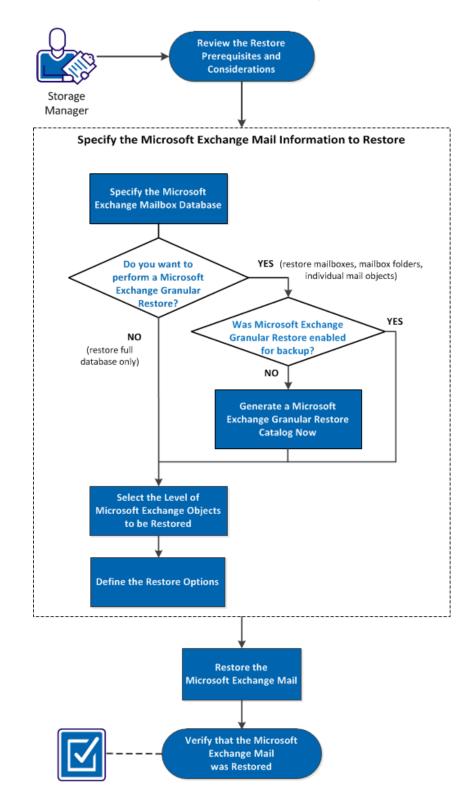
    If you select to restore the virtual machine to the Alternate location, then login to the alternate ESX server provided in the restore options and check if the virtual machine exists.

2. Verify the virtual machine was restored.

The virtual machine is restored successfully.

How to Restore Microsoft Exchange Mail

Each time CA ARCserve D2D performs a successful backup, a point-in-time snapshot image of your backup is created (recovery point). This collection of recovery points allows you to locate and specify exactly which backup image you want to restore. If at some later time, you suspect any of the backed up information is missing, corrupted, or not reliable, you can then locate and restore from a previous known good version. For Microsoft Exchange Mail you can then browse these recovery points to locate the individual objects (mailboxes, mailbox folders, or mail) that you want to restore.

The following diagram illustrates the process to restore Microsoft Exchange Mail:

How to Restore Microsoft Exchange Mail

Storage Manager

Review the Restore Prerequisites and Considerations

Specify the Microsoft Exchange Mail Information to Restore

Specify the Microsoft Exchange Mailbox Database

Do you want to perform a Microsoft Exchange Granular Restore?

YES (restore mailboxes, mailbox folders, individual mail objects)

NO (restore full database only)

Was Microsoft Exchange Granular Restore enabled for backup?

YES

NO

Generate a Microsoft Exchange Granular Restore Catalog Now

Select the Level of Microsoft Exchange Objects to be Restored

Define the Restore Options

Restore the Microsoft Exchange Mail

Verify that the Microsoft Exchange Mail was Restored

Perform the following tasks to restore a virtual machine:

1. Review the Restore Prerequisites and Considerations (see page 204)

2. Specify the Microsoft Exchange Mail Information to Restore (see page 206)

   a. Specify the Microsoft Exchange Mailbox Database (see page 206)

      ■ Generate a Microsoft Exchange Granular Restore Catalog Now (see page 208)

   b. Select the Level of Microsoft Exchange Objects to be Restored (see page 210)

   c. Define the Restore Options (see page 212)

3. Restore the Microsoft Exchange Mail (see page 214)

4. Verify that the Microsoft Exchange Mail was Restored (see page 215)

SUPPLEMENTAL VIDEO

This procedure contains a supplemental instructional video. Select either CA Support or YouTube as the source for viewing this video. The versions of the video from CA Support and YouTube are identical, and only the viewing source is different.

CA Support: How to Restore Microsoft Exchange Mail

YouTube: How to Restore Microsoft Exchange Mail

Review the Restore Prerequisites and Considerations

Verify that the following prerequisites exist before performing a Microsoft Exchange restore:

Database-level restore

■ The target machine has the same name and the same version of Microsoft Exchange installed.

■ The target database has the same database name and the same storage group name (Microsoft Exchange 200X) and be a part of the same Microsoft Exchange organization.

Granular-level restore

■ If the restore is set to original location, the mailbox whose contents are to be restored should be available in Microsoft Exchange.

■ If the restore is set to alternate location, the mailbox to which restore is targeted should be available in Microsoft Exchange.

■ Sufficient space available in the target mailbox to restore the specified Exchange objects.

■ To perform a Microsoft Exchange Granular Restore, the account specified in the CA ARCserve D2D user interface for restore must have sufficient restore permissions. The following permissions are required for the account:

  – The account must be a domain account.

  – The account must be a member of the Administrator group.

  – The account must be a member of the Backup Operators group.

  – There must be a mailbox associated with the account and the mailbox must be initialized.

    For Microsoft Exchange Server 2003, 2007, and Exchange 2010 this mailbox must be in same Organization (Microsoft Exchange Organization) of the Exchange server to which you plan to restore to (restore destination).

  – The name of the mailbox must be unique.

    A unique name is a name that does not exist in the organization as a subset of characters in another mailbox name.

    For example, if there is a mailbox named Administrator in your organization, you cannot use the name Admin.

  – The account user must have the proper role assignments:

    ■ For Microsoft Exchange Server 2003 systems, the User Name must be a domain account with Exchange full administrator role.

    ■ For Microsoft Exchange Server 2007 systems, the User Name must be a domain account with either the Microsoft Exchange Organization administrator role or the Exchange server administrator role.

    ■ For Microsoft Exchange Server 2010 systems, the User Name must be a domain account with Microsoft Exchange Organization management role.

Review the following restore considerations:

■ CA ARCserve D2D only allows one restore job to run at the same time. If you attempt to launch a restore job manually, while another restore job is running, an alert message opens informing you another job is running and requests you to try again later.

Note: On Microsoft Exchange 2007 and later, Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1 (and later) are not provided as part of the base product installation. Messaging API (MAPI) is a prerequisite for Microsoft Exchange Granular Restore. If MAPI is not installed on your Exchange server, mailbox or mail level granular restores may fail. To remedy any potential problem, Microsoft provides a download package that contains Microsoft Exchange MAPI and the latest version of Collaboration Data Objects (CDO). To download and install the latest version of this package, see the Microsoft Download Center.

■ If you have two or more databases in the storage group and the option "Dismount the database before restore and mount the database after restore" is checked, then any attempt to restore one single database will force the dismount of all the other databases within that same storage group. This dismount of all databases will occur before the restore is launched and will then mount them after the restore is complete.

Specify the Microsoft Exchange Mail Information to Restore

CA ARCserve D2D provides granular mailbox recovery capabilities for Microsoft Exchange Server. You can browse and select the recovery points that were captured on the production Microsoft Exchange Server and recover specified messages, folders, and mailboxes that were in the Exchange database at the time of the selected recovery point.

The process involved in restoring Microsoft Exchange Mail is as follows:

1. Specify the Microsoft Exchange Mailbox Database (see page 206)

   ■ Generate an Microsoft Exchange Granular Restore Catalog Now (see page 208)

2. Select the Level of Microsoft Exchange Objects to be Restored (see page 210)

3. Define the Restore Options (see page 212)

Specify the Microsoft Exchange Mailbox Database

CA ARCserve D2D lets you browse recovery points to locate individual objects within an Microsoft Exchange database to perform granular restore. You can either select restore to the original location or restore to a different location option. The Microsoft Exchange Server recovery can only be made using the Restore by Recovery Point method.

Follow these steps:

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog opens.

2. Click the Restore Exchange Mails option.

   The Restore Exchange Mails dialog opens.

3. Navigate to the Microsoft Exchange mailbox database that you want to restore:

   a. Specify the backup location. You can either specify a location or browse to the location where your backup images are stored. If necessary, enter the Username and Password credentials to gain access to that location. You can click the green arrow validate icon to verify proper access to the source location.

      The calendar view highlights (in green) all dates during the displayed time period that contain recovery points for that backup source.

   b. Select the calendar date for the backup image you want to restore.

      The corresponding Microsoft Exchange mailbox databases for that date are displayed, with the time of the backup, the type of backup that was performed (Full, Incremental, or Verify), and the name of the backup.

c. Specify a Microsoft Exchange mailbox database that you want to restore and click Next.

Note: If you did not enable the Exchange Granular Restore option during backup (no catalog generated), a notification message will be displayed asking you if you want to generate an Exchange Granular Restore catalog at this time. If you select No for generating a catalog now, you will not be able to browse to or select a granular recovery point. As a result you will only be able to perform full database restore from the Browse Recovery Points Restore dialog.

The Restore Exchange Mails dialog is updated to display a listing of the mailbox content for the selected database.

Note: Exchange Granular Restore supports email restores only. Calendar, Contacts, Notes and Tasks restores are not supported.

The Microsoft Exchange mailbox database is specified.

Generate a Microsoft Exchange Granular Restore Catalog Now

If you enabled the Exchange Granular Restore option at backup, the corresponding Exchange Granular Restore catalogs are generated during each backup. These catalogs help you to perform granular recoveries (at mailbox, mailbox folder, and or mail item levels) by letting you browse and select exactly which Exchange object you want to recover. However, if you disabled the Exchange Granular Restore option at backup, the Exchange mailboxes may not be displayed when you are trying to browse the mailbox database in a recovery point because the corresponding catalog was not generated.

Before you perform the restore, you can generate the catalog manually from the Restore Exchange Mails dialog.

Follow these steps:

1. From the CA ARCserve D2Dhome page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog opens.

2. Click the Restore Exchange Mails option.

   The Restore Exchange Mails dialog opens.

3. Navigate to the Microsoft Exchange mailbox database that you want to restore:

   a. Specify the backup location. You can either specify a location or browse to the location where your backup images are stored. If necessary, enter the User name and Password credentials to gain access to that location. You can click green arrow validate icon to verify proper access to the source location.

      The calendar view will highlight (in green) all dates during the displayed time period that contain recovery points for that backup source.

   b. Select the calendar date for the backup image you want to restore.

      The corresponding Microsoft Exchange mailbox databases for that date are displayed, along with the time of the backup, the type of backup that was performed, and the name of the backup.

4. Select a Microsoft Exchange mailbox database that you want to restore and click Next.

    A pop-up message displays informing you that the Exchange Granular Restore catalog has not been generated for the selected database and asking you if you want to generate the catalog now.

5. Click Yes to launch the process of generating an Exchange Granular Restore catalog.

    The Exchange Granular Restore catalog for the selected database is generated. The process of generating a catalog could be time-consuming depending upon the size of the database.

    During the catalog generating process, the Job Monitor displays information about the ongoing event, with the estimated time remaining to complete the catalog job.

    Note: If you select No for generating a catalog now, you cannot browse to or cannot select a granular recovery point. As a result you can only perform a full database restore.

6. When the catalog generating process is finished, click Next to continue the Exchange Granular Restore of the selected database.

    The granular restore can now be continued.

    Note: If you attempt to click Next while the catalog is still being generated, a pop-up message appears informing you of this condition.

    The Microsoft Exchange Granular Restore catalog is generated.

Select the Level of Microsoft Exchange Objects to be Restored

After generating the Microsoft Exchange Granular Restore catalog, specify the level of Exchange objects to be restored.

Note: CA ARCserve D2D does not support granular recovery of Exchange public folder objects. You need to use Application Restore to recover the entire public folder database and then extract the specific Exchange object you need.

Follow these steps:

1. From the Exchange Database dialog, select the level of Exchange object(s) to be restored (mailbox, folder, or individual mail).

    You can select the entire content or partial content of the Exchange object to restore. You can select multiple Exchange objects to restore

    Note: When using CA ARCserve D2D to restore individual mailbox/mail objects from the Exchange mailbox database, the operating system used for the restore must be same as used when it was backed up (including the same Windows Version number and Service Pack level and also the related version of the visual C++ redistributable package required to support it).

    Note: During browse and restore of emails from the CA ARCserve D2D UI, the "From" field property of the message may not display in the UI for mailboxes which have never logged in to the exchange server. However, if this occurs the emails will still be correctly restored.

    The available Microsoft Exchange objects are:

    a. Mailbox database

        If you select a mailbox database, all of the mailboxes in that database will be restored.

    b. Mailbox (or mailboxes)

        If you select a mailbox level, all corresponding content (folders and individual mail) within that mailbox will be restored.

    c. Folder(s)

        If you select the mailbox folder level, all corresponding mail content within that folder will be restored.

    d. Individual mail object(s)

        If you select the individual mail level, only the selected mail object(s) will be restored.

        Note: For Microsoft Exchange 2003 only, if the individual mail to be restored was sent using any email client other than Outlook and the mail had some type of flag status marker attached to it when it was backed up, the mail itself will be restored, but the attached marker will not be included with the restored mail.

2. Click Next.

    The Restore Options dialog Opens.

The Microsoft Exchange objects to be restored are specified.

Define the Restore Options

After you select the level of Microsoft Exchange objects, specify the destination for your backup. You can either select to restore to the original location or restore to a different location option.

Note: For Microsoft Exchange 2010, archived mailbox items cannot be restored to the original location. Archived mailbox items can only be restored to an alternate location or to a local disk. In addition, regular mailbox items cannot be restored to archive mailboxes.

Follow these steps:

1. From the Restore Options dialog, select the restore destination.

The available destination options are:

Restore to Original Location

Restores the mails to the original location from where the backup image was captured. Mails will retain the same hierarchy and be restored to its original mailbox and original folder.

■ If current machine is not the active Microsoft Exchange server, CA ARCserve D2D will detect the location of the active server and then restore the mails to that active server.

■ If mailbox has been moved to another Microsoft Exchange server, but still in the same organization, CA ARCserve D2D will detect the new Exchange server where the original mailbox resides, and then restore to that new server.

■ If the display name of the mailbox is changed, any attempt to restore the mailbox (from an earlier backup session) to its original location will fail because CA ARCserve D2D will not be able to find the changed name. To solve this problem, you can specify to restore this mailbox to an alternate location.

Note: When restoring a mailbox or mail to the original location, make sure the destination mailbox is available, or else the restore will fail. CA ARCserve D2D only validates the destination when the restore job is submitted.

Dump File Only

Restores the mails to a disk. This disk location can be local or a remote machine. The restored mails will maintain the same hierarchy as they had in the corresponding Microsoft Exchange mailbox. The file name will become the subject of mail.

Note: If the mail subject, folder name, or mailbox name includes any of the following characters, the character will be replaced by hyphen (-) in file name: \ / : * ? " < > |

For this option, you also need to specify what you want CA ARCserve D2D to do to resolve a conflict situation. In Microsoft Exchange, you can have multiple mail objects with the same name under the same folder. However in a File System, two files with the same name cannot co-exist under the same folder.

There are two options to resolve this conflict situation:

Rename

If on the disk, there is a file with the same name as the mail subject, CA ARCserve D2D will still name the mail subject, but will append a number at the end of the mail subject.

Overwrite

If on the disk, there is a file with the same name as the mail subject, CA ARCserve D2D will overwrite that file.

Note: When you select individual mail objects to restore to the disk (dump), by default the format of the restored mail object will be an Outlook Message (.MSG) file and not a Personal Storage Table (.PST) file.

Restore to Alternate Location

Restores the mails to a specified location or lets you browse to the location where your backup images will be restored. The destination must be a mailbox in the same Microsoft Exchange organization, and a new folder name is required. (If you are attempting to restore mails to an alternate location, the destination cannot be a public folder).

Note: When restoring mail to an alternate location, if the specified destination folder already exists, the restore will continue. However, if the specified folder does not exist, then CA ARCserve D2D will create the folder first and then continue the restore.

a. Specify the User Name and Password credentials, click the Browse button to navigate through a list of all Microsoft Exchange Servers, Storage Groups, Exchange Databases, and Mailboxes in the current organization.

b. Select a mailbox as the destination.

2. Click Next.

The Restore Summary dialog opens.

Restore the Microsoft Exchange Mail

The Restore Summary helps you to review all the restore options that you defined and modify them if necessary.

Follow these steps:

1. On the Restore Summary dialog, review the displayed information to verify that all the restore options and settings are correct.

- ■ If the summary information is incorrect, click Previous and go back to the applicable dialog to change the incorrect setting.

- ■ If the summary information is correct, click Finish to launch the restore process.

The Microsoft Exchange Mail is restored.

Verify that the Microsoft Exchange Mail was Restored

After the completion of the restore process, verify that the Microsoft Exchange Mail was restored to the specified destination.

Follow these steps:

1. Navigate to the CA ARCserve D2D restore destination you specified.

    For example, if you select to restore the Microsoft Exchange Mail to the restore destination as Original Location or Alternate Location, then login to the user's mailbox to check the restored email.

    If you select to restore the Microsoft Exchange Mail to Dump email items, then navigate to the dump folder to check the restored email.

    For example, if you select to restore the Microsoft Exchange Mail to C:\dump_folder1, then after restore navigate to this location to verify email

2. Verify emails of the restored Exchange Mail.

The Microsoft Exchange Mail is restored successfully.

Application Restore

CA ARCserve D2D allows you to not only protect and recover your data, but also helps you to get the applications that will use that data back up and running. All application recoveries can only be made using the Restore by Recovery Point method. During an application recovery, CA ARCserve D2D takes advantage of Windows Volume Shadow Copy Service (VSS) to help ensure data consistency for any VSS-aware application. With CA ARCserve D2D, you can recover the following applications without performing a full disaster recovery:

-   Microsoft Exchange Server (see page 216)
-   Microsoft SQL Server (see page 223)

Application Restore - MS Exchange Server

CA ARCserve D2D allows you to not only protect and recover your data, but also helps you to get the Microsoft Exchange Server application that uses that data back up and running. The Microsoft Exchange Server recovery can only be made using the Restore by Recovery Point method.

| CA Support: | How to: Restore MS Exchange Application |
| YouTube: | How to: Restore MS Exchange Application |

CA ARCserve D2D supports the following versions of Microsoft Exchange Server:

- **Exchange 2003** - Single Server Environment.

- **Exchange 2007** - Single Server Environment, Local Continuous Replication (LCR), and Cluster Continuous Replication (CCR) environment.

   For Exchange 2007 CCR environment, CA ARCserve D2D must be installed on both the active node and passive node of Microsoft Cluster. Backup can be performed from an active node and passive node, but restore can only be performed to an active node.

- **Exchange 2010** - Single Server Environment and Database Availability Group (DAG) environment.

   For Exchange 2010 DAG environment, CA ARCserve D2D must be installed on all member servers in the DAG group. A backup job can also be performed from any member server for both active and passive database copies, but restore can only be performed to an active database copy.

   Note: Microsoft Exchange Server 2003 Cluster Environment and Microsoft Exchange Server 2007 Single Copy Cluster (SCC) environment are not supported by CA ARCserve D2D.

Microsoft Exchange Server can be restored at the following levels:

Microsoft Exchange Writer Level

If you want to restore all the Microsoft Exchange Server data, you can perform a restore at Microsoft Exchange Writer level.

Storage Group Level

If you want to restore a specific Storage Group, you can perform a restore at the Microsoft Exchange Storage Group level.

(Does not apply for Microsoft Exchange Server 2010).

Mailbox Store Level (Exchange 2003)

If you want to restore a specific Mailbox Store, you can perform a restore at the Mailbox Store level.

Mailbox Database Level (Exchange 2007 and 2010)

If you want to restore a specific Mailbox Database, you can perform a restore at the Mailbox Database level.

Restore Microsoft Exchange Server Application

Note: When performing a Microsoft Exchange Server database restore (to either the original location or a recovery storage group/recovery database), you must verify that the account also has the following administrative privileges:

- Exchange 2003 - Exchange Full Administrator Role

- Exchange 2007/2010 - Exchange Organization Administrator or Exchange Server Administrator Role

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog opens.

2. Click the Browse Recovery Points option.

   The Browse Recovery Points dialog opens.

3. Select the recovery point (date and time) and then select the Microsoft Exchange database to be restored.

The corresponding marker box becomes filled (green) to indicate that the database has been selected for the restore.

Note: If you do not want the transaction log files to be applied after the restore, you must manually delete it before the restore is performed. For more information about manually deleting transaction log files, refer to the Microsoft Exchange Server documentation.

4. Click Next.

    The Restore Options dialog opens.

5. Select the destination for the restore.

    The available options are to restore to the original location of the backup, restore the dump file only, or restore to a Recovery Storage Group/Recovery Mailbox Database.

    Restore to original location

    Restores to the original location from where the backup image was captured.

    Dump file only

    Restores the dump files only.

    For this option, CA ARCserve D2D will restore the Microsoft Exchange database file to a specified folder, and will not bring it online after recovery. You can then move this file to a different server and mount it to exchange server manually to view data contained in it.

    Note: When a Recovery Mailbox Database exists, restore with 'Dump file only' option will fail.

Replay log on database

Specifies that when the database files are dumped to the destination folder, you can replay and apply all Microsoft Exchange transaction log files and commit them to the database file. When the database next starts, and transaction log files that were not yet written to the database files are then applied before the database is again made available to you.

Note: This option is not applicable for Microsoft Exchange Server 2003

Restore to Recovery Storage Group (Exchange 2007)

Restores the database to a Recovery Storage Group (RSG).

An RSG is a storage group that can be used for recovery purposes. You can restore a Microsoft Exchange Mailbox Database from a backup in a Recovery Storage Group and then recover and extract data from it, without affecting the production database that is being accessed by end users.

– If single storage group or database (except a public folder database) from the same storage group are selected to restore, the default restore destination is "Restore to Recovery Storage Group" (or "Restore to Recovery Database").

– If multiple storage groups or databases from multiple storage groups are selected to restore, Exchange can only be restored to the original location or restore with "Dump file only" option. The default restore destination is "Restore to original location".

Before restoring an Exchange 2007 database to a Recovery Storage Group, you must create a Recovery Storage Group and Mailbox Database with the same name.

For example, if you want to restore MailboxDatabase1 from the First Storage Group to a Recovery Storage Group, you must create a Recovery Storage Group and add the database "MailboxDatabase1" to the Recovery Storage Group.

Note: This option is not applicable for Microsoft Exchange Server 2003

Dismount the database before restore and mount the database after restore

Typically before a restore, Microsoft Exchange will perform some checks to help ensure the following:

– The database to be restored is in "Dismounted" status.

– The database is not restored unexpectedly.

To protect a Microsoft Exchange production database from being restored unexpectedly, a switch is added to allow the database to be overwritten during the restore process. Microsoft Exchange will refuse to restore a database if this switch is not set.

For CA ARCserve D2D, these two options are controlled by this "Dismount the database before restore and mount the database after restore" option. With this option, CA ARCserve D2D lets you launch the restore process automatically without any manual operations. (You can also specify to dismount/mount database manually).

- If checked, specifies that the recovery process will automatically dismount the Exchange database before the restore process and then mount the database after the restore process is completed. In addition, if checked, this option will also allow the Exchange database to be overwritten during the restore.

- If unchecked, specifies that the recovery process will not automatically dismount the Exchange database before recovery and mount the database after recovery.

  The Exchange administrator would have to perform some manual operations such as dismount the Exchange database, set the Allow Overwrite flag on the database, and mount the Exchange database. (The recovery procedure is performed by Exchange during the mounting of the database).

  In addition, if unchecked, this option does not allow the Exchange database to be overwritten during restore.

Restore to Recovery Database (Exchange 2010)

Restores the database to a Recovery Database. A Recovery Database is a database that can be used for recovery purposes. You can restore a Microsoft Exchange Mailbox Database from a backup to a Recovery Database and then recover and extract data from it, without affecting the production database that is being accessed by end users.

Before restoring an Exchange 2010 database to a Recovery Database, you must first create a Recovery Database.

Note: This option is not applicable for Microsoft Exchange Server 2003 and 2007.

6. Click Next.

    The Restore Summary dialog opens.

7. Review the displayed information to verify that all the restore options and settings are correct.

    ■   If the summary information is not correct, click Previous and go back to the applicable dialog to change the incorrect setting.

    ■   If the summary information is correct, click Finish to launch the restore process.

Application Restore - MS SQL Server

CA ARCserve D2D allows you to not only protect and recover your data, but also helps you to get the Microsoft SQL Server application that uses that data back up and running. The Microsoft SQL Server recovery can only be made using the Restore by Recovery Point method.

CA Support: How to: Restore MS SQL Server Application

YouTube: How to: Restore MS SQL Server Application

Restore Microsoft SQL Server Application

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Restore.

   The restore methods selection dialog opens.

2. Click the Browse Recovery Points option.

   The Browse Recovery Points dialog opens.

3. Select the recovery point (date and time) and then select the Microsoft SQL Server database to be restored.

   The corresponding marker box becomes filled (green) to indicate that the database has been selected for the restore. You can select a single database or multiple databases to be restored.

4. Click Next.

    The Restore Options dialog opens.

5. Select the destination for the restore.

    The available options are to restore to the original location of the backup, restore the dump file only, or restore to an alternate location.

    Note: When restoring a Microsoft SQL Server 2012 database that is part of an AlwaysOn Availability Group (AAG), there are some considerations that you should be aware of. For more information, see MS SQL Server 2012 AAG Restore Considerations (see page 229).

    Restore to original location

    Restores to the original location from where the backup image was captured.

    Dump file only

    Restores the dump files only.

    Dump files are created when an application crashes and contains additional (time-stamped) information that can be used to troubleshoot the cause of the problem.

When you select this option, you can then specify or browse to the folder location where the dump file will be restored to.

Restore to alternate location

Restores to an alternate location (not the original location).

Instance Name	Database Name	New Database Name	Alternative file location	
MSSQLSERVER	LogShippingDatabase	LogShippingDatabase		Browse
MSSQLSERVER	MirrorDatabase001	NewDatabaseName	C:\NewDBLocation	Browse

Because backups can be copied to network locations, they can be used by multiple SQL Server instances. Multiple database restore can be performed (simultaneously) from the instance level. From this listing, you can select the database instance and specify a new database name and alternate location to restore the database to. In addition, you can also browse to the alternate location where the database will be restored to.

When restoring a Microsoft SQL Server application to an alternate location, there are some considerations that you should be aware of. For more information, see MS SQL Server Restore to Alternate Location Considerations (see page 227).

6. Click Next.

   The Restore Summary dialog opens.

7. Review the displayed information to verify that all the restore options and settings are correct.

   ■ If the summary information is not correct, click Previous and go back to the applicable dialog to change the incorrect setting.

   ■ If the summary information is correct, click Finish to launch the restore process.

MS SQL Server Restore to Alternate Location Considerations

When you specify to restore a Microsoft SQL Server application to an alternate location, you can either restore it to an alternate location on the same machine or on a different machine.

Prior to performing a CA ARCserve D2D restore of a Microsoft SQL Server application to an alternate location, you should consider the following:

If alternate location is on the same machine

For this option, you can either restore a database to a new location (with the same name) or restore with a new name (to the same location):

- **Same Name - New Location**

  For example, if Database A is installed in the current SQL Server at "C:\DB_A" and has been backed up. You can use this option and specify "Alternate File Location" to restore Database A to an alternate location such as "D:\Alternate_A.

  After the database has been restored, the database file located at the new location "D:\Alternate_A" will then be used.

  While you restore to an alternate location, the Instance Name section is unavailable. The Instance name should always be the same. Therefore, you cannot restore a database to an alternate instance present on the same MS SQL Server.

- **Same Location - New Name**

  For example, if you have two databases (Database A and Database B) installed in the current SQL Server and both have been backed up. You can use this option and specify "New database Name" to restore Database A to same location as Database A_New.

  After the databases have been restored, this location will now have three databases (Database A, Database B, and Database A_New).

If alternate location is on the different machine

- The SQL Server installation path must be the same as the path that existed when the backup was performed.

  For example, if the backup of the SQL Server is installed at "C:\SQLServer", then the SQL Server on the new CA ARCserve D2D server must also be installed at C:\SQLServer.

- The same instance name for the database that existed when the backup was performed must be installed on CA ARCserve D2D server, otherwise the database associated with that instance will be skipped from the restore.

  For example, if the backup of the SQL Server contained "Instance_1" with Database A and Database B and "Instance_2" with Database C, but the CA ARCserve D2D server only has "Instance_1". After the restore is complete, Database A and Database B will be restored, but Database C will not be restored.

- The SQL Server version on the CA ARCserve D2D server must be backwards compatible to the version of the SQL Server used during the backup session.

  For example, you can restore a SQL Server 2005 machine to a SQL Server 2008 machine; however, you cannot restore a SQL Server 2008 machine to a SQL Server 2005 machine.

- Restoring a database of 64-bit instance to 32-bit instance is not supported.

MS SQL Server 2012 AAG Restore Considerations

When restoring a Microsoft SQL Server 2012 database that is part of an AlwaysOn Availability Group (AAG), there are some considerations that you should be aware of.

If the MS SQL database is part of the MS SQL 2012 AlwaysOn Availability Group (AAG), and restoring to the original location fails, perform the following tasks:

1. Remove the database to be restored away from the Availability Group. For more information, see http://msdn.microsoft.com/en-us/library/hh213326.aspx.

2. Share the backup session to CA ARCserve D2D on every Availability Group node and then restore the session by CA ARCserve D2D on every Availability Group node.

3. Add the database back to an Availability Group. For more information, see http://msdn.microsoft.com/en-us/library/hh213078.aspx.

Restore from Windows Explorer Using ARCserve D2D View

You can use the ARCserve D2D View from Windows Explorer as an alternate method to restore objects that were backed up. The ARCserve D2D View lets you perform such functions as recover, copy, and paste to quickly and easily restore objects.

From the ARCserve D2D View, you can perform two types of restore:

- Restore a file/folder (see page 229)
- Restore mail objects from Exchange (see page 232)

Restore a File/Folder Using ARCserve D2D View

For a file/folder restore, you can use the copy and paste function to restore backed up objects (files or folders) from the backup destination to your specific restore destination. (The drag-and-drop method is not supported for a file/folder restore from the ARCserve D2D View).
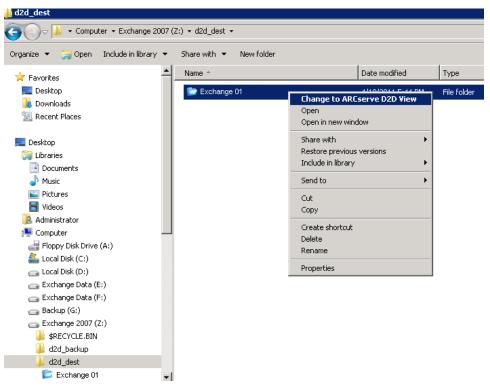
CA Support: How to Restore a File/Folder Using ARCserve D2D View.

YouTube: [How to Restore a File/Folder Using ARCserve D2D View](#).

Follow these steps:

1. Access Windows Explorer and from the folders in the left pane, navigate to and select the backup destination.

2. From the right pane, right-click on the backup destination.

   A pop-up menu is displayed listing the available options.

3. Select the "Change to ARCserve D2D View" option.

   The Windows Explorer View changes to the ARCserve D2D View. When you enter into that directory, all views are logic views from a CA ARCserve D2D user perspective and displays the recovery points stored at that location.

Note: When using the ARCserve D2D View, if you attempt to browse to or locate a recovery point and all recovery points are not displayed, it may be because your backup destinations were split between your local machine and a remote share machine. For the ARCserve D2D View to display all recovery points, the backup locations (for full and corresponding incremental backups) should all be at the same location (either local or remote). If this occurs, it is a limitation only when using the ARCserve D2D View. To remedy this problem, you can use the CA ARCserve D2D restore UI instead to properly display all recovery points, regardless of being at the same or different locations.

4. Select the recovery point that you want to restore from and expand that directory until you can gain access to the file or folder that you want to restore.

Note: From the ARCserve D2D View, the Copy option is only available for file and folder level objects. You cannot use this option to copy volume or machine level objects.

5. Right-click on the file or folder to be restored and select Copy. Navigate to the restore location, right-click on the location, and select Paste.

    Note: Manual operations (such as copy, cut, or paste) for the backup destination folder are not successful if a job is active or a user is browsing recovery points using the ARCserve D2D View.

    Note: When restoring backed-up files (with long file names) from the ARCserve D2D View using the copy-and-paste method, the job can fail without any corresponding error or warning. (Windows Explorer has a limitation on the maximum file path length, which can lead to a file copy failure). If this occurs, you can use the installed CA ARCserve D2D UI to perform the restore.

6. When the restore is successfully completed, right-click on the backup destination and select the "Change to Windows Normal View" option.

    The ARCserve D2D View changes back to the Windows Explorer View.

    Note: During the time that you are in the ARCserve D2D View mode, the merge/purge process for retaining the maximum number of recovery points will be disabled. As a result, CA ARCserve D2D will continue to save recovery points beyond the specified number of recovery points until you exit the ARCserve D2D View and return to the Windows Normal View. When you exit the ARCserve D2D View, all retained recovery points beyond the specified number will then be merged/purged.

Restore an Exchange Object Using ARCserve D2D View

For an Exchange object restore, you can use the recovery function or the copy and paste (or drag-and-drop) functions to restore backed up Exchange (mailboxes, mail folders, mail) from the backup destination to your specific restore destination.

Note: If you are using a non-Windows shared folder as your backup destination, you will not be able to switch to the ARCserve D2D View for a local or remote Windows machine.
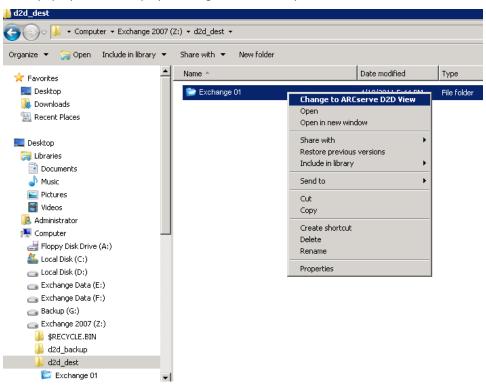
CA Support: How to: Restore an Exchange Object Using ARCserve D2D View

YouTube: How to: Restore an Exchange Object Using ARCserve D2D View

Restore an Exchange object using ARCserve D2D View

1. Access Windows Explorer and navigate to the backup destination.

2.   Right-click on the backup destination.

A pop-up menu is displayed listing the available options.

3.   Select the "Change to ARCserve D2D View" option.

The Windows Explorer View changes to the ARCserve D2D View. When you enter into that directory, all views are logic views from a CA ARCserve D2D user perspective and displays the recovery points stored at that location.

Note: When using the ARCserve D2D View, if you attempt to browse to or locate a recovery point and all recovery points are not displayed, it may be because your backup destinations were split between your local machine and a remote share machine. For the ARCserve D2D View to display all recovery points, the backup locations (for full and corresponding incremental backups) should all be at the same location (either local or remote). If this occurs, it is a limitation only when using the ARCserve D2D View. To remedy this problem, you can use the CA ARCserve D2D restore UI instead to properly display all recovery points, regardless of being at the same or different locations.

4. Select the recovery point that you want to restore from and expand that directory until you can gain access to the Exchange object that you want to restore.

5. From the ARCserve D2D View, the Recovery and Copy options are only available for mailbox, folder, and individual mail objects. You cannot use these options to restore an entire Exchange mailbox database.

Note: If the Exchange mailboxes are not displayed when you are trying to browse the mailbox database in a recovery point, the Exchange Granular Restore may not have been enabled during backups and the corresponding catalog was not generated. Prior to performing the restore, you can generate the catalog manually from the Restore Exchange Mails dialog. For more information, see Generate an Exchange Granular Restore Catalog before Restore.

6. Right-click on the file or folder to be restored and select Recovery or Copy.

    a. If you select Copy, you can then navigate to the restore location, right-click on the location, and select Paste. (You can also use the drag and drop method to copy an Exchange object to a restore destination).

      Note: If you are attempting to use the drag-and-drop function to restore items (mail objects) from a remote destination and this function does not work, verify that the remote folder URL is included to the "Trusted Sites' in Internet Explorer.

    b. If you select Recovery, the Restore Options dialog opens. Select the destination for the restore.

The available options are to restore to the original location of the backup or restore dump files only.

Restore to Original Location

Restores the mails to the original location from where the backup image was captured. Mails retain the same hierarchy and be restored to its original mailbox and original folder.

■ If the current machine is not the active Exchange server, CA ARCserve D2D detects the location of the active server and then restores the mails to that active server.

■ If the mailbox has been moved to another Exchange server, but is still in the same organization, CA ARCserve D2D detects the new Exchange server where the original mailbox resides, and then restores to that new server.

Dump File Only

Restores the mails to a disk. This disk location must be a local path. The restored mails maintain the same hierarchy as they had in the corresponding Exchange Mailbox. The file name will be the subject of mail.

Note: If the mail subject, folder name, or mailbox name includes any of the following characters, the character are replaced by a hyphen (-) in file name: \ / : * ? " < > |

There are two options to resolve a conflict situation in a File System. Two files in File System cannot exist under the same folder, while Exchange mails can.

■ **Rename** - If on the disk, there is a file with the same name as the mail subject,CA ARCserve D2D still names the mail subject, but appends a number at the end of the mail subject.

■ **Overwrite** - If on the disk, there is a file with the same name as the mail subject, CA ARCserve D2D overwrites that file.

7. Click OK to save the restore options and launch the restore process.

   Note: When the Catalog and Restore Job for Exchange Granular Restore is in progress, the backup session will be in a mounted state. Do not perform any operation (format, change drive letter, delete partition, etc.) on this mounted volume.

8. When the restore is successfully completed, right-click on the backup destination and select the "Change to Windows Normal View" option.

   The ARCserve D2D View changes back to the Windows Explorer View.

   Note: During the time that you are in the ARCserve D2D View mode, the merge/purge process for retaining the maximum number of recovery points will be disabled. As a result, CA ARCserve D2D will continue to save recovery points beyond the specified number of recovery points until you exit the ARCserve D2D View and return to the Windows Normal View. When you exit the ARCserve D2D View, all retained recovery points beyond the specified number will then be merged/purged.

How to Copy a Recovery Point

Each time CA ARCserve D2D performs a successful backup, a point-in-time snapshot image of the backup is created. This collection of recovery points lets you locate and specify the exact backup image to copy.

The following diagram illustrates the process to copy a recovery point:

Perform the following tasks to copy a recovery point:

1. Review the Prerequisites (see page 238)

2. Configure the Copy Recovery Point Settings (see page 109)

3. Copy a Recovery Point (see page 243)

   a. Select the Recovery Point to Copy (see page 243)

   b. Define the Copy Options and Copy the Recovery Point (see page 245)

4. Verify the Copied Recovery Point (see page 247)

SUPPLEMENTAL VIDEO

This procedure contains a supplemental instructional video. Select either CA Support or YouTube as the source for viewing this video. The versions of the video from CA Support and YouTube are identical, and only the viewing source is different.

CA Support: How to Copy a Recovery Point

YouTube: How to Copy a Recovery Point

Review the Prerequisites

Review the following prerequisites before copying a recovery point:

- You have at least one full backup available to copy.

- You need a valid destination to copy the recovery point.

Configure the Copy Recovery Point Settings

CA ARCserve D2D lets you specify the recovery point copy settings. Before you copy a recovery point, configure the copy recovery point settings. For a better understanding about how the options on this dialog can be used to configure your recovery point copy schedule, see Copy Recovery Points - Example Scenarios (see page 112).

Note: The recovery point copy process is a copy and paste operation only and not a cut and paste operation. As a result, whenever a scheduled copy recovery point job is performed CA ARCserve D2D creates an additional copy of the recovery point to the specified copy destination, while still retaining the original copy of the recovery point at the backup destination that was specified in Backup Settings.

Follow these steps:

1. On the CA ARCserve D2D home page, select Settings from the taskbar.

   The Settings dialog opens.

2. Click the Copy Recovery Points tab.

   The Copy Recovery Points dialog opens.

3. Select Enable Copy Recovery Points.

   When selected, enables the copying of recovery points.

   Note: If you do not select this option, no scheduled copying of recovery points is performed.

4. Specify the following recovery point copy schedule settings:

   Destination

   Specifies the storage location for the copy of the selected recovery point. (Optional) You can click the green arrow button to verify the connection to the specified location.

   Note: The maximum length for the specified destination path is 158 characters.

   Copy Recovery Points job will be run after the specified number of backups are performed

   Specifies when the scheduled recovery point copy process is automatically launched. This process is launched based on your selected copy policies and specified number of successful backups (Full, Incremental, and Verify).

You can use this setting to control how many times a recovery point copy process is triggered each day. For example, if you schedule to run a backup job every 15 minutes, and copy job after every 4 backups, then it performs 24 recovery point copy jobs each day (1 each hour).

Default: 8

Minimum: 1

Maximum: 1344

Important! If you schedule backup and copy jobs to run at regular intervals and if the copy job is currently running (in active state) when the scheduled time for the backup job time arrives, the backup job fails. (The next backup job will run as scheduled and should be successful if it does not conflict with another copy job). Because the copy operation takes almost same amount of time as performing a full backup, the best practice is not to set a frequent schedule for your recovery point copy jobs.

Specify the number of recovery points to keep

Specifies the number of recovery points that are retained and stored at the specified copy destination. Discards the oldest recovery point, when this number is exceeded.

Note: If you do not have sufficient free space at the target destination, reduce the number of saved recovery points.

Default: 1

Maximum: 1344

5. Select the Compression level.

Compression is typically performed to decrease your disk space usage, but also has an inverse impact on your backup speed due to the increased CPU usage.

The available options are:

- **No Compression** - Compression is not performed. Files are pure VHD. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

- **No Compression - VHD** - Compression is not performed. Files are converted to .vhd format directly, without the need for manual operations. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

- **Standard Compression** - Some compression is performed. This option provides a good balance between CPU usage and disk space usage. This setting is the default setting.

- **Maximum Compression** - Maximum compression is performed. This option provides the highest CPU usage (lowest speed), but also has the lowest disk space usage for your backup image.

Note: If your backup image contains uncompressible data (such as JPG images or ZIP files), additional storage space can be allocated to handle such data. As a result, if you select any compression option and you have uncompressible data in your backup, it can actually result in an increase in your disk space usage.

6. If you also want the copied recovery point to be encrypted, specify the following information:

   Encryption Algorithm

   Specifies the type of encryption algorithm that is used for the recovery point copies.

   The available format options are No Encryption, AES-128, AES-192, and AES-256.

   Encryption Password

   Lets you specify and confirm the encryption password being used to encrypt the destination session.

7. Click Save Settings.

   Your recovery point copy settings are saved.

The copy recovery point settings are successfully configured.

Copy Recovery Points - Example Scenarios

The following example scenarios are provided to give you a better understanding of how the various options can affect your scheduled copying of recovery points.

For this example, assume that you configured your CA ARCserve D2D backup schedule as follows:

- Full Backup - Every 7 days

- Incremental Backup - Every 1 hour

- Verify Backup - Every 3 days

and assume:

- First backup is on Day #1 at 5:00PM (by default, the first backup is always a Full Backup)

- First Incremental Backup will be on Day #1 at 6:00PM (and every hour after)

- Recovery Points retention count is set to 31 (default number)

- Location "D" is configured as the copy destination

Scenario #1

For this scenario, the Copy Recovery Point settings are as follows:

■ Copy after 4 backups

■ Retain 1 recovery point

Result:

– At 8:00PM (after the 4th backup), the scheduled copy job will run and consolidate all 4 recovery points into a single recovery point and store it at destination D.

– At 12:00 midnight (after the 8th backup), the next scheduled copy job will run and consolidate all 8 recovery points into a single recovery point and store it at destination D.

The previous recovery point is removed from destination D because the setting is to retain only 1 recovery point at the destination.

Scenario #2

For this scenario, the Copy Recovery Point settings are as follows:

■ Copy after 4 backups

■ Retain 4 recovery points

Result:

– At 8:00PM (after the 4th backup), the scheduled copy job will run and consolidate all 4 recovery points into a single recovery point (Recovery Point #1) and store it at destination D.

– At 12:00 midnight (after the 8th backup), the next scheduled copy job will run to create Recovery Point #2 and store it at destination D.

– At 4:00AM on Day #2 (after the 12th backup), the next scheduled copy job will run to create Recovery Point #3 and store it at destination D.

– At 8:00AM on Day #2 (after the 16th backup), the next scheduled copy job will run to create Recovery Point #4 and store it at destination D.

– At 12:00 noon on Day #2 (after the 20th backup), the next scheduled copy job will run. A new recovery point will be created and the first recovery point (created after the 8:00PM backup on previous day) is removed from destination D, because the setting is to retain only 4 recovery points at the destination.

Scenario #3

For this scenario, the Copy Recovery Point settings are as follows:

- Copy after 1 backup

- Retain 4 recovery points

    Result:

    – At 5:00PM (after the 1st backup), the scheduled copy job will run to create a single recovery point (Recovery Point #1) and store it at destination D.

    – At 6:00PM (after the 2nd backup), the next scheduled copy job will run to create Recovery Point #2 and store it at destination D.

    – At 7:00PM (after the 3rd backup), the next scheduled copy job will run to create Recovery Point #3 and store it at destination D.

    – At 8:00PM (after the 4th backup), the next scheduled copy job will run to create Recovery Point #4 and store it at destination D.

    – At 9:00PM (after the 5th backup), the next scheduled copy job will run. A new recovery point will be created and the first recovery point (created after the 5:00PM backup) is removed from destination D, because the setting is to retain only 4 recovery points at the destination.

Copy a Recovery Point

When you select a recovery point to copy, all previous backup blocks (full and incremental) are consolidated and captured to recreate a full and most recent backup image.

You can perform the following tasks to protect your backups:

- Copy/export recovery point information to store it safely off-site in the event of a catastrophe.

- Save your recovery points to multiple locations.

- Consolidate your backups to preserve all your recovery points.

The process involved in copying a recovery point is as follows:

1. Select the Recovery Point to Copy (see page 243).

2. Define the Copy Options and Copy the Recovery Point (see page 245).

Select the Recovery Point to Copy

CA ARCserve D2D provides a list of available recovery points and lets you select the recovery point to create a copy. You can specify the destination, recovery point date, and time range to copy a recovery point.

Follow these steps:

1. On the CA ARCserve D2D home page, select Copy Recovery Point.

   The Copy Recovery Point dialog opens.

2. Specify or browse to the location where your backup images are stored and select the appropriate backup source.

   You can click the green arrow button to verify the connection to the specified location. If necessary, enter the Username and Password credentials to gain access to that location.

   The calendar view appears.

   Note: All the dates containing recovery points for the specified location are highlighted in green.

3. Select the calendar date for the backup image to copy.

   The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed, and the name of the backup.

   Note: A clock icon with a lock symbol indicates that the recovery point contains encrypted information and can require a password for the restore.

4. Select a Recovery Point to copy.

    The backup content (including any applications) for the selected recovery point displays.

5. Click Next.

    The Copy Options dialog opens.

The recovery point to copy is specified.

Define the Copy Options and Copy the Recovery Point

After you specify a recovery point to copy, define the copy options to create a copy that combines the previous full and incremental backups for the selected recovery point.

Follow these steps:

1. From the Copy Options dialog, specify the following Copy Options:

Password

Specify the encrypted password for backup.

Note: This dialog includes two password fields. The upper field is for the password to decrypt the source session, and the lower field is used to encrypt the destination session.

If the recovery point you select to copy was previously encrypted, provide the password.

- If the recovery point to be copied is a backup session of the same computer that is running the copy recovery point job, the encryption password is remembered and this field is automatically populated.

- If the recovery point to be copied is a backup session of another computer, enter the encryption password.

Destination

Specify (or browse to) the storage location of the selected recovery point. (Optional) You can click the green arrow button to verify the connection to the specified location.

If necessary, enter the Username and Password.

2. Select the Compression level.

Note: The specified backup compression level has no relation with the copy compression level. For example, in backup destination the compression level can be set to Standard; however, when you submit the copy job, the compression can be changed to No Compression or Maximum Compression.

Compression is typically performed to decrease your disk space usage, but also has an inverse impact on your backup speed due to the increased CPU usage.

The available options are:

- **No Compression** - Compression is not performed. Files are pure VHD. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

- **No Compression - VHD** - Compression is not performed. Files are converted to .vhd format directly, without the need for manual operations. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

- **Standard Compression** - Some compression is performed. This option provides a good balance between CPU usage and disk space usage. This setting is the default setting.

- **Maximum Compression** - Maximum compression is performed. This option provides the highest CPU usage (lowest speed), but also has the lowest disk space usage for your backup image.

Note: If your backup image contains uncompressible data (such as JPG images or ZIP files), additional storage space can be allocated to handle such data. As a result, if you select any compression option and you have uncompressible data in your backup, it can actually result in an increase in your disk space usage.

Note: If you change the compression level from "No Compression" to either "Standard Compression" or "Maximum Compression", or if you change from either "Standard Compression" or "Maximum Compression" to "No Compression", the first backup that is performed after this compression level change is automatically a Full Backup. After performing the Full Backup, performs all future backups (Full, Incremental, or Verify) as scheduled.

3. If you also want the copied recovery point to be encrypted, specify the following information:

   Encryption Algorithm

   Specifies the type of encryption algorithm that is used for the recovery point copies.

   The available format options are No Encryption, AES-128, AES-192, and AES-256.

   Encryption Password

   Lets you specify and confirm the encryption password being used to encrypt the destination session.

   Note: When you enable the encryption, specify a new password. You need this password to restore the copied recovery point.

4. Click Create a Copy.

   A status notification window appears and the copy process for the selected recovery point type is launched immediately.

   Note: CA ARCserve D2D allows only one recovery point copy job to run at the same time. If you attempt to launch a recovery point copy job manually while running another scheduled copy job, an alert message opens. The message informs you that another job is running and requests you to try again at a later time.

The recovery point is copied from the backup source to the copy target destination.

Verify the Copied Recovery Point

After you copy a recovery point, verify that the copied recovery point is available at the specified destination.

Follow these steps:

1. Navigate to the CA ARCserve D2D destination you specified.

   A list of folders appears.

2. Open the hostname folder, and navigate to the following subordinate folder:

   hostname\VStore

3. Open the VStore folder, and navigate to the following session folder:

   VStore\S0000000001

4. Locate all files with a D2D extension to verify your copied recovery point at the specified location.

   For example, if your computer name is "Department_A" and you copied the recovery point (backup) to "E:\copied_vhd\", navigate to the following location:

   E:\copied_vhd\Department_A\VStore\S0000000001.

The copy of your recovery point is successfully verified.

Mount a Recovery Point

Mount Recovery Point provides the ability to mount a recovery point to a drive letter (volume) or an NTFS folder, to view, browse, copy, or open the backup files directly in Windows Explorer.

Note: For CA ARCserve Central Host-Based VM Backup, the recovery points are mounted on the backup proxy system.

Instead of using the CA ARCserve D2D web interface to find or recover files and folders, you can mount the volumes from a given CA ARCserve D2D backup recovery point to a drive letter, so that you can use Windows Explorer to find or recover any files and folders. The benefit is that Windows Explorer can be more familiar and convenient to use.

Follow these steps:

1. From the CA ARCserve D2D home page (or CA ARCserve D2D Monitor), select Mount Recovery Point.

   The Mount Recovery Point dialog opens.

2. In the Select and Mount Backup Volume section, specify the backup source. You can either specify a location or browse to the location where your backup images are stored. You can click the green arrow icon button to verify the connection to the specified location. If necessary, enter the Username and Password credentials to gain access to that location.

   The calendar view highlights (in green) all dates during the displayed time period that contain recovery points for that backup source.

3. Specify the recovery point to mount.

   a. Select the calendar date for the backup image you want to mount.

      The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed, and the name of the backup.

      Note: A clock icon with a lock symbol indicates that the recovery point contains encrypted information and can require a password to mount the recovery point.

      b.   Select a recovery point that you want to mount.

           The corresponding backup content (including any applications) for that recovery point is displayed.

      c.   Locate the Volume that you want to mount and click Mount.

           You can mount the recovery point to a drive letter (volume) or an empty NTFS folder.

           Note: If a volume is mounted already, you cannot mount it again from the same recovery point.

           The Mount Recovery Point dialog opens.

4.   Select whether you want to mount to a volume or path.

      a.   If you mount to a volume, select the volume from the drop-down list.

      b.   If you mount to a path, enter or browse for the location.

           Important! The path must be to an empty NTFS folder.

5.   If the selected recovery point was encrypted, provide the encryption password and click OK.

    The selected backed up volume is mounted and displayed in the List of Mounted Volumes on the Mount Recovery Point dialog. You can now use Windows Explorer to view, browse, copy, or open the backup files.

    Note: You cannot delete any backup files from Windows Explorer.

6.   When the mounted recovery point is no longer needed, the best practice is to dismount it. Otherwise, the mounted recovery point prevents the CA ARCserve D2D backup from performing a session merge/purge operation.

If CA ARCserve D2D attempts to merge a mounted recovery point, a status alert also displays on the Home Page to inform you the selected recovery point cannot be merged.

Recovery Points
14 Recovery Points out of 5
Recovery point D:\laptop\sample-pc1\VStore\S0000000007\ is mounted and cannot currently be merged.

Note: If the merge fails and you want to be notified, you can configure Email Alerts in the Preferences Settings to receive an email alert. For more information, see Specify Email Alert Preferences (see page 116).

a. To dismount the mount points, select the mount point that you want to dismount and click Dismount.

   The selected mount point is dismounted and no longer displays in the List of Mounted Volumes on the Mount Recovery Point dialog.

b. To refresh the list of mount points, click Refresh.

   The updated list of mount points displays.

Create a VHD File from a CA ARCserve D2D Backup

Each time CA ARCserve D2D performs a successful backup, a point-in-time snapshot image of your backup is also created. Before creating a Virtual Hard Disk (VHD) file from a CA ARCserve D2D backup, you must have at least one CA ARCserve D2D recovery point available.

Follow these steps:

1. From the CA ARCserve D2D home page, select Copy Recovery Point.

   The Copy Recovery Point dialog opens.

2. Specify the backup source. You can either specify a location or browse to the location where your backup images are stored. If necessary, enter the Username and Password credentials to gain access to that location.

   The calendar view highlights (in green) all dates during the displayed time period that contain recovery points for that backup source.

3. Specify the recovery point to copy.

   a. Select the calendar date for the backup image you want to copy.

   The corresponding recovery points for that date are displayed, with the time of the backup, the type of backup that was performed, and the name of the backup.

   b. Select a recovery point that you want to copy.

   The corresponding backup content (including any applications) for that recovery point is displayed.

4. Specify the copy options.

   a. Select the destination. You can either specify a location or browse to the location where the copy of your selected recovery point is going to be stored. If necessary, enter the Username and Password.

   Note: Verify that you select a location that has sufficient free space available to hold the entire VHD.

   b. Set the level of compression to "No Compression - VHD".

   Compression is not performed. Files are converted to .vhd format directly, without the need for manual operations. This option has the lowest CPU usage (fastest speed), but also has the highest disk space usage for your backup image.

5. Click Create a Copy.

   A status notification window appears and the copy process for the selected recovery point type is launched immediately.

   The recovery point image is copied from the backup source to the destination.

6. When the copy process is finished, browse to the destination and navigate to the subordinate folder corresponding to the hostname of the CA ARCserve D2D computer.

7. Open the hostname folder and navigate to the following subordinate folder:

   "VStore\S0000000001"

   For example, if your computer name is "Department_A" and you copied the recovery point (backup) to "E:\export_vhd\" you would navigate to:

   E:\export_vhd\Department_A\VStore\S0000000001

8. Open the "S0000000001" folder to locate all files with a ".vhd" extension.

   Each of these files corresponds to an actual physical disk on the source computer which can be used as regular VHD files.

Important! The VHD created by CA ARCserve D2D during the copy process may not boot in the hypervisor because the VHD files may not contain the correct drivers for the VM.

Deploy CA ARCserve D2D Remotely

After CA ARCserve D2D is installed on a server, you can then deploy it remotely to other selected servers using the CA ARCserve D2D UI. When CA ARCserve D2D is deployed remotely you get all the files and folders you would get if you deployed it locally without having to visit the remote system.

Before deploying CA ARCserve D2D remotely to other selected servers, see Remote Deployment Considerations (see page 257).

Note: This task is only available from the CA ARCserve D2D UI and not from the CA ARCserve D2D Monitor.

Videos

CA Support: How to: Deploy CA ARCserve D2D Remotely

YouTube: How to: Deploy CA ARCserve D2D Remotely

Deploy CA ARCserve D2D remotely

1. From the CA ARCserve D2D home page, select Deploy.

    The Remote Deployment dialog opens.

2. Click Add.

The Add dialog opens.

3. Enter the following information:

   a. Server name where CA ARCserve D2D will be deployed to.

   b. A valid User Name and Password to access the selected server.

      The user name should be given as <machine name>/<username>

   c. Port number. This port number is used to connect to the web-based UI.

      By default, the port number is 8014.

   d. Installation path on the remote server for CA ARCserve D2D.

      By default, this location is %Program Files%\CA\ARCserve D2D

   e. Specify if you want to use https as your web communication protocol.

   f. Specify if you want the required reboot to be performed automatically upon completion of the deployment process or if you want to reboot manually at a later time.

      A system reboot is required (now or later) for the remote deployment of CA ARCserve D2D to take effect.

      Note: During remote deployment if for any reason a reboot is not required, CA ARCserve D2D will not reboot even if you have selected automatic reboot after deployment.

   g. Specify if you want the setup to start the remote registry service automatically.

4. Click OK to close the Add dialog.

   After you click OK, the deploy tool checks whether the remote machine can be accessed with no problems. If no error is reported, then the server is automatically added to the remote deployment list. If an error is reported, you are notified of the appropriate error and the server is not added to the remote deployment list.

   The Remote Deployment dialog lists all related information for the added server.

5. Select the server for remote deployment and click Deploy Now to launch the remote deployment process.

   A status message is displayed indicating if the remote deployment was successful or not. When the remote deployment is successful, you can access CA ARCserve D2D from that remote server; however, you can only perform backups on servers that are properly licensed.

   In addition the name of the remotely deployed server is now added to the Server drop-down list on the CA ARCserve D2D home page, which lets you quickly and easily manage or view the status of these servers.

Remote Deployment Considerations

Before you deploy CA ARCserve D2D remotely to other selected servers, note the following considerations:

1. Ensure that the following ports are available:

   ■ Port 15011 (used for ADT internal communication)

   ■ Port 445 (used to access the "admin$" and %HOMEDRIVE%$, and remote registry settings)

2. Ensure that pinging of the remote machine is enabled.
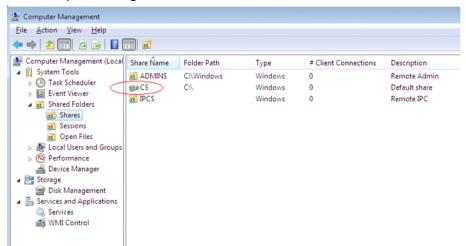
   To verify if the machine can be pinged, perform the following task:

   a. Access the Firewall advance settings for "In-Bound Rule".

   b. For the current network profile:

      ■ Enable "Networking – Echo Request (ICMPv4-In)"

      ■ Enable "Networking – Echo Request (ICMPv6-In)"

3. Allow access to the remote "admin$" share.

   If the firewall is turned on from the remote machine, to enable the access to "Admin$" on the remote machine, perform the following task:

   a. Access the Firewall advance settings for "In-Bound Rule"

   b. For the current network profile:

      ■ Enable "Netlogon Service (NP-In)"

      ■ Enable the inbound role for the network profile and allow "File and Printer Sharing (SMB-In)" for port 445

4. By default, only the build-in "administrator" has access rights to "admin$" in Windows 7. To allow non-built-in administrator (users in "Administrators" group) to access the "admin$", perform the following task:

    a. Start edit registry

    b. Locate key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"

    c. Manually create a DWORD value for "LocalAccountTokenFilterPolicy" = 0x1.

5. Allow access the remote %HOMEDrive%$ (e.g C$), ensure that the share is available from "Computer Management"

View Logs

The Activity Log contains comprehensive information about all the operations performed by CA ARCserve D2D. The log provides an audit trail of every job that is run (with the most recent activities listed first) and can be helpful in troubleshooting any problems that occur.

Note: This task is only available from the CA ARCserve D2D UI and not from the CA ARCserve D2D Monitor.

View Logs

1. From the CA ARCserve D2D home page, select View Logs.

   The CA ARCserve D2D Activity Log opens, displaying the following information:

   ■ Type of Message (Error, Warning, Information)

   ■ Job ID

   Note: The Job ID can be used to easily locate log entries that are related to a specific job and can be helpful when troubleshooting job-related problems.

   ■ Time that the message was recorded

   ■ Message indicating the activity performed or the problem encountered.

2. If necessary, you can click the Delete button to purge some or all of the log entries.

   The Delete Activity Log dialog opens.

   You can then specify to Delete all log records or Delete log records older than a specific date. If you select the "Delete log records older than" option, you can then specify from the calendar which date will be used as the older than date.

Manage Server Selection List

From the CA ARCserve D2D home page, you can select a server to manage from the Server Selection List. The Server drop-down list lets you quickly and easily manage or view the status of these servers. Servers are automatically added to the Server Selection list when you successfully deploy CA ARCserve D2D to a remote server. In addition, you can also manually add or delete a server on the Server Selection list.

Manage the Server Selection List

1. From the CA ARCserve D2D home page, click the Manage link.

   The Manage the list of servers dialog opens.

2. To delete a server from this list, select the server and click Delete.

   A confirmation warning message is displayed asking if you are sure that you want to delete this server from the list.

   Click Yes to continue and the server is no longer listed.

3. To add a server to this list, click Add.

   The Add host to server list dialog opens.

   Enter the requested information: Server Name, User Name, Password, and Port.

   If you want the communication protocol for the new server to be HTTPS, enable the https check box. By default this protocol is set to HTTP.

   Click OK to continue and the new server is added to the list.

Create a Boot Kit

Creating a boot kit consists of copying the required CA ARCserve D2D files to a USB stick that can then be used either with the Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 installation media or the Windows PE image.

Note: The created USB stick cannot be used to boot the computer. The USB stick must work with the Windows 7/Windows Vista/Windows 2008/Windows 2008R2 installation media (CD/DVD) to perform the actual BMR.

![Videos icon]

CA Support: How to: Create a Boot Kit
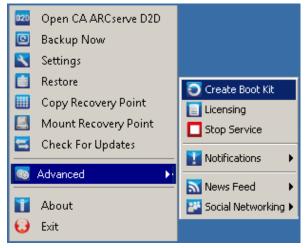
YouTube: How to: Create a Boot Kit

To create a boot kit

1. From the CA ARCserve D2D Monitor, click the Advanced option and then select Create Boot Kit.

    The CA ARCserve D2D Boot Kit wizard is launched and the Welcome screen opens.

2. Click OK to acknowledge the Welcome message.

The CA ARCserve D2D Boot Kit dialog opens.

3. Specify or browse to the location for the installed USB stick.

If you do not have a USB stick available or you do not want to create the boot image on a USB stick at this time, you can save the boot kit data temporarily to another location and then copy it to a USB stick later.

4. If necessary, select the driver integration option.

■ Add third-party NIC/SCSI/FC drivers that this computer uses.

If your server has any third-party driver installed, a copy of this driver is made during backup. If there is no third-party driver installed, this check box is not enabled.

- Add third-party NIC/SCSI/FC drivers from specified location.

  To include any necessary network (NIC), Small Computer System Interface (SCSI), or Fibre Channel (FC) drivers in the boot kit creation process. You can also manually add or delete drivers from the displayed list.

  Note: The USB stick does not contain the data of the particular computer unless you select the Add third-party NIC/SCSI/FC drivers from specified location option.

  The selected drivers are then loaded during the recovery process.

5. Click Start.

   The Boot Kit creation progress is displayed and a confirmation message is displayed when the USB stick has been successfully created.

6. After the successful creation of the Boot Kit, you can find the CA ARCserve D2D Boot Kit files on your USB stick.

   Note: The created USB stick can be used for other similar computers. A USB stick that is created from a 32-bit platform can only be used to restore a 32-bit server. A USB stick that is created from a 64-bit platform can only be used to restore a 64-bit server.

Perform Bare Metal Recovery

Bare Metal Recovery (BMR) is the process of restoring a computer system from "bare metal" including reinstalling the operating system and software applications, and then restoring the data and settings. The BMR process lets you restore a full computer with minimal effort, even to different hardware. BMR is possible because during the block-level backup process, CA ARCserve D2D not only captures the data, but also all information that is related to:

- Operating system

- Installed applications

- Configuration settings

- Necessary drivers

All relevant information that is necessary to perform a complete rebuild of the computer system from "bare metal" is backed up into a series of blocks and stored on the backup location.

CA Support:	How to: Perform a Bare Metal Recovery
YouTube:	How to: Perform a Bare Metal Recovery

Before you can perform BMR, you must have:

- At least one full backup available.

- At least 1-GB RAM installed on the virtual machine and the source server that you are recovering.

- To recover VMware virtual machines to VMware virtual machines that are configured to behave as physical servers, verify the VMware Tools application is installed on the destination virtual machine.

Dynamic disks are restored at the disk level only. If your data is backed up to a local volume on a dynamic disk, you cannot to restore this dynamic disk during BMR. In this scenario, to restore during BMR you must perform one of the following tasks and then perform BMR from the copied Recovery Point:

- Back up to a volume on another drive.

- Back up to a remote share.

- Copy a recovery point to another location.

Note: If you perform BMR to a dynamic disk, do not perform any pre-BMR disk operations (such as cleaning or deleting volume) or else the presence of the disk may not be recognized.

Regardless of which method you used to create the Boot Kit image, the BMR process is basically the same.

To restore data using bare metal recovery:

1. Insert the saved Boot Kit image media and boot the computer.

   ■ If you are using a saved Windows PE Image, insert the Boot Kit image CD/DVD.

   ■ If you are using a USB stick, insert the Windows Server Installation CD/DVD and connect the USB stick with the saved Boot Kit image.

   The BIOS Setup Utility screen is displayed.

2. From the BIOS Setup Utility screen, select the CD-ROM Drive option to launch the boot process.
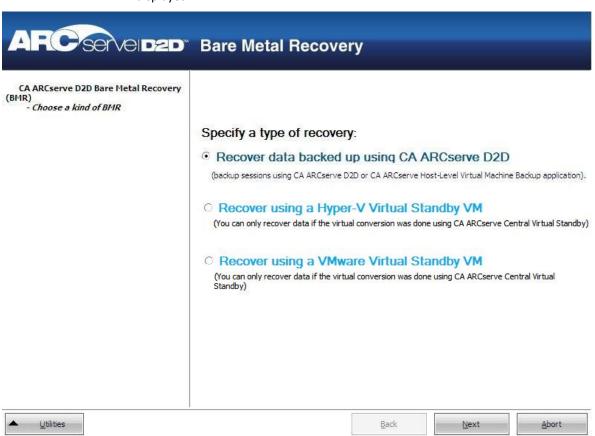
   Note: If you are using Windows PE image to perform BMR, select an architecture (x86/x64) and press Enter to continue.

```
                        Windows Boot Manager

   Choose an operating system to start:
   (Use the arrow keys to highlight your choice, then press ENTER.)


        CA ARCserve D2D Bare Metal Recovery (BMR) - x86            >
        CA ARCserve D2D Bare Metal Recovery (BMR) - x64







   To specify an advanced option for this choice, press F8.
   Seconds until the highlighted choice will be started automatically: 16




   ENTER=Choose                                              ESC=Exit
```

3. The CA ARCserve D2D language select screen is displayed. Select a language and press "Next" to continue.

   Note: If you perform BMR with a BMR USB stick and a Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 installation media (CD/DVD) not supported with a Multilingual User Interface (MUI), the language select screen is suppressed.

The Bare Metal Recovery process is initiated and the initial BMR wizard screen is displayed.

4. From the BMR wizard screen, select the type of BMR you want to perform:

■ **Recover data backed up using CA ARCserve D2D**

Lets you recover data that was backed up using CA ARCserve D2D. This option is used in connection with backup sessions performed with CA ARCserve D2D or with the CA ARCserve Central Host-Based VM Backup application.

If you select this option, continue this procedure from here.

■ **Recover using a Hyper-V Virtual Standby VM**

Lets you recover data for a machine for which virtual conversion is performed to a Hyper-V virtual machine. This option is used in connection with the CA ARCserve Central Virtual Standby application.

Note: For this option, you can only recover data if the virtual conversion to a VHD file (for Hyper-V) was performed using CA ARCserve Central Virtual Standby.

If you select this option, see Recover using a Hyper-V Virtual Standby VM (see page 281) to continue this procedure.

■ **Recover using a VMware Virtual Standby VM**

Lets you recover data for a machine for which virtual conversion is done to a VMware virtual machine. This option is used in connection with the CA ARCserve Central Virtual Standby application.

Note: For this option, you can only recover data if the virtual conversion to a VMDK file (for VMware) was performed using CA ARCserve Central Virtual Standby.

If you select this option, see Recover using a VMware Virtual Standby VM (see page 287) to continue this procedure.

5. Click Next.

    The Select a Recovery Point wizard screen is displayed.

6. From the Select a Recovery Point wizard screen, select the machine (or volume) which contains recovery points for your backup image.

    CA ARCserve D2D lets you recover from any local drive or from a network share.

    ■   If you recover from a local backup, the BMR wizard automatically detects and displays all volumes containing recovery points.

    ■   If you recover from a remote share, browse to the remote location where the recovery points are stored. If there are multiple machines containing recovery points, all machines are displayed.

        You may also need access information (User Name and Password) for the remote machine.

        Note: The network must be up and running to browse to remote recovery points. If necessary, you can check/refresh your network configuration information or you can load any missing drivers from the Utilities menu.

7. If the BMR module cannot detect any local destination volume, the "Select a Folder" dialog automatically displays. Provide the remote share where the backups are residing.

8. Select the folder where the recovery points for your backup are stored and click OK. (You can click the arrow icon to validate the connection to the selected location).

The BMR wizard screen now displays the following information:

■ Machine name (in the upper left pane).

■ Related backup information (in the upper right pane).

■ All the corresponding recovery points (in the lower left pane).

Note: To perform BMR for a UEFI system, you must boot the computer in UEFI mode. BMR does not support restoring a computer with different firmware. To verify that the boot firmware is UEFI and not BIOS, click Utilities, About.

9. Select which recovery point to restore.

   The related information for the selected recovery point is displayed (in the lower right pane). This display includes such information as the type of backup that was performed (and saved), the backup destination, and the volumes that were backed up.

   If the recovery point contains encrypted sessions (the recovery point clock icon includes a lock), a password required screen appears. Enter the session password and click OK.

   Enter Encryption Password

	OK
Current password length: 0 characters	
Maximum password length: 23 characters	Cancel

   Note: If your machine is a Domain Controller, CA ARCserve D2D supports a nonauthoritative restore of the active directory (AD) database file during BMR. (CA ARCserve D2D does not support restoring MSCS clusters).

10. Verify the recovery point that you want to restore and click Next.

A BMR wizard screen is displayed with the available recovery mode options.

11. Select the recovery mode.

The available options are Advanced Mode and Express Mode.

■ Select Advanced Mode if you want to customize the recovery process.

■ Select Express Mode if you want minimal interaction during the recovery process.

Default: Express Mode.

Note: The remainder of this procedure is applicable only if you selected the Advanced Mode and the procedure provides information to guide you through the BMR process.

12. Click Next.

The BMR utility starts locating the machine that is going to be recovered and displays the corresponding disk partition information.

The upper pane shows the disk configuration that you have on the current (target) machine and the lower pane shows the disk partition information that you had on the original (source) machine.

Important! A red X icon displaying for a source volume in the lower pane indicates that this volume contains system information and has not been assigned (mapped) to the target volume. This system information volume from the source disk must be assigned to the target disk and restored during BMR or the reboot fails.

Note: If you perform BMR and you restore the system volume to a disk which is not configured as the boot disk, it will fail to boot the machine after BMR is completed. Ensure that you are restoring the system volume to a properly configured boot disk.

Note: When restoring to another disk/volume, the capacity of new disk/volume must be the same size or larger than original disk/volume. In addition, disk resizing is for basic disks only, and not for dynamic disks.

13. If the current disk information you are seeing does not appear correct, you can access the Utilities menu and check for missing drivers.

14. If necessary, on the target volume pane you can click the Operations drop-down menu to display the available options.

From this menu, you can reset any existing partitions or you can create new partitions to correspond to the disk partitions on the source volume. (Reset means to reload the source and target disk layout information from the configure file and current OS, and discard any user changed disk layout information).

Note: When mapping to another disk, the capacity of each mapped target volume must be the same size or larger than the corresponding source volume.

15. Click on each target volume and from the pop-up menu, select the Map Volume From option to assign a source volume to this target volume.

The Select a Basic Source Volume dialog opens.

16. From Select a Basic Source Volume dialog, click the drop-down menu and select the available source volume to assign to the selected target volume. Click OK.

■ On the target volume, a checkmark icon is displayed, indicating that this target volume has been mapped to.

■ On the source volume, the red X icon changes to a green icon, indicating that this source volume has been assigned to a target volume.

17. When you are sure all volumes that you want to restore and all volumes containing system information are assigned to a target volume, click Next.

The Submit Disk Changes screen opens, displaying a summary of the selected operations. For each new volume being created, the corresponding information is displayed.

18. When you have verified the summary information is correct, click Submit. (If the information is not correct, click Cancel).

Note: All operations to the hard drive do not take effect until you submit it.

On the target machine, the new volumes are created and mapped to the corresponding source machine.

19. When the changes are completed, click OK.

The Summary of Restore Settings screen opens, displaying a summary of the volumes that are going to be restored.

Note: On the bottom of restore summary window, the drive letters listed in "Destination Volume" column are automatically generated from the Windows Preinstallation Environment (WinPE). They can be different from the drive letters listed in "Source Volume" column. However, the data is still restored to proper volume even if drive letters are different.

Summary of Restore Settings

Summary of Disk Restore Settings:

Source Disk	Destination Disk

Summary of Volume Restore Settings:

Source Volume	Destination Volume	On Disk
C:\ (32.00 GB)	\\?\Volume{80bc50db-bf9d-11df-be69-000...	Disk 0

Confirm your restore settings and click OK to continue.

[OK]   [Cancel]

20. After you have verified that the summary information is correct, click OK.

The restore process starts. The BMR wizard screen displays the restore status for each volume.

■ Depending upon the size of the volume being restored, this operation can take some time.

■ During this process you are restoring, block-by-block whatever you had backed up for that recovery point and creating a replica of the source machine on the target machine.

■ By default, the option to reboot your system automatically after recovery is selected. If necessary, you can clear this option and you can reboot manually at a later time.

■ If necessary, you can cancel or abort the operation at any time.

21. From the Utilities menu, you can access the BMR Activity Log and you can use the Save option to save the Activity Log.

    By default, the Activity Log is saved to the following location:

    X:\windows\system32\dr\log.

    Note: To avoid getting a Windows-generated error, do not save the Activity Log on your desktop or create a folder on your desktop using the "Save As" option from the BMR Activity Log window.

22. If you are restoring to dissimilar hardware (the SCSI/FC adapter which used to connect hard drives could have been changed) and no compatible driver is detected in your original system, a "driver injection" page is displayed to allow you to provide drivers for these devices.

    You can browse and select drivers to inject to the recovered system so that even if you are recovering to a machine with dissimilar hardware, you can still bring back the machine after BMR.

23. When the BMR process is completed, a confirmation notification is displayed.

Notes: After completion of BMR:

- The first backup that is performed is a Verify Backup.

- Verify that the BIOS is configured to boot from the disk on which the boot volume was restored to.

- When the machine has been rebooted, you may need to configure the network adapters manually if you restored to dissimilar hardware.

- For dynamic disks, if the status of the disk is offline, you can manually change it to online from the disk management UI (accessed by running the Diskmgmt.msc control utility).

- For dynamic disks, if the dynamic volumes are in a failed redundancy status, you can manually resynchronize the volumes from the disk management UI (accessed by running the Diskmgmt.msc control utility).

Recover using a Hyper-V Virtual Standby VM

CA ARCserve D2D provides the capability to perform Bare Metal Recovery for V2P (Virtual to Physical) machines. This feature lets you perform V2P recovery from the latest state of a standby virtual machine and helps you reduce the loss of your production machine.

After you select the "Recover using a Hyper-V Virtual Standby VM" option, perform the following steps before returning to the Bare Metal Recovery procedure to complete the process.

Follow these steps:

1. From the select the Type of Bare Metal Recovery (BMR) wizard screen, select the Recover using a Hyper-V Virtual Standby VM option.

2. Click Next.

The Select a virtual machine snapshot screen is displayed, with the Hyper-V Authentication dialog, prompting you for Hyper-v server details.

3. Enter the authentication information and click OK.

   CA ARCserve D2D detects and displays the Hyper-V Server with a listing of all the virtual machines that are converted to the specified Hyper-V server using CA ARCserve Central Virtual Standby.

4. Select the virtual machine that contains the recovery point snapshots for your backup image.

The backup sessions (recovery point snapshots) for the selected virtual machine are displayed.

5. Select the virtual machine backup session (recovery point snapshot) that you want to recover.

The corresponding details for the selected recovery point snapshot (virtual machine name, backup session name, backed up volumes) are displayed in the right pane.

In addition to selecting one of the listed recovery points, you also have the option to select the "Current State" or the "Latest State" recovery point.

– If the virtual machine that you are recovering from is powered on, the "Current State" recovery point is displayed.

– If the virtual machine that you are recovering from is powered off, the "Latest State" recovery point is displayed.

If you select the "Latest State" recovery point, an error message is displayed to inform you that the recovery point you are recovering from is the Latest (and not the Current) state and requesting that you start the virtual machine before continuing with the recovery process.

6. Verify this is the recovery point that you want to restore and click Next.

   A BMR wizard screen is displayed with the available recovery mode options.

   See Perform Bare Metal Recovery (see page 266) for the remaining steps of this procedure and continue at the corresponding step where the recovery mode is selected.

Recover using a VMware Virtual Standby VM

CA ARCserve D2D provides the capability to perform Bare Metal Recovery for V2P (Virtual to Physical) machines. This feature lets you perform V2P recovery from the latest state of a standby virtual machine and helps you reduce the loss of your production machine.

After you select the "Recover using a VMware Virtual Standby VM" option, perform the following steps before returning to the Bare Metal Recovery procedure to complete the process.

Follow these steps:

1. From the select the Type of Bare Metal Recovery (BMR) wizard screen, select the Recover using a VMware Virtual Standby VM option.

2. Click Next.

   The Select a Recovery Point screen is displayed with the ESX/VC Credentials dialog.

3. Enter the credential information and click OK.
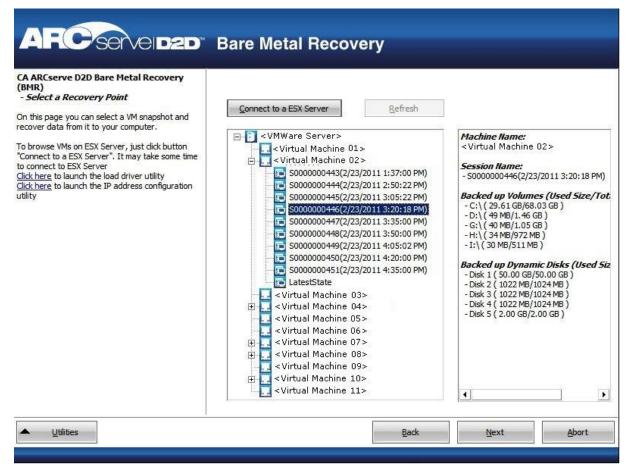
The Select a Recovery Point screen is displayed.

CA ARCserve D2D then retrieves all the recovery point snapshots for the selected VMware server and displays the VMware Server in the left pane, with a listing of all the virtual machines that are hosted on the selected VMware server.

4. Select the virtual machine which contains recovery points for your backup image.

The backup sessions (recovery point snapshots) for the selected virtual machine are displayed.

5. Select the virtual machine backup session (recovery point snapshots) that you want to recover.

The corresponding details for the selected recovery point snapshot (virtual machine name, backup session name, backed up volumes, backed up dynamic disks) are displayed in the right pane.

In addition to selecting one of the listed recovery points, you also have the option to select the "Current State" or the "Latest State" recovery point.

– If the virtual machine that you are recovering from is powered on, the "Current State" recovery point is displayed.

– If the virtual machine that you are recovering from is powered off, the "Latest State" recovery point is displayed.

If you select the "Latest State" recovery point, an error message will be displayed to inform you that the recovery point you are recovering from is the Latest (and not the Current) state and requesting that you start the virtual machine before continuing with the recovery process.

6. Verify this is the recovery point that you want to restore and click Next.

   A BMR wizard screen is displayed with the available recovery mode options.

   See Perform Bare Metal Recovery (see page 266) for the remaining steps of this procedure and continue at the corresponding step where the recovery mode is selected.

Add CA ARCserve D2D Licensing

CA ARCserve D2D requires you to license your product to receive authorized and uninterrupted access to the related components. In addition, if you want to deploy CA ARCserve D2D to remote locations, license these remote sites to take advantage of the benefits CA ARCserve D2D provides.

CA ARCserve D2D will function for a period of 30 days after you begin using it. Then, apply an appropriate license key to continue using it.

To add CA ARCserve D2D licensing, access the CA ARCserve D2D Monitor Advanced options.

Note: For Windows Core Operating Systems (Windows Server 2008/R2 Core edition), run the "CALicnse.exe" file and provide the proper license key information. The CALicnse.exe file is located in the following directory: C:\Program Files\CA\SharedComponents\CA_LIC

Follow these steps:

Note: Perform this operation locally on the computers running CA ARCserve D2D software.

1. Access the CA ARCserve D2D Monitor, click the Advanced option, and select Licensing.

    The License Verification Entry dialog opens, displaying all valid CA licensed products.

    Note: If no CA products were previously licensed, the field of this dialog is empty.

2. Enter the 25-digit license key and then click Add.

    The component is licensed.

3. Select the next component to license and repeat Step 2.

4. Click OK to accept the key after all components are defined as a licensed product.

    All components you specified are licensed.

    The license key information is stored in the ca.olf file on each of the computers that are running your CA software.

Change Server Communication Protocol

By default, CA ARCserve D2D uses the Hypertext Transfer Protocol (HTTP) for communication among all of its components. If you are concerned about the security of information that is communicated between these components (including passwords), you can select this option to change the protocol being used to Hypertext Transfer Protocol Secure (HTTPS). In addition, if you do not need this extra level of security, you can easily change the protocol being used back to HTTP.

Note: After you change the protocol from HTTP to HTTPS or from HTTPS to HTTP, restart the browser and reconnect to CA ARCserve D2D.

Follow these steps:

1. To change the protocol from HTTP to HTTPS, launch the "changeToHttps.bat" utility tool from the following default location:

   C:\Program Files\CA\ARCserve D2D\BIN

   Note: The location of the BIN folder can vary depending upon your CA ARCserve D2D installation path.

   When the protocol has been successfully changed, the following message displays:

   "Protocol has been changed to HTTPS. Use https://localhost:8014 to access CA ARCserve D2D system."

   Note: When the protocol is changed to HTTPS, a warning displays in the web browser due to a self-signed security certificate. The message asks you to either:

   ■ Ignore the warning and proceed.

   ■ Add that certificate to the browser to prevent that warning from coming back in the future.

2. To change the protocol from HTTPS to HTTP, launch the "changeToHttp.bat" utility tool from the following default location:

   C:\Program Files\CA\ARCserve D2D\BIN

   Note: The location of the BIN folder can vary depending upon your CA ARCserve D2D installation path.

   When the protocol has been successfully changed, the following message displays:

   "Protocol has been changed to HTTP. Use http://localhost:8014 to access CA ARCserve D2D system."

Install CA ARCserve D2D Updates

The process of getting and installing a CA ARCserve D2D update is a three-part process: checking for a new update, downloading the update, and then installing the update.

Note: All updates that are released for CA ARCserve D2D are cumulative. As a result, each update also includes all previously released updates to ensure that your computer is always up-to-date. The Help "About" dialog displays the update level that is installed on a computer. If necessary, you can use this information for building another server with the same configuration/patch level.

Follow these steps:

1. Launch a check for updates to contact the CA Technologies server (or staging server) to determine if any new updates are available.

   a. The check for updates can be launched automatically as scheduled. For more information about configuring the schedule settings, see Specify Updates Preferences (see page 122).

   b. The check for updates can be launched manually from the CA ARCserve D2D Help menu or from the CA ARCserve D2D Monitor.

2. If a new update is available, it is automatically downloaded from CA Technologies to the specified server (staging or client).

    Note: If necessary, the automatic download function can be disabled from the D2DPMSettings.INI configuration file. For more information, see D2DPMSettings.INI file (see page 329) in Appendix A.

    A yellow Updates icon is displayed on the home page to provide a visual indication that a new update is ready to install.

    Note: Update status balloon messages are also displayed from the CA ARCserve D2D Monitor.

3. Click the Updates icon.

    The Install Updates dialog opens to display information that is related to the available update. The dialog includes information such as description, download status, size, reboot requirement, and a link to the CA Technologies server for additional update details.

4. Review the update details, select whether it is OK to reboot the computer, and click Install to trigger the installation of the CA ARCserve D2D update.

    The new update is installed in your local computer. If the update requires a reboot and you selected the "OK to reboot machine" option, the computer reboots automatically as part of the install process. Depending on the update status of each computer, you could have different reboot requirements for each computer.

    Note: If the update requires a computer reboot and you do not select the "OK to reboot machine" option, the Install button is disabled. You can then install the update at a more convenient time.
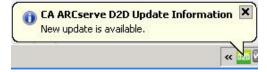
    Note: During installation of the update, CA ARCserve D2D stops the D2D web service and connection to UI is lost.

5. When the update is successfully installed, the Updates icon changes to a green status icon. The green status icon indicates that your computer has been updated and the updates function is enabled.

    Updates
    Updates is enabled.

    Updates can also be installed from the tray icon by clicking the "New Update is available" balloon message.

    CA ARCserve D2D Update Information
    New update is available.

Chapter 6: Troubleshooting CA ARCserve D2D

This section contains the following topics:

Troubleshooting Overview

When a problem is detected, CA ARCserve D2D generates a message to help you identify and resolve the problem. These messages are contained in the CA ARCserve D2D Activity Log, which is accessed from the View Logs option on the home page UI. In addition, when an incorrect action is attempted, CA ARCserve D2D generally displays a pop-up message to help you identify and quickly resolve the problem.

Unable to Reboot Hyper-V VM After BMR

If you performed BMR to a Hyper-V machine consisting of more than one disk connected to an Integrated Drive Electronics (IDE) controller and if the server does not reboot, perform the following troubleshooting procedure:

1. Verify that the disk that contains the system volume is the master disk.

    The Hyper-V BIOS searches for the system volume on the master disk (disk 1) which is connected to the master channel. If the system volume is not located on the master disk, the VM will not reboot.

    Note: Verify that the disk that contains the system volume is connected to an IDE controller. Hyper-V cannot boot from a SCSI disk.

2. If necessary, modify the Hyper-V settings, to connect the disk that contains the system volume to the IDE master channel and reboot the VM again.

Unable to Reboot VMware VM After BMR

If you performed BMR to a VMware machine consisting of more than one disk connected to an Integrated Drive Electronics (IDE) controller or a SCSI adapter and the server does not reboot, perform the following troubleshooting procedure:

1. Verify that the disk that contains the system volume is the master disk.

    The VMware BIOS searches for the system volume on the Master disk (disk 0) which is connected the master channel. If the system volume is not on the Master disk, the VM does not reboot.

2. If necessary, modify the VMware settings, to connect the disk that contains the system volume to the IDE master channel and reboot the VM again.

3. If the disk is a SCSI disk, verify the disk which contains boot volume is the first disk which connects to the SCSI adapter. If not, assign the boot disk from the VMware BIOS.

4. Verify the disk which contains boot volume is in the previous eight disks, because the VMware BIOS only detect eight disks during the boot. If there are more than seven disks ahead the disk which contains system volumes connected to the SCSI adapter, the VM cannot boot.

Unable to boot the server after performing a BMR

Unable to boot the server after performing a BMR.

Symptom:

When the source machine is an Active Directory server performing a BMR to a physical machine with different hardware or to a virtual machine on a hyper-v server, the server does not boot and a blue screen displays with the following message:

STOP: c00002e2 Directory Services could not start because of the following error: a device attached to the system is not functioning. Error status: 0xc0000001.

Solution:

Reboot the system to the BMR PE environment, rename all *.log files in the C:\Windows\NTDS folder, and restart the system. For example, rename the file edb.log to edb.log.old and restart the system.

After BMR, dynamic volumes are not recognized by the operating system

To keep dynamic disks in a consistent state, the Windows operating system automatically synchronizes the Logical Disk Manager (LDM) metadata on each dynamic disk. So when BMR restores one dynamic disk and brings it online, the LDM metadata on this disk is automatically updated by the operating system. This may result in a dynamic volume not being recognized by the operating system and missing after the reboot.

To remedy this problem, when you perform BMR with multiple dynamic disks, do not perform any pre-BMR disk operations such as cleaning, deleting volume, and so on.

Slow throughput performance during BMR

This problem can be caused by SATA controllers with "AHCI" enabled.

During BMR, CA ARCserve D2D will install drivers for critical unknown devices. If the device already has a driver installed, CA ARCserve D2D will not update that driver again. For some devices, Windows 7PE may have the drivers for them, but these drivers may not be the best ones and this can cause the BMR to run too slow.

To remedy this problem, perform one of the following tasks:

- Check if the driver pool folder contains the newest disk drivers. If it does, and you are restoring to the original machine, please install the new driver from the driver pool folder. If you are restoring to alternate machine, download the latest disk drivers from the Internet, and load it before you start data recovery. To load the driver, you can use the "drvload.exe" utility, which is included in Windows PE.

- Change the device operating mode from "AHCI" (Advanced Host Controller Interface) to Compatibility mode. (Compatibility mode provides a better throughput).

Unable to display CA ARCserve D2D UI in Firefox

If you are using Firefox to connect to the local CA ARCserve D2D server, where the browser and CA ARCserve D2D are both on the same machine, certain proxy settings may cause the CA ARCserve D2D UI not to be displayed.

If this condition occurs, connect to the loopback address 127.0.0.1 or use the hostname in Firefox instead of using localhost.

Unable to display CA ARCserve D2D home page when you attempt to open it from Internet Explorer (IE) web browser

If you are using an Internet Explorer (IE) web browser to access the CA ARCserve D2D home page and it does not display, it may be that the CA ARCserve D2D website is not included as a "Trusted Site" in your IE browser.

If this condition occurs, add this website as a Trusted Site in your IE browser. For more information about adding a website as a Trusted Site, see Security zones: adding or removing websites.

Unable to install/uninstall CA ARCserve D2D if a previous attempt was interrupted

If during an attempt to install or uninstall CA ARCserve D2D, the install/uninstall process was interrupted, you may not be able to successfully continue and complete the process.

For example, any of the following conditions could cause a partial install/uninstall state:

- Your network connection becomes broken while you are installing CA ARCserve D2D from a remote computer.

- Your computer is shut down in middle of install/uninstall process.

- You encounter a power outage during install/uninstall and there is no Uninterruptible Power Supply (UPS).

- You click the Cancel button during CA ARCserve D2D install/uninstall process.

To resolve this problem, perform the following steps:

1. Enter "regedit" in the Run dialog and click OK to open Registry Editor.

2. Locate and delete the following entry:

   "HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D"

3. Use the search option in the Registry Editor to locate and delete <u>all</u> occurrences of the following string:

    ■ [CA ARCserve D2D for x86]: {97270DB5-DB8F-467F-9C52-1AF57C55EA60}

    ■ [CA ARCserve D2D for x64]: {611E0884-4C83-4740-A3A9-9EB00D784E8D}

4. Use the search option in the Registry Editor to locate and delete all occurrences of the string "CA ARCserve D2D"under the following key:

    HKEY_CLASSES_ROOT\Installer\Products

    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Products

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

5. From the command line, delete the service by entering the following commands:

    sc delete ShProvd

    sc delete CASAD2DWebSvc

6. Reboot the computer and re-attempt the installation/uninstallation of CA ARCserve D2D.

Windows failed to start after CA ARCserve D2D has just been installed

If Windows failed to start with the following error after CA ARCserve D2D has recently been installed, it can be caused by a Windows internal failure.

File: ARCFlashVolDrv.sys

Status: 0xc0000098

Info: Windows failed to load because a required file is missing, or corrupt.

The probable causes for this problem are:

■ User temporary folder is not writable

■ Insufficient privilege

■ Windows update database corrupted

Important! This procedure contains information about modifying the registry. Before you modify the registry, make sure to create a backup of the registry and ensure that you understand how to restore the registry if a problem occurs. For more information about how to back up, restore, and edit the registry, see the relevant Microsoft Knowledge Base articles at <u>support.microsoft.com</u>.

To resolve this problem, perform the following steps to uninstall the driver:

1. For CA ARCserve D2D r16, boot the computer with the BMR ISO image.

    For CA ARCserve D2D r16.5 or later, use the Create Boot Kit for Bare Metal Recovery utility to create the BMR ISO image if you do not already have it.

2. Click Run from the Utilities menu.

3. Enter "regedit" in the Run dialog and click OK to open Registry Editor.

4. Select HKEY_LOCAL_MACHINE and click "Load Hive..." from the File menu in the Registry Editor.

5. Locate SYSTEM file under the %systemroot%\system32\config directory on your system and click open.

6. Enter a name for the hive to be loaded.

7. From the Registry Editor, check the "Current" entry under "HKEY_LOCAL_MACHINE\SYSTEM\Select".

8. Depending on the Current value that is displayed, delete the corresponding entries under the new hive that was just loaded:

    For example:

    ■   If the Current Value is **1**, then delete the following entries:

        –   HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet001**\Services\ARC FlashVolDrv

        –   HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet001**\Services\Eve ntlog\System\ARCFlashVolDrv

    ■   If the Current Value is **2**, then delete the following entries:

        –   HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet002**\Services\ARC FlashVolDrv

        –   HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet002**\Services\Eve ntlog\System\ARCFlashVolDrv

9. Depending on the Current value that is displayed, delete the corresponding value "ARCFlashVolDrv" for the following registry keys:

   Important! The "LowerFilters" registry key may also contain other Windows driver names. Be sure to delete only the "ARCFlashVolDrv" value from the list. Do not delete the entire registry key or any other driver names from within the key.

   For example:

   - If the Current Value is **1**, then delete the following entries:

     – HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet001**\Control\Class \{533C5B84-EC70-11D2-9505-00C04F79DEAF}\LowerFilters

     – HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet001**\Control\Class \{71A27CDD-812A-11D0-BEC7-08002BE2092F}\LowerFilters

   - If the Current Value is **2**, then delete the following entries:

     – HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet002**\Control\Class \{533C5B84-EC70-11D2-9505-00C04F79DEAF}\LowerFilters

     – HKEY_LOCAL_MACHINE\%your_hive_name%**ControlSet002**\Control\Class \{71A27CDD-812A-11D0-BEC7-08002BE2092F}\LowerFilters

10. Click "Unload Hive..." from the File menu in the Registry Editor.

11. Reboot the computer and start Windows typically.

12. Perform the following troubleshooting steps:

    a. Verify that the user account has administrator privileges on this machine.

    b. Verify that the user account has write permissions on the following temp folders:

       - %windir%/temp

       - %temp%

    c. For Microsoft Windows Vista and Microsoft Windows 2008 and later, download and run the Microsoft System Update Readiness Tool. This tool helps to fix any inconsistencies or corruption in the installed updates and system files.

    d. Determine if there are any pending Windows updates or reboots and take the necessary action. Perform one of the following tasks to show Windows Update related information for the computer:

       - Click Start, All Programs, Windows Update.

       - Access windowsupdate.microsoft.com.

    e. If there are problems installing several Windows Updates, then examine why the updates cannot be installed on this computer before proceeding to the next step.

13. Reboot the computer and start Windows typically.

14. Reinstall the ARCFlashVolDrv driver by running "ARCFlashVolDrvINSTALL.exe –i –output=c:\install.log" after the machine reboot.

   ■ ARCFlashVolDrvINSTALL.exe is located on D2D_HOME\bin\Driver.

   ■ D2D_HOME is located on the CA ARCserve D2D install path.

15. Reboot the computer and start Windows typically.

Unable to display Exchange backup session for Windows Small Business Server 2003

By default, Windows Small Business Server 2003 disables the Exchange Writer. As a result a successful Exchange backup session are not displayed at the backup destination when attempting to restore. To remedy this problem, you can manually turn on the Exchange writer for use with CA ARCserve D2D.

For more information about turning on the Exchange writer, see How to turn on the Exchange writer for the Volume Shadow Copy service in Windows Small Business Server 2003.

SQL Server backup failed due to "out of memory" error

This is caused by a Microsoft known issue: Volume Shadow Copy Service (VSS) cannot create a volume snapshot even when VSS has sufficient memory space.

To resolve this problem, apply the Microsoft patch <http://support.microsoft.com/kb/940239/>

Failed to Restore Exchange Object with Invalid Service Error

If you are attempting to restore an Exchange object (mail, mailbox folder, or entire mailbox) to either the original or an alternate location and the job fails with an invalid service error, check if the Microsoft Exchange Information Store Service is in a running state and if the database which the current user (administrator) belongs to is in a mounted state.

If both states are correct check for an "MAPI_E_NETWORK_ERROR 80040115" error. If you have this error, you can change your protocol and host file as follows:

1. Disable the IPv6 or select the IPv4 as the preferred protocol in the Network properties.

2. Add the following lines into the host file:

   127.0.0.1   <hostname of the computer>

   127.0.0.1   <FQDN of the computer>

   actual IPv4 address   <hostname of the computer>

   actual IPv4 address   <FQDN of the computer>

3. Reboot the machine.

Catalog Job fails when backing up a large number of files on Windows 2003 x86 machine

For Windows 2003 x86, if you are attempting to back up a large number of files (in excess of 80 million) and the catalog generation job fails, perform the following:

1. Locate the boot.ini file (c:\boot.ini) and increase the virtual memory from 2 GB (default value) to 3 GB by adding the "/3GB" switch as follows:

   [boot loader]

   timeout=30

   default=multi(0)disk(0)rdisk(0)partiti on(2)\WINDOWS

   [operating systems]

   multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Windows Server 2003, Enterprise" /noexecute=optout /fastdetect **/3GB**

   Note: For more information about increasing memory support, see
   http://msdn.microsoft.com/en-us/windows/hardware/gg487508

2. Reboot the computer.

3. Set the "DoListSort" registry value as follows:

   ■ Enter "regedit" in the Run dialog and click OK to open Registry Editor.

   ■ Locate the following entry:

   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D

   ■ Create a DWORD named "DoListSort" with the value set to 1.

Catalog Job fails when backing up a large number of files because not enough space

If you are attempting to back up a large number of files and the catalog generation job fails because there is not enough available space in the ARCserve D2D home folder, perform the following task to create a new temp location:

Important! Verify that this new location contains enough free space to hold all of your catalog temporary data.

1. Within the ARCserve D2D home folder, access the Configuration folder. (The ARCserve D2D home folder is located on the CA ARCserve D2D install path).

   Program Files\CA\ARCserve D2D\Configuration

2. Within the Configuration folder, create a "CatalogMgrDll.ini" file. (File name is case-sensitive).

3. Within the new "CatalogMgrDll.ini" file, add the following content:

   [Common]
   TmpPath4Catalog="I:\catalogtemp"

4. Run the backup job again.

   The catalog generation part of the job will now go to the newly created temp folder.

Failed to validate backup destination

If you are attempting to configure your backup settings from another machine to a Windows XP shared destination and you are unable to save these settings, it may be because the same user is using more than one user name to access this CA ARCserve D2D configured shared destination.

For example:

- You have two machines, A and B

- Machine A is a Windows XP operating system and exposes a shared folder

- Machine B has CA ARCserve D2D installed

- User on Machine B attempts to configure the CA ARCserve D2D backup destination to this shared folder exposed by Machine A

- User on Machine B will not be able to save backup destination setting because it fails to connect to this shared folder.
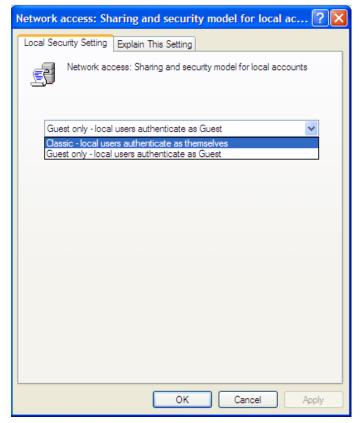
If this happens, you can change the local security policy on your Windows XP machine as follows:

1. Access the local Group Policy editor (gpedit.msc) utility.

    gpedit.msc -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options

2. Select "Network access: Sharing and security model for local accounts" and change the value from "Guest only" to "Classic".

Unable to change backup destination folder to ARCserve D2D View

On Windows Vista and later operating systems, if you create an account which belongs to a local administrator group, and from this new account you attempt to change the CA ARCserve D2D backup destination folder to ARCserve D2D View, the folder view cannot be changed and no error message is displayed. This can happen when the User Account Control is enabled.

If this condition occurs, you can either disable the User Account Control or you can grant Modify privileges to the created Windows account.

To disable the User Account Control, perform the following task:

1. From the Windows Control Panel, select User Accounts, User Accounts, and then Change User Account Control Settings.

   The User Account Control Settings dialog displays.

2. For the Choose when to be notified about changes to your computer option, drag the slide bar to the bottom (Never notify).

3. When you disable the User Account Control, reboot your computer.

To grant Modify privileges to the created Windows account, perform the following task:

1. From the Windows Explorer view, navigate to the specified backup destination.

2. Right-click on the backup destination folder, select Properties, and click the Security tab.

3. Click Edit and Add a user for this destination folder.

    The Permissions dialog is displayed.
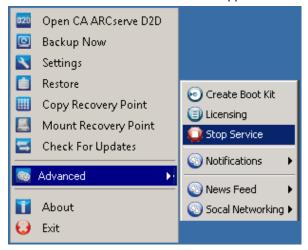
4. For this user, check the Modify permissions option to allow control specifically to this user and add it to the folder security list.

CA ARCserve D2D Service could not be started because of port conflict

The port that CA ARCserve D2D uses can conflict with the default port that Tomcat uses. This conflict causes Tomcat to fail when CA ARCserve D2D is started before it. To remedy this problem, you can change the Tomcat default port as follows:

1. Access the CA ARCserve D2D Monitor, click the Advanced option, and select Stop Service.

   The CA ARCserve D2D Web Service is stopped.

2. Access the Tomcat server.xml file to edit/configure the behavior of Tomcat.

   The Tomcat server.xml file is located in the following folder structure:

   C:\Program Files\CA\ARCserve D2D\TOMCAT\conf

3.   Locate the <Server> tag inside the server.xml file.

4. Edit the <Server> tag as follows:

    From:

    <Server>

    To:

    <Server port="8015" shutdown="SHUTDOWN">

5. Save and close the server.xml file.

    The command to shut down Tomcat has now been configured so that it must be received by the server on the named port (8015).

6. Access the CA ARCserve D2D Monitor, click the Advanced option, and select Start Service.

    The CA ARCserve D2D Web Service is started.

Unable to Connect to Cloud

If you are attempting to file copy to cloud, but cannot connect your machine to the cloud server, perform the following troubleshooting procedure:

1. From the File Copy Settings Destination dialog, click the Configure button to display the Cloud Configuration dialog and verify the following are correct:

   ■ Proxy credentials (Username and password)

   ■ Proxy Server IP address and corresponding port number

   ■ Access key and Secret key for access to the specified proxy server

   ■ Vendor URL address for the specified cloud provider

2. To eliminate any potential clock skew error, verify that your machine has the correct time zone set and the clock is in sync with the global time.

3. Resubmit the file copy job.

Backup sessions for CA ARCserve D2D r16 do not include any Microsoft SQL database information

After upgrading from CA ARCserve D2D r15 to r16, the backup sessions do not include any Microsoft SQL database information. This may be caused by the SQL server not starting automatically in a virtual environment. If this occurs, verify that the SQL database is in a good state and retry the backup.

If the problem persists, you can change the startup type of the SQL server to "Automatic (Delayed Start)".

Merge Session is Skipped

If the oldest recovery point is skipped in the merge operation, perform the following troubleshooting procedure after you submit a new backup when the specified recovery point count limit is exceeded:

1. Open the Mount Recovery Point dialog to see if you have any recovery points mounted. If any recovery points are mounted, dismount them.

2. Open Windows Explorer and switch to the backup destination to see if the session is under the ARCserve D2D View. If it is, change to the Windows Explorer View.

3. Verify if any file copy jobs are running.

Failed to create snapshot for selected volumes

If a volume does not have enough disk space, the backup job can fail with the error message "Failed to create snapshot for selected volumes". If the backup job fails, you can perform either task:

■ Free up some disk space on the volumes being backed up.

■ Reconfigure the Volume Shadow Copy settings to save shadow copy to a volume with sufficient free disk space.

Job Monitor data speed displays a 0 or some other abnormal value

Reason:

Windows Performance Counters are disabled.

Action:

From the Registry Editor, delete or enable the following registry keys on all Windows versions:

■ Perflib

    Path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

    Name: "Disable Performance Counters"

    Type: DWORD

    Value: Set to 0 to enable performance counter.

■ Performance

    Path: HKLM\SYSTEM\CurrentControlSet\Services\PerfProc\Performance

    Name: "Disable Performance Counters"

    Type: DWORD

    Value: Set to 0 to enable performance counter.

Merge Job Failed when Configured to Retain Recovery Sets

Reason:

Possible network failure or busy network.

Action:

Perform any of the following to fix this problem:

- Run a new backup job which will trigger a merge job after the backup is completed.

- Access the Backup Settings dialog and save the Retention Setting again.

- Restart the D2D web service.

Merge Job Fails After Being Paused by a Restore Job

If a merge job is running and you perform another job at the same time, the merge job will automatically pause. After the other job is finished, if you attempt to resume the merge job, then the merge job will fail. This may be caused by the session not being released after the other job is finished, and the unreleased session could not be merged. If a mounted session was not cleanly dismounted, the session lock may not disappear and as a result the session will not be released after the job is finished. If this occurs, run the following command to force a clean session dismount:

"%caarcflash_home%\bin\driver\afstorhbainstall.exe" -d all
-output=c:\stopmountingdriver.log

If the problem persists, use Live Chat to contact CA Support. Live Chat lets you optimize intelligent conversation between you and the CA ARCserve D2D Technical Support team, allowing you to address your concerns and questions immediately, while still maintaining access to the product.

Unable to Change Destination to Removable Device

If you are attempting to configure your backup destination setting to a removable device, and you are unable to save the setting without a failure, it may be caused by the local security policy settings. If this occurs, perform the following troubleshooting procedure:

Note: This problem may occur in multiple cases, such as when you are attempting to browse to a destination or saving a backup destination setting.

1. Run GPEDIT.msc to open the "Local Group Policy Editor" dialog.

2. Select Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy.

3. Double click "Audit object access" to access the "Audit object access Properties" dialog.

4. On the Local Security Settings tab, uncheck the Success and Failure options, and click Apply to save the settings.

5. Reboot the server or run 'GPupdate/force'. (If you run 'GPupdate/force' then after the command is completed, log off and then log back on).

6. If the trouble continues, the computer is most likely a part of a domain. You will need to find out which group policy has the setting enabled by running the following in an administrative command-prompt:
gpresult /H C:\gpresult.html

7. Open the file C:\gpresult.html and navigate to the following section:

   Computer Details -> Settings -> Policies -> Windows Settings -> Security Settings -> Local Policies\Audit Policy -> Audit Object Access.

   Note: For Windows 7 operating systems, the location of Audit object access in the file C:\gpresult.html varies slightly by replacing "Computer Details -> Settings" with "Computer Configuration" in the navigation path.

8. The group policy is located under the "Winning GPO" column. Edit that group policy, and then reboot the server.

If the problem persists, use Live Chat to contact CA Support. Live Chat lets you optimize intelligent conversation between you and the CA ARCserve D2D Technical Support team, allowing you to address your concerns and questions immediately, while still maintaining access to the product.

Troubleshooting Remote Deployment Issues

When a problem is detected, CA ARCserve D2D generates a message to help you identify and resolve the problem. These messages are contained in the CA ARCserve D2D Activity Log, which is accessed from the View Logs option on the home page UI. In addition, when an incorrect action is attempted, CA ARCserve D2D generally displays a pop-up message to help you identify and quickly resolve the problem.

This section contains the following topics:

Unable to Access CA ARCserve D2D After Reboot

If you are not able to access the CA ARCserve D2D UI, perform the following troubleshooting procedure:

1. From the Add or Remove Programs dialog, click the Add/Remove Windows Components option to access the Windows Components Wizard screen and remove the Internet Explorer Enhanced Security Configuration component.

2. Add the host name URL to the Trusted Sites in Internet Explorer.

3. Adjust the security level in Internet Explorer.

If the problem persists, use Live Chat to contact CA Support. Live Chat lets you optimize intelligent conversation between you and the CA ARCserve D2D Technical Support team, allowing you to address your concerns and questions immediately, while still maintaining access to the product.

Setup cannot connect to <<machine name>> during Remote Deployment

If you encounter the error "Setup cannot connect to <<machine name>>. The network share \\<<machine name>>\admin$ is not available using the network.", check the following items to resolve the problem:

■ The Username/Password details provided in the Deploy UI are correct.

■ The target host is reachable over the network from the current CA ARCserve D2D server.

■ The file and printer sharing service is enabled on the target host. If the firewall is enabled on the target host, an exception should be added for File and Printer Sharing service.

If the problem persists, use Live Chat to contact CA Support. Live Chat lets you optimize intelligent conversation between you and the CA ARCserve D2D Technical Support team, allowing you to address your concerns and questions immediately, while still maintaining access to the product.

Troubleshooting Update Issues

When a problem is detected, CA ARCserve D2D generates a message to help you identify and resolve the problem. These messages are contained in the CA ARCserve D2D Activity Log, which is accessed from the View Logs option on the home page UI. In addition, when an incorrect action is attempted, CA ARCserve D2D generally displays a pop-up message to help you identify and quickly resolve the problem.

This section contains the following topics:

Unable to Access CA ARCserve D2D After Reboot

If you are not able to access the CA ARCserve D2D UI, perform the following troubleshooting procedure:

1. From the Add or Remove Programs dialog, click the Add/Remove Windows Components option to access the Windows Components Wizard screen and remove the Internet Explorer Enhanced Security Configuration component.

2. Add the host name URL to the Trusted Sites in Internet Explorer.

3. Adjust the security level in Internet Explorer.

If the problem persists, use Live Chat to contact CA Support. Live Chat lets you optimize intelligent conversation between you and the CA ARCserve D2D Technical Support team, allowing you to address your concerns and questions immediately, while still maintaining access to the product.

Appendix A: Frequently Asked Questions (FAQ)

This section contains the following topics:

File Copy Related FAQ

The following Frequently Asked Questions are related to the File Copy feature.

Can I restore data if I lose the encryption password?

No. To restore encrypted data that was backed up, you must provide the proper encryption password.

What is the maximum file size that can be backed up/restored (for example large Outlook PST files, CAD files, video broadcast files)?

There is no limitation for the file size that can be backed up or restored using CA ARCserve D2D (for example large Outlook PST files, CAD files, video broadcast files).

Are there any preset files/folders which will not be deleted during a File Copy – Delete Source job?

Yes. CA ARCserve D2D will exclude deletion of all system state files and application files and folders during a File Copy – Delete Source job. CA ARCserve D2D only supports Microsoft Exchange and SQL Server and the list of application files is obtained by querying the VSS writers.

Does a File Copy job copy data directly from the local source disks?

A File Copy job will mount the CA ARCserve D2D backup disks and it will then copy the data. It does not actually read from the local source disks.

What is the maximum file size that can be stored on Amazon S3 cloud?

There is no maximum file size that can be stored on an Amazon S3 cloud location.

The minimum size for a block-level incremental (BLI) backup is 64K. Does this mean that for any file size less than 64K, CA ARCserve D2D will copy the entire file?

Yes. The granularity limit for block-level incremental backups is set for 64K.

Can a File Copy job and a Backup run simultaneously?

Yes. CA ARCserve D2D allows both jobs to be run at the same time.

During a File Copy job, will the stub files be copied again?

No. During a File Copy job, CA ARCserve D2D will ignore the stub files and not copy them again.

Does every File Copy job initiate a VSS snapshot like a regular CA ARCserve D2D Backup job?

No. The VSS snapshot is performed only during a Backup job and not during a File Copy job.

Will a File Copy that is stored on an Amazon S3 cloud location be open source archive format?

No. A File Copy that is stored on an Amazon S3 cloud location will be proprietary only format.

If a File Copy – Delete Source job deletes files, will I be able to perform a BMR from the file copy destination?

No. You just need to perform a restore from the file copy destination. The files that are deleted are only deleted from the source, and not from the recovery point. The recovery points contain the full volume information necessary to perform a complete BMR.

For a File Copy job, is the Delete Source option enabled by default?

No. This option is selected by you when you add a policy.

Encryption Related FAQ

The following Frequently Asked Questions are related to the Encryption feature.

If I change the encryption type or the encryption password and the maximum number of recovery points are then reached, what happens?

The image consolidation during backups will continue as usual for images with the older password. When the remaining oldest image is the last Full Backup with the old password, that Full Backup will be deleted.

If I enter a new encryption password, will the old encryption password be asked for first?

No. CA ARCserve D2D will immediately apply the new password and no longer request the old password.

What happens to data which is already encrypted either using Windows Encrypting File System (EFS) or a third-party encryption system?

- For Windows EFS encryption, CA ARCserve D2D will write in encrypted format used in the EFS and BitLocker format.

- For third-party-encryption, it depends on the technology. If volume encryption is enabled or locked, CA ARCserve D2D will not be able to read it and will generate an error.

Updates Related FAQ

The following Frequently Asked Questions are related to the Updates feature.

Can I use scripted information for specifying Updates proxy settings?

Yes. You can select the "Use Browser Settings" option on the Proxy Settings dialog to inherit the browser proxy settings (accessed from the Updates Preferences).

Can I use a workstation node as an Updates staging server?

Yes. Your workstation node can be used as a staging server for downloading CA ARCserve D2D updates.

Can I manage/operate Updates centrally or do I need to configure each node separately (one by one)?

No. You must configure each node individually for Updates.

Does an Updates staging server need a separate CA ARCserve D2D license if I am not using any CA ARCserve D2D functions on this staging server?

No. If you are not using CA ARCserve D2D for any function other than just as an Updates staging server, you do not need to have a separate CA ARCserve D2D license for the staging server.

Exchange Granular Restore FAQ

The following Frequently Asked Questions are related to the Exchange Granular-Level Restore feature.

Is an Exchange search limited to the email subject or can I search on attachments?

The most granular-level search that CA ARCserve D2D can perform is for an email subject.

Can I only restore mail objects for granular-level restore or can I also restore such objects as contacts or calendars?

CA ARCserve D2D allows you to only restore mail objects (mailboxes, mailbox folders, or mail).

Can I restore an entire mailbox and will it overwrite the existing data in the mailbox store?

Yes you can restore an entire mailbox and it will not overwrite the existing data in the mailbox store.

Appendix B: Configuration Files

Configuration (.INI) files are plain-text files that contain configuration information. The various configuration options and process rules are stored in these INI configuration files. You can manually edit an INI file, import/export it, or ignore it and pretend it does not exist. ("INI" stands for *initialization*).

This section contains the following topics:

Use the D2DPMSettings.INI File to Disable Automatic Downloads

The D2DPMSettings.INI is the configuration file that is used to define how the CA ARCserve D2D updates are collected. By default, the D2DPMSettings.INI is located in the <ProductHome>\Update Manager directory and can be viewed or edited using a text editing application such as Notepad.

Syntax

The following options are available for CA ARCserve D2D updates:

[DownloadServer]
        ServerType=1
        ServerName=155.35.16.61
        Protocol=HTTP
        Port=8014
        ServerCount=2

[Schedule]
        AutoCheckUpdate=1
        AutoDownload=1
        DisableActiveUpdate=0
        WeekDay=1
        Hour=04

[ProxySettings]
        UseProxy=0
        ProxyRequireAuth=0
        ProxyServer=
        ProxyPort=
        ProxyUserName =
        ProxyPassword =

```
[DOWNLOADCONFIG]
        RetryCount=3
        TimeOutForEachTry=60
        PacketCount=16

[Debug]
        DebugLevel=3
        LogFileSize=10

[D2DUpdates]
        path=C:\Program Files\CA\ARCserve D2D\D2DUpdates

[CA ARCserve D2D]
        Date=0
        Time=0
        [Staging server #1]
        Server name = stgsvr1
        Server port = 8014

        [Staging server #2]
        Server name = stgsvr2
        Server port = 8014
```

Download Server:

■ **ServerType**

0 = Download server will contact the CA Technologies server directly for updates. (Default value)

1 = Download server will contact the specified staging server for updates.

■ **ServerName**

Name or IP address of the staging server that will be used (only if ServerType is set to 1).

■ **Protocol**

CA ARCserve D2D only supports HTTP communication protocol.

■ **Port**

Port number used for communication. By default this is set to 80.

■ **Server Count**

Displays total number of configured staging servers.

Schedule:

- **AutoCheckUpdate**

  0 = Automatic check for updates is disabled. Check for updates must be triggered manually.

  1 = Automatic check for updates is enabled. Check for updates will be triggered automatically as scheduled. (Default value)

- **AutoDownload**

  0 = Automatic download is disabled. The download must be triggered manually.

  1 = Automatic download is enabled. Download will be coordinated with check for updates and automatically triggered when a new update is determined. (Default value)

- **DisableActiveUpdate**

  0 = Active update is enabled. Automatic check for updates and download functions are enabled. (Default value)

  1 = Active update is disabled. Check for updates and download functions must be triggered manually.

- **WeekDay**

  Scheduled day of the week that the automatic check for updates will be performed:

  > 0 = every day
  >
  > 1 = Sunday
  >
  > 2 = Monday
  >
  > 3 = Tuesday
  >
  > 4 = Wednesday
  >
  > 5 = Thursday
  >
  > 6 = Friday
  >
  > 7 = Saturday

  Note: Since there is no default setting for the day or hour that these checks will be automatically performed, CA ARCserve D2D will randomly assign these values at the time of installation.

- **Hour**

  Scheduled time of the specified "WeekDay" day that the automatic check for updates will be performed (in 24-hour time settings).

ProxySettings:

■ **UseProxy**

0 = No proxy is required. Instead the client server will connect directly to the CA Technologies server to obtain update information.

1 = Use the provided proxy server settings. If you select this option, you must also include the IP address (or machine name) of the proxy server and the corresponding port number that is used by the proxy server for internet connections.

■ **ProxyRequireAuth**

0 = proxy server does not require authentication.

1 = proxy server requires authentication information (which enables User ID and Password fields).

■ **ProxyServer**

Proxy server name (or IP address) will be entered and stored here.

■ **ProxyPort**

Port number used by the proxy server for internet connections. (Only numbers will be accepted).

DOWNLOADCONFIG:

■ **RetryCount**

Number of times CA ARCserve D2D will attempt to download a new update. If after a specified number of retry attempts, the download still cannot continue, an error message will be displayed indicating the most likely reason for the failure.

RetryCount range is: 1 - 5

Default value = 3

■ **TimeOutForEachTry**

Time (in minutes) that CA ARCserve D2D will wait between retry attempts to download a new update.

Default value = 60 minutes

■ **PacketCount**

Number of packets downloaded from CA Technologies support server to your client server during each transfer, with each packet size at 1KB. The available range is 4 to 64 packets.

Default value = 16 packets

Note: During download, CA ARCserve D2D divides the update file into individual (PacketCount) 1KB chunks, which are then efficiently routed over the internet and reassembled into the original file at the destination.

Debug:

■ **DebugLevel**

Level of details to include in the debug log. A higher debug level value means more detailed information will be included in the debug log. The available range is 0 to 4.

Default value = 3

■ **LogFileSize**

Size (in MB) of the debug log file.

Default value = 10 MB

D2DUpdates:

Path location for downloaded updates.

Default path = <ProductHome>\D2DUpdates

Important! The path of the download directory should always have a "D2DUpdates" folder at the end (for example: "C:\Test\D2DUpdates"). If this path is changed, then you must also manually update the docBase value to include this changed path. The docBase parameter is located in the following file "<ProductHome>\TOMCAT\conf\server.xml" and can be changed by stopping the web service. This is mandatory otherwise other CA ARCserve D2D machines cannot access this CA ARCserve D2D machine as a staging server.

CA ARCserve D2D:

■ **Date/Time**

Displays the last modified date and time of the available update information file (AvailableUpdateInfoDll_x86.dll / AvailableUpdateInfoDll_x64.dll) that has been downloaded from the CA Technologies server to your client server. (After the first check, these date and time values will become reference points for future checks to determine if the file has changed).

When triggered, CA ARCserve D2D will check the date and time values of the available patch information file from the CA Technologies server to determine if it has been modified since the last check. If the values have changed, the latest file will be downloaded from the site and the date and time values in this configuration file will be updated to display the new information.

Date format = yyyymmdd

Time format = hhmmss

- **[Staging server #1] ... [Staging server #2] ...**

  Server name =

  Server port =

  This section displays all the configured staging servers (server name and port) in the order which they are configured as download servers in the Updates Preferences dialog.

  The first listed server will be designated as the primary staging server. CA ARCserve D2D will initially attempt to connect to the primary staging server. If for any reason the first listed server is not available, then the next listed server will become the primary staging server. The same sequence will be continued until the last listed server becomes the primary staging server. (The staging server list is limited to the maximum of 5 servers).

Appendix C: Files Affected During Installation/Uninstallation

By default, CA ARCserve D2D is installed in the following location: C:\Program Files\CA\ARCserve D2D and is uninstalled using the standard Add or Remove Programs application located in the Windows Control Panel. However, during the CA ARCserve D2D installation and uninstallation processes, some files may not be located or uninstalled as expected. This appendix contains information about those files that are unexpectedly affected during the installation/uninstallation process.

This section contains the following topics:

Files Not Removed During Uninstallation

The following is a listing of the CA ARCserve D2D file names and corresponding paths that are not removed by the uninstaller after the uninstallation process is completed:

Files left behind by Uninstaller

C:\D2DPMConfig.txt

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CA Licensing User Help.chm

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CALicnse.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CAminfo.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CAregit.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\countries.txt

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\countriesTrial.txt

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\ErrBox.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic_comp_codes.dat

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.cap

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.dat

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.err

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98_64.dll

Files left behind by Uninstaller

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98_uninstaller.zip

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib_amd64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib_ia64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98log.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\Lic98Msg.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98-port

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98Service.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98version.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LicDebug.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licinfo_win.zip

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LicRCmd.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg_64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres_64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LogWatNT.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\mergecalic.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\mergeolf.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\prod_codes.txt

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\silntreg.tmp

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\states.txt

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\statesTrial.txt

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\vendor.dat

C:\Program Files (x86)\Common Files\microsoft shared\VC\amd64\msdia80.dll

C:\Program Files (x86)\Common Files\microsoft shared\VC\msdia80.dll

C:\Users\Administrator.RIGONE\AppData\Local\IconCache.db

C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\696F3DE637E6DE85B458996D
49D759AD

Files left behind by Uninstaller

C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B8CC409ACDBF2A2FE04C56F2875B1FD6

C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\696F3DE637E6DE85B458996D49D759AD

C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B8CC409ACDBF2A2FE04C56F2875B1FD6

C:\Users\Administrator\CA ARCserve D2D\TrayIcon\ARCFlashTrayIcon.log

C:\Windows\Downloaded Installations\{3D52BE33-2E8C-4A39-BECF-878DD4D58252}\1033.MST

C:\Windows\Downloaded Installations\{3D52BE33-2E8C-4A39-BECF-878DD4D58252}\CALicense.msi

C:\Windows\inf\WmiApRpl\0009\WmiApRpl.ini

C:\Windows\inf\WmiApRpl\WmiApRpl.h

C:\Windows\System32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms

C:\Windows\System32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.1.regtrans-ms

C:\Windows\System32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.2.regtrans-ms

C:\Windows\System32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf

C:\Windows\System32\drivers\Msft_Kernel_AFStorHBA_01009.Wdf

C:\Windows\System32\drivers\Msft_Kernel_ARCFlashVolDrv_01009.Wdf

C:\Windows\System32\drivers\Msft_User_AFStorHBATramp_01_09_00.Wdf

C:\Windows\System32\LogFiles\WUDF\WUDFTrace.etl

C:\Windows\System32\winevt\Logs\Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx

C:\$Mft

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CALicnse.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CALicnse.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CAminfo.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CAminfo.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CAregit.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\CAregit.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\ErrBox.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\ErrBox.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98_64.dll

Files left behind by Uninstaller

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98_64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib_amd64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib_amd64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib_ia64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98FileSockLib_ia64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98log.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98log.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\Lic98Msg.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\Lic98Msg.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98Service.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98Service.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98version.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\lic98version.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LicDebug.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LicDebug.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LicRCmd.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LicRCmd.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg_64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg_64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licreg_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres_64.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres_64.dll

Files left behind by Uninstaller

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\licregres_64_amd.dll

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LogWatNT.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LogWatNT.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\LogWatNT.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\mergecalic.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\mergecalic.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\mergeolf.exe

C:\Program Files (x86)\CA\SharedComponents\CA_LIC\mergeolf.exe

C:\Program Files (x86)\Common Files\microsoft shared\VC\amd64\msdia80.dll

C:\Program Files (x86)\Common Files\microsoft shared\VC\amd64\msdia80.dll

C:\Program Files (x86)\Common Files\microsoft shared\VC\msdia80.dll

C:\Program Files (x86)\Common Files\microsoft shared\VC\msdia80.dll

C:\Users\Administrator.RIGONE\AppData\Local\Microsoft\Windows\UsrClass.dat

C:\Users\Administrator.RIGONE\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1

C:\Users\Administrator.RIGONE\NTUSER.DAT

C:\Users\Administrator.RIGONE\ntuser.dat.LOG1

C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\94308059B57B3142E455B38A
6EB92015

C:\Users\Administrator\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\94308059B57B3142E455B38
A6EB92015

C:\Users\Administrator\NTUSER.DAT

C:\Users\Administrator\ntuser.dat.LOG1

C:\Windows\AppCompat\Programs\RecentFileCache.bcf

C:\Windows\inf\setupapi.dev.log

C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwareProtectionPlatform\Cache\c
ache.dat

C:\Windows\setupact.log

C:\Windows\SoftwareDistribution\DataStore\DataStore.edb

C:\Windows\SoftwareDistribution\DataStore\Logs\edb.chk

C:\Windows\SoftwareDistribution\DataStore\Logs\edb.log

C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D00
5A0

Files left behind by Uninstaller

C:\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0

C:\Windows\System32\catroot2\{127D0A1D-4EF2-11D1-8608-00C04FC295EE}\catdb

C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb

C:\Windows\System32\catroot2\dberr.txt

C:\Windows\System32\catroot2\edb.chk

C:\Windows\System32\catroot2\edb.log

C:\Windows\System32\config\COMPONENTS

C:\Windows\System32\config\COMPONENTS.LOG1

C:\Windows\System32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms

C:\Windows\System32\config\COMPONENTS{016888b8-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf

C:\Windows\System32\config\COMPONENTS{016888b9-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms

C:\Windows\System32\config\DEFAULT

C:\Windows\System32\config\DEFAULT.LOG1

C:\Windows\System32\config\SAM

C:\Windows\System32\config\SAM.LOG1

C:\Windows\System32\config\SOFTWARE

C:\Windows\System32\config\SOFTWARE.LOG1

C:\Windows\System32\config\SYSTEM

C:\Windows\System32\config\SYSTEM.LOG1

C:\Windows\System32\config\TxR\{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.0.regtrans-ms

C:\Windows\System32\config\TxR\{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf

C:\Windows\System32\config\TxR\{016888cd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms

C:\Windows\System32\DriverStore\INFCACHE.1

C:\Windows\System32\DriverStore\infpub.dat

C:\Windows\System32\DriverStore\infstor.dat

C:\Windows\System32\DriverStore\infstrng.dat

C:\Windows\System32\LogFiles\Scm\3cdb3c57-5945-4fa9-8e4d-f8bd141f0f8f

C:\Windows\System32\LogFiles\Scm\63ee8552-a444-4ba2-8e1e-c8350d6d412a

C:\Windows\System32\LogFiles\Scm\c7847981-48e6-476f-9581-4bbd8e73f7c5

Files left behind by Uninstaller

C:\Windows\System32\LogFiles\Scm\cd264f70-fd14-48ea-9d74-f52f1d1d3f89

C:\Windows\System32\perfc009.dat

C:\Windows\System32\perfh009.dat

C:\Windows\System32\PerfStringBackup.INI

C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT

C:\Windows\System32\SMI\Store\Machine\SCHEMA.DAT.LOG1

C:\Windows\System32\wbem\Performance\WmiApRpl.h

C:\Windows\System32\wbem\Performance\WmiApRpl.ini

C:\Windows\System32\wbem\Repository\INDEX.BTR

C:\Windows\System32\wbem\Repository\MAPPING1.MAP

C:\Windows\System32\wbem\Repository\OBJECTS.DATA

C:\Windows\System32\WdfCoinstaller01009.dll

C:\Windows\System32\winevt\Logs\Application.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API Service.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-NlaSvc%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-PrintService%4Admin.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Service%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-WindowsUpdateClient%4Operational.evtx

C:\Windows\System32\winevt\Logs\Microsoft-Windows-WinRM%4Operational.evtx

Files left behind by Uninstaller

C:\Windows\System32\winevt\Logs\Security.evtx

C:\Windows\System32\winevt\Logs\Setup.evtx

C:\Windows\System32\winevt\Logs\System.evtx

C:\Windows\System32\winevt\Logs\Works with Tool.evtx

C:\Windows\System32\WudfUpdate_01009.dll

C:\Windows\WindowsUpdate.log

C:\Windows\winsxs\amd64_microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.4053_none_8a1a02152edb659b\ ATL80.dll

C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_88e046c92fae6f57\m svcm80.dll

C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_88e046c92fae6f57\m svcp80.dll

C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_88e046c92fae6f57\m svcr80.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_8444db7d32915e4c \mfc80.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_8444db7d32915e4c \mfc80u.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_8444db7d32915e4c \mfcm80.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_8444db7d32915e4c \mfcm80u.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be087 90\mfc80CHS.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be087 90\mfc80CHT.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be087 90\mfc80DEU.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be087 90\mfc80ENU.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be087 90\mfc80ESP.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be087 90\mfc80FRA.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be087 90\mfc80ITA.dll

Files left behind by Uninstaller

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be08790\mfc80JPN.dll

C:\Windows\winsxs\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be08790\mfc80KOR.dll

C:\Windows\winsxs\amd64_microsoft.vc80.openmp_1fc8b3b9a1e18e3b_8.0.50727.4053_none_f360fbe6b533bb31\vcomp.dll

C:\Windows\winsxs\Catalogs\0ca7bc78490b20539c7da204d33c9abfde4f767e04153a52935e1bd9524ae14d.cat

C:\Windows\winsxs\Catalogs\146faa10eda7090d809f5c1983eddfefef12eb1023360209db981208d5f6b6a1.cat

C:\Windows\winsxs\Catalogs\17d99f91c05697b4b725ca4e72638a53ae174a1cc8f909f02aed9f3150ec725d.cat

C:\Windows\winsxs\Catalogs\1ab02a94e548e9858ada0d9129d8cb8da13c987893c88a55b95506be1751d4e0.cat

C:\Windows\winsxs\Catalogs\2c0305f00ea5bbc4b158fbb6ca0978157701db1c7d04505a701b2da4e5ee0d4a.cat

C:\Windows\winsxs\Catalogs\3a2eb93af7df73651872b222dde139b56057c83e49d165fd8d71f0f61624a5a3.cat

C:\Windows\winsxs\Catalogs\51c55792a77ddffa2c36fc5cc92cf7e67263b0004bb0b4970f3a00524f5bdbec.cat

C:\Windows\winsxs\Catalogs\57d5c1e17d3b003378ace5418d822c42353f8141380788c095a600def44f4913.cat

C:\Windows\winsxs\Catalogs\63c729a8a078402d99cb45b3a9b86ce4fcdeddc2d37d66e29ce018c1a1705f14.cat

C:\Windows\winsxs\Catalogs\73dfdd8f4f777c27a3a7f3b2bf95daa46d7b7d46b977c4b156b63830090d1b7a.cat

C:\Windows\winsxs\Catalogs\7abe3fad0ecf950e374ccde2fd8ada8bfa55b48432c9faa7489e03c575905284.cat

C:\Windows\winsxs\Catalogs\813c74c7711815cf656f96f0ce5d9e57a31c3c4f98b607c8425cdbe8d5ccb436.cat

C:\Windows\winsxs\Catalogs\81bffdab9f49ea0cc7eea7633b89d1381a501f384fb6e2698d6143ba4951cc8f.cat

C:\Windows\winsxs\Catalogs\9588f2e1edc7f64f7d173987afefc7627ffdfc3484441debe5a25d2310d9d49e.cat

C:\Windows\winsxs\Catalogs\9a9fc9145bc02262ecf1e9bd109a3fa6cb370f75f44154a0dd44446a4fd95424.cat

C:\Windows\winsxs\Catalogs\a7fdfe008c9847f2165399a7d6fd0d1c2ddae44bde43a87548389055dc0bae94.cat

C:\Windows\winsxs\Catalogs\aba56e2149c6c95a633e6e4e0b1b5f101272db96f1350467ebedb3375b5767a4.cat

C:\Windows\winsxs\Catalogs\d3e19e02e9e3366e40372f11e7e0cd545cc64bca5c2d750ac5529b9948b725cb.cat

C:\Windows\winsxs\Catalogs\db75056fb2f0bd417a827e9ff9f96e4a661d67d826329356e7bf55a902a7408a.cat

C:\Windows\winsxs\Catalogs\f28ac29692205dd3a8273062193579a1cb3f42cffa72a1cd94e453bc281865da.cat

C:\Windows\winsxs\ManifestCache\e4e8be02b8fae2a7_blobs.bin

C:\Windows\winsxs\Manifests\amd64_microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.4053_none_8a1a02152edb659b.manifest

C:\Windows\winsxs\Manifests\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_88e046c92fae6f57.manifest

C:\Windows\winsxs\Manifests\amd64_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_8444db7d32915e4c.manifest

Files left behind by Uninstaller

C:\Windows\winsxs\Manifests\amd64_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_bc1d1e5b0be08790.manifest

C:\Windows\winsxs\Manifests\amd64_microsoft.vc80.openmp_1fc8b3b9a1e18e3b_8.0.50727.4053_none_f360fbe6b533bb31.manifest

C:\Windows\winsxs\Manifests\amd64_policy.8.0.microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.4053_none_06328ff5fd1670fc.manifest

C:\Windows\winsxs\Manifests\amd64_policy.8.0.microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_09c0f789facc94a0.manifest

C:\Windows\winsxs\Manifests\amd64_policy.8.0.microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_024211bfff9b1183.manifest

C:\Windows\winsxs\Manifests\amd64_policy.8.0.microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_0605300f695657e9.manifest

C:\Windows\winsxs\Manifests\amd64_policy.8.0.microsoft.vc80.openmp_1fc8b3b9a1e18e3b_8.0.50727.4053_none_23d98a129b9d3e60.manifest

C:\Windows\winsxs\Manifests\x86_microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.4053_none_d1c738ec43578ea1.manifest

C:\Windows\winsxs\Manifests\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_d08d7da0442a985d.manifest

C:\Windows\winsxs\Manifests\x86_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_cbf21254470d8752.manifest

C:\Windows\winsxs\Manifests\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096.manifest

C:\Windows\winsxs\Manifests\x86_microsoft.vc80.openmp_1fc8b3b9a1e18e3b_8.0.50727.4053_none_3b0e32bdc9afe437.manifest

C:\Windows\winsxs\Manifests\x86_policy.8.0.microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.4053_none_4ddfc6cd11929a02.manifest

C:\Windows\winsxs\Manifests\x86_policy.8.0.microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_516e2e610f48bda6.manifest

C:\Windows\winsxs\Manifests\x86_policy.8.0.microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_49ef489714173a89.manifest

C:\Windows\winsxs\Manifests\x86_policy.8.0.microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_4db266e67dd280ef.manifest

C:\Windows\winsxs\Manifests\x86_policy.8.0.microsoft.vc80.openmp_1fc8b3b9a1e18e3b_8.0.50727.4053_none_6b86c0e9b0196766.manifest

C:\Windows\winsxs\x86_microsoft.vc80.atl_1fc8b3b9a1e18e3b_8.0.50727.4053_none_d1c738ec43578ea1\ATL80.dll

C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_d08d7da0442a985d\msvcm80.dll

Files left behind by Uninstaller

C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_d08d7da0442a985d\msvcp80.dll

C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_d08d7da0442a985d\msvcr80.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_cbf21254470d8752\mfc80.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_cbf21254470d8752\mfc80u.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_cbf21254470d8752\mfcm80.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_cbf21254470d8752\mfcm80u.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80CHS.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80CHT.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80DEU.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80ENU.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80ESP.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80FRA.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80ITA.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80JPN.dll

C:\Windows\winsxs\x86_microsoft.vc80.mfcloc_1fc8b3b9a1e18e3b_8.0.50727.4053_none_03ca5532205cb096\mfc80KOR.dll

C:\Windows\winsxs\x86_microsoft.vc80.openmp_1fc8b3b9a1e18e3b_8.0.50727.4053_none_3b0e32bdc9afe437\vcomp.dll

Files Installed Outside the Default Location

By default, CA ARCserve D2D is installed in the following location: C:\Program Files\CA\ARCserve D2D. However some CA ARCserve D2D files are installed outside this default folder.

File Path and Name	Reason
C:\Windows\Downloaded Installations\{3D52BE33-2E8C-4A39-BECF-878DD4D58252}\CALicense.msi	CA Licensing Component (shared)
C:\Windows\inf\oem1.inf	Installed by mount driver in recommended location
C:\Windows\inf\oem2.inf	Installed by mount driver in recommended location
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\oem1.CAT	Installed by mount driver in recommended location
C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\oem2.CAT	Installed by mount driver in recommended location
C:\Windows\winsxs\Catalogs\0ca7bc78490b20539c7da204d33c9abfde4f767e04153a52935e1bd9524ae14d.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\146faa10eda7090d809f5c1983eddfefef12eb1023360209db981208d5f6b6a1.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\17d99f91c05697b4b725ca4e72638a53ae174a1cc8f909f02aed9f3150ec725d.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\1ab02a94e548e9858ada0d9129d8cb8da13c987893c88a55b95506be1751d4e0.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\2c0305f00ea5bbc4b158fbb6ca0978157701db1c7d04505a701b2da4e5ee0d4a.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\3a2eb93af7df73651872b222dde139b56057c83e49d165fd8d71f0f61624a5a3.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\51c55792a77ddffa2c36fc5cc92cf7e67263b0004bb0b4970f3a00524f5bdbec.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\57d5c1e17d3b003378ace5418d822c42353f8141380788c095a600def44f4913.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\63c729a8a078402d99cb45b3a9b86ce4fcdeddc2d37d66e29ce018c1a1705f14.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\73dfdd8f4f777c27a3a7f3b2bf95daa46d7b7d46b977c4b156b63830090d1b7a.cat	Microsoft Visual C++ component

C:\Windows\winsxs\Catalogs\7abe3fad0ecf950e374ccde2fd8ada8bfa55b48432c9faa7489e03c575905284.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\813c74c7711815cf656f96f0ce5d9e57a31c3c4f98b607c8425cdbe8d5ccb436.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\81bffdab9f49ea0cc7eea7633b89d1381a501f384fb6e2698d6143ba4951cc8f.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\9588f2e1edc7f64f7d173987afefc7627ffdfc3484441debe5a25d2310d9d49e.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\9a9fc9145bc02262ecf1e9bd109a3fa6cb370f75f44154a0dd44446a4fd95424.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\a7fdfe008c9847f2165399a7d6fd0d1c2ddae44bde43a87548389055dc0bae94.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\aba56e2149c6c95a633e6e4e0b1b5f101272db96f1350467ebedb3375b5767a4.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\d3e19e02e9e3366e40372f11e7e0cd545cc64bca5c2d750ac5529b9948b725cb.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\db75056fb2f0bd417a827e9ff9f96e4a661d67d826329356e7bf55a902a7408a.cat	Microsoft Visual C++ component
C:\Windows\winsxs\Catalogs\f28ac29692205dd3a8273062193579a1cb3f42cffa72a1cd94e453bc281865da.cat	Microsoft Visual C++ component

Appendix D: Using the CA ARCserve D2D Probe for Nimsoft

This section contains the following topics:
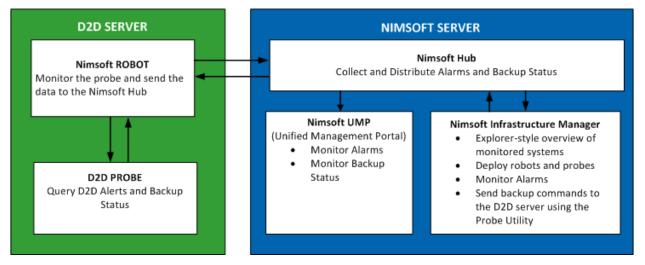
Overview

The CA ARCserve D2D Probe for Nimsoft (D2D probe) is a software module that sends the CA ARCserve D2D alerts and backup job status to the Nimsoft server. You can view the alerts from both the Nimsoft Infrastructure Manager and the Nimsoft Unified Management Portal (UMP). However, you can only view the job status data from the UMP. The advantage of using Nimsoft to monitor the alerts and status is that you can monitor multiple CA ARCserve D2D servers from one central location. Nimsoft also lets you run CA ARCserve D2D commands such as full backup, incremental backup, and verify backup using the Nimsoft Probe utility. For more information about the Nimsoft Infrastructure Manager and the UMP, see the *CA Nimsoft Monitor Getting Started Guide*.

The D2D probe queries the CA ARCserve D2D server and sends the D2D alerts and backup job status to the corresponding Nimsoft robot. Each computer that is being monitored by a probe must also have a robot installed on it. The robot is the first line of management for these probes. The robot starts and stops the probes at the required times, collects, queues and forwards messages from the probes to the corresponding hub. The hub then collects the messages from the robot and distributes them as alerts (alarms) and backup status to the Nimsoft Infrastructure Manager and the Nimsoft UMP. The hub is a message concentrator and re-distributor. It is the collection point for all messages coming from the various installed robots. The hub can also be used to 'group' a set of similar robots, such as ones that perform the same operations, have the same geographical locations, have the same departmental code, and so on.
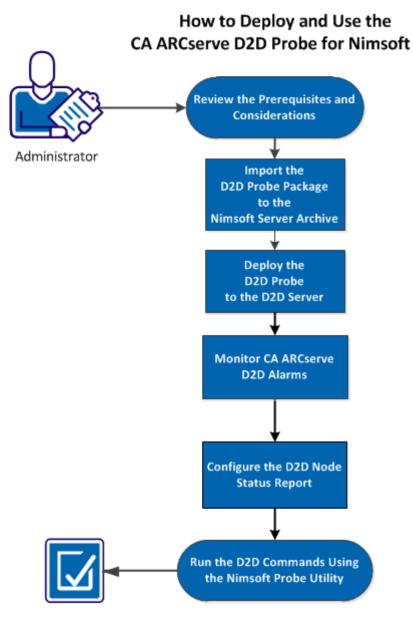
Note: The D2D probe can send alerts that are related to CA ARCserve Central Virtual Standby and CA ARCserve Central Host-Based VM Backup. However, to receive complete CA ARCserve Central Virtual Standby alerts, the D2D probe needs to be installed on both the source server (for conversion-related alerts) and monitor server (for failover-related alerts).

The following architecture diagram illustrates how the D2D probe captures the D2D alerts and backup job status and sends them to the Nimsoft server.

How to Deploy and Use the CA ARCserve D2D Probe for Nimsoft

The D2D probe is a software module that lets you monitor the D2D alerts and the backup status from the Nimsoft monitor. The benefit of using Nimsoft is that you can monitor multiple CA ARCserve D2D servers (D2D servers); however, each D2D probe can only monitor one D2D server. So you must deploy a D2D probe on each D2D server that you want to monitor.

The following diagram illustrates how to deploy and use the D2D probe for Nimsoft.

How to Deploy and Use the CA ARCserve D2D Probe for Nimsoft

Administrator

Review the Prerequisites and Considerations

Import the D2D Probe Package to the Nimsoft Server Archive

Deploy the D2D Probe to the D2D Server

Monitor CA ARCserve D2D Alarms

Configure the D2D Node Status Report

Run the D2D Commands Using the Nimsoft Probe Utility

Perform the following tasks to deploy and use the D2D probe:

-

-

-

-

-

-

Review the Prerequisites and Considerations
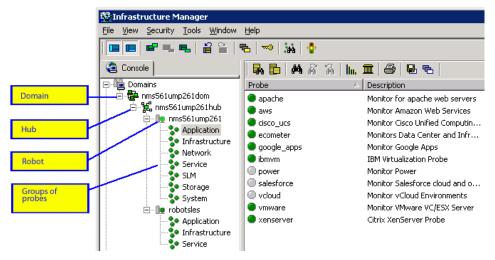
Verify that the following prerequisites exist before you install the D2D probe:

The Nimsoft robot is installed on the D2D server. For more information on how to install the Nimsoft robot, see the *CA Nimsoft Server Installation Guide*.

- The Nimsoft Infrastructure Manager is installed on the Nimsoft server. For more information on how to install the Nimsoft Infrastructure Manager, see the *CA Nimsoft Server Installation Guide*.

- You have access to the Nimsoft Unified Management Portal (UMP). For more information about the Nimsoft UMP, see the *CA Nimsoft Monitor Getting Started Guide.*

Review the following considerations:

- You are familiar with the details of the Nimsoft Infrastructure Manager.

Import the D2D Probe Package to the Nimsoft Server Archive

To install the D2D probe on the Nimsoft server, download the zip file (D2DProbeForNimsoft.zip) from the Nimsoft Internet Archive. This zip file contains the following two files:

- ARCserve_D2D_1.0.zip

  This zip file is the D2D probe package that needs to be imported in to the Nimsoft server. The Nimsoft server automatically unzips this file when you import the probe. You can save the zip file to a desired location.

- D2D node status.xml

  Contains the formatting definitions used by the Nimsoft Unified Management Portal (UMP) to display the D2D Node Status report.

Follow these steps:

1. Download the zip file from the Nimsoft Internet Archive and save the file to a desired folder and unzip it.

   The D2D probe package is available to be imported.

2. Log in to the Nimsoft Infrastructure Manager as an Administrator.
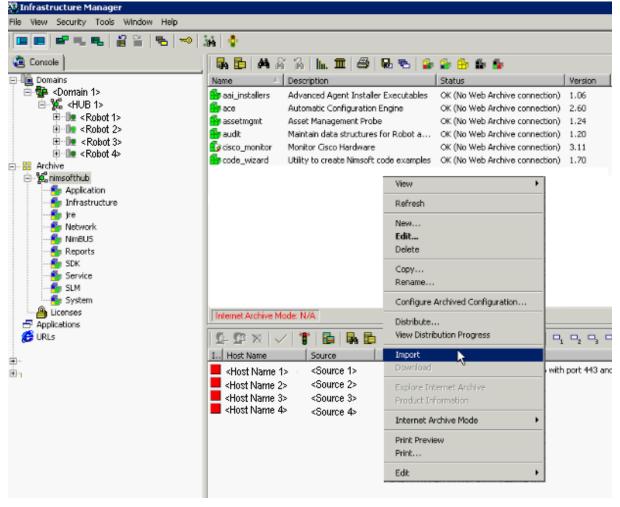
   The Nimsoft Infrastructure Manager UI is displayed.

3. From the Console pane, expand the Archive listing and click on the name for your Nimsoft hub.

   The existing Nimsoft packages are displayed on the right pane of the main window.

4. From the right pane, right-click to display the task menu and select Import.

    The Open dialog opens.

5. Navigate to the folder where you have saved the D2D probe package and click Open.

    The D2D probe package is imported to Nimsoft.

Deploy the D2D Probe to the D2D Server

After importing the D2D probe package to the Nimsoft server, you can deploy the package to the D2D server using the Nimsoft Infrastructure Manager. You drag and drop the D2D probe package to the robot on the D2D server. After the D2D probe is deployed to the D2D server, the probe sends the D2D alerts and backup statuses to the Nimsoft server. For more information about the Nimsoft Infrastructure Manager, see the *CA Nimsoft Monitor Infrastructure Manager Reference and User Guide.*

Note: If you change the CA ARCserve D2D communication protocol (HTTP or HTTPS) or you change the port number after the D2D probe is deployed, D2D alerts will not be sent until the probe is restarted.

Follow these steps:

1. Log in to the Nimsoft Infrastructure Manager as Administrator.
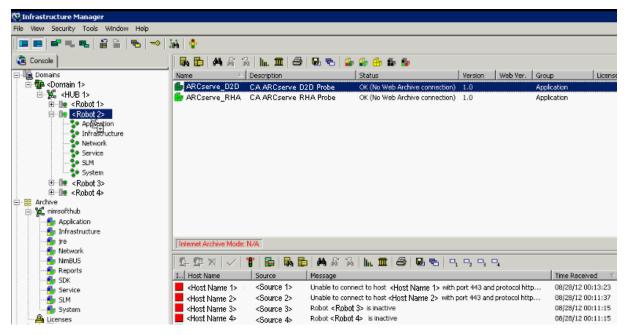
   The Nimsoft Infrastructure Manager interface is displayed.

2. From the Console pane, expand the Archive listing. Select your Nimsoft hub, and click Application.

   The D2D probe is listed on the right pane.

3. Drag-and-drop the D2D probe from the right pane onto the Nimsoft robot running on the D2D server (listed on the Console pane).

   The View Distribution Progress dialog is displayed to show the status of the deployment.

4.   Click Close Dialog after the deployment is complete.

5.   Select the robot and click Application to verify the status of the D2D probe on the right panel.

A green dot symbol indicates that the probe is successfully deployed.

The D2D probe is deployed on the D2D server and is ready to send the D2D data to the Nimsoft server.

Monitor CA ARCserve D2D Alarms

After the D2D probe is deployed on the D2D server, the probe sends all the enabled D2D alerts to the Nimsoft server as alarms. You can monitor these alarms either from the Nimsoft Infrastructure Manager or Nimsoft Unified Management Portal (UMP).

Note: If you change the CA ARCserve D2D communication protocol (HTTP or HTTPS) or you change the port number after the D2D probe is deployed, D2D alerts will not be sent until the probe is restarted.

Follow these steps to monitor D2D alarms from the Nimsoft Infrastructure Manager:

1.   Log in to the Nimsoft Infrastructure Manager as an Administrator.

The Infrastructure Manager is displayed and all the Nimsoft alarms are listed in the Dock pane.

2.   Click the Filter icon.

The Filter dialog opens.

3.   Enter D2D to display the CA ARCserve D2D alarms.

The CA ARCserve D2D alarms are listed in the Dock pane.

Follow these steps to monitor D2D alarms from the Nimsoft Unified Management Portal (UMP):

1. Log in to the Nimsoft Unified Management Portal as an Administrator.

   Note: To log in to the Nimsoft UMP, enter the following URL address (where <IP address> is the IP address of the machine that has UMP installed on it). http://<IP address>/web/guest/home

   The Nimsoft UMP interface is displayed.

2. Click the Alarms tab.

   All alarms are displayed.

3. Enter D2D in the filter text box to view only CA ARCserve D2D alarms.

   The listing is filtered to only display the CA ARCserve D2D alarms.

Configure the D2D Node Status Report

The D2D Node status report shows the status of last backups, number of available recovery points, and operating systems on each D2D node. You view this report from the Nimsoft UMP. To add this report to the Nimsoft UMP, you must import the D2D node status.xml file. This file is part of the D2D probe zip file that you previously downloaded from the CA ARCserve D2D website.

Follow these steps:

1. Log in to the Nimsoft Unified Management Portal (UMP) as an Administrator.

   The UMP interface is displayed.

2. From the top menu, click Design and select Lists.

   The List Designer page opens.

3. From the top right side of the page, click the Open View icon.

   The Open View dialog opens.

4. Click Import and select the D2D node status.xml file.

   Note: The D2D node status.xml file is downloaded with the D2D probe package. You can locate the file in the folder where you saved the downloaded zip file.

   The node status report is displayed on the List Designer page.

5. Click the Save View As icon to save the report with a descriptive name such as D2D Node Status.

6. From the Menu bar, click Add and select Page to add a new tab for the status report.

   A new text box is displayed to the right of the last tab.

7. In the text box on the new tab, enter a title for the D2D node status report and click the check icon.

   The title is added to the new tab. For example, assume you entered "D2D Reports" then that would be the title for the new tab.

8. From the Menu bar, click Manage, and select Page to add subtabs to the D2D Reports page.

   The Manage Pages page opens.

9. Click the Pages tab and select D2D Reports.

   The D2D Reports page opens.

10. Click Children, and select New Page to enter a name for the new subtab.

    The title is added to the new subtab. For example, assume you entered "Node Status" then that would be the title for the new subtab.

11. Click Add Page to save the new subtab.

12. Click Return to Full Page to open the List Viewer page.

13. Click D2D Reports, and select Node Status on the top bar to open the Node Status page.

14. Click the Wrench icon, and select Preferences.

    A list of reports is displayed.

15. Select the D2D Node Status report and click Save.

16. Click Return to Full Page to display the List Viewer page.

The D2D Node Status report is configured. You can now quickly view the D2D Node Status report when you click D2D Reports and select Node Status.

Run the D2D Commands Using the Nimsoft Probe Utility

The Nimsoft Probe utility lets you run specific commands to launch backup jobs from CA ARCserve D2D (Full Backup, Incremental Backup, and Verify Backup). When you run these commands, the commands are executed at the CA ARCserve D2D server.

Follow these steps:

1. Log in to the Nimsoft Infrastructure Manager as an Administrator.

   The Nimsoft Infrastructure Manager interface is displayed.

2. From the main window, select the D2D probe and press Control+P to start the Nimsoft Probe utility.

   The Nimsoft Probe utility dialog is displayed.

3. From the Probe commandset pane, click on the drop-down menu, select one of the backup commands, and click the Start button to send the command request. The available commands are Submit Full Backup, Submit Incremental Backup, and Submit Verify Backup.

   The selected D2D command is submitted to the D2D server and the corresponding job is launched. The status of the command is displayed on the Command Output pane.

   From the CA ARCserve D2D interface, you can view the status of the backup job on the Job Monitor.

Appendix E: Recovery Point Merge Failure May Render Recovery Point Unrecoverable

What is the issue?

CA ARCserve® D2D r16 Update 7 added the ability to resume the recovery point merge process if a previous merge job failed or crashed. However, since releasing Update 7 we have determined that if a merge fails or crashes after more than 10% of the merge job has been completed, the recovery point chain may be corrupted resulting in continued backup, merge, and restore errors.

Notes:

- This issue has only been found with systems running Update 7. Systems running previous updates do not have this issue.

- This issue has been fixed and tested in CA ARCserve D2D r16.5. If you have determined that the existing recovery points in your environment have been affected, you must run a Full Backup to a different backup destination to restart the recovery point chain.

- Data corruption could have occurred during the merge process of previous CA ARCserve D2D r16 Update 7 recovery points. Upgrading to CA ARCserve D2D r16 Update 8 or CA ARCserve D2D r16.5 will not repair any data corruption already present in existing recovery points.

- Data from the corrupted recovery points may not be recoverable using the CA ARCserve D2D recovery interface. We strongly recommend testing multiple recovery points to determine your level of recoverability.

Additional information related to merge issues and data corruption can be found in KB article:

http://arcserve-knowledgebase.com/index.php?View=entry&EntryID=4032

What to do?

The AFUtil.exe utility can be used to scan your backup sessions and confirm the integrity of the backed-up data. It is strongly recommended that you access the following KB article to download the utility and then run the utility immediately:

http://arcserve-knowledgebase.com/index.php?View=entry&EntryID=4512

Important! Because this utility performs a complete scan of your backed-up data for the selected recovery point, this can be a time-consuming process. The utility cannot run if other jobs are running at the same time. Verify that the CA ARCserve D2D Web Service is stopped and that there are no active jobs running.

For more information about this utility, see AFUtil.exe Utility (see page 362).

AFUtil.exe Utility

The AFUtil.exe utility is used to scan a CA ARCserve D2D backup session to confirm the integrity of the backed-up data. This utility should be placed in the "Bin" folder for the CA ARCserve D2D installation prior to using it. When this utility is executed without any parameters, by default it will determine the configured backup destination and scan the oldest Full Backup session of all the machines that are protected by CA ARCserve D2D. However, it is strongly recommended to scan all backup images to ensure that data from these recovery points are restorable.

Usage

AFUtil [<-|/><switch> [parameters]]

Note: To ensure each and every image is scanned, use the /sid switch as described in the second example. You will have to run the utility one time for every session.

Examples:

- Run the following command to scan the oldest base session:

  AFUtil

- Run the following command to scan the 5th backup session:

  AFUtil.exe /AFStor /dest <destination_path> /un <username> /upwd <password> /sid 5

- Run the following command to scan the oldest Full backup for all of the VMs connected to the backup proxy system for the Host-Based VM Backup server:

  AFUtil.exe /AFStor /vm

The following commands are supported by the AFUtili.exe utility:

Command	Description
/?	Displays a list of all supported commands.
/help	Displays a list of all supported commands.
/AFStor	Session related commands.

The following switches are supported by the AFStor command:

Note: You can view a list of all supported switches by using the "AFUtil.exe /? AFStor" command.

Switch	Description
/dest <destination_path>	Backup destination folder to scan.
	By default, the utility will try to determine the backup path from the configured CA ARCserve D2D settings. If the settings are not configured or if you want to scan a different path, this switch can be used.
	Note: Path names with spaces in them should be enclosed in double quotes.
/un <username>	Use this user name to connect to the remote destination.
	By default, the user name is retrieved from the CA ARCserve D2D backup settings. If different credentials are to be used to connect to the remote destination, this switch can be used.
/upwd <password>	Use this password to connect to the remote destination.
	By default the password is retrieved from the CA ARCserve D2D backup settings. If different credentials are to be used to connect to the remote destination, this switch can be used.
/vhd <D2D file>	Use this to scan a specific CA ARCserve D2D file. This switch requires the full path and name of the CA ARCserve D2D file to scan.
	This switch cannot be combined with '/dest' switch.
	Note: Path names with spaces in them should be enclosed in double quotes.
/pwd <password>	Use the provided password for decrypting the sessions.
	By default, the utility will attempt to read the password from the CA ARCserve D2D files if the utility is run on the machine where the backups were performed. If the utility is not able to auto read the encryption password, then this switch can be used to specify a password.
/offset <start offset>	Start scanning at the given offset value. The offset value must be specified in bytes. Valid range is from 0 to the size of the disk.
	If this parameter is not specified, the scan starts from offset 0.

Switch	Description
/sid <session number>	Scan the specified session number. If this switch is not specified, the utility will only scan the oldest base session.
/size <size>	Size of data (in bytes) of the source to be scanned. If this parameter is not specified, the utility will scan the entire disk.
/vm [VM UUID]	Used to scan the backup proxy system for the Host-Based Backup VM server based on the specified UUID for the VM. If the UUID for the VM is not specified, then the oldest Full backup of all the VMs protected by the CA ARCserve D2D proxy are scanned one by one.

Return Value

If the AFUtil.exe utility runs successfully, the return value is 0. If any error is encountered during the running of this utility, then the return value will not be 0.

The following table contains a listing of all possible error codes that can occur when attempting to run this utility and a corresponding description.

Return Value/Code	Description
SCAN_RET_ENV_ERROR 0xE0000001	Attempted to run the utility on a machine where CA ARCserve D2D was not installed. Scan is aborted immediately when this error is encountered and the error message is displayed.
SCAN_RET_ACT_JOB 0xE0000002	Attempted to run this utility, but there is an active job running at the same time (such as a backup or merge job). Scan is aborted immediately when this error is encountered and the error message is displayed.
SCAN_RET_NET_ERROR 0xE0000003	Failed to connect to the specified destination folder because of an incorrect destination path, username, or password. Scan is aborted immediately when this error is encountered and the error message is displayed.

Return Value/Code	Description
SCAN_RET_ENV_ERROR 0xE0000001	Attempted to run the utility on a machine where CA ARCserve D2D was not installed. Scan is aborted immediately when this error is encountered and the error message is displayed.
SCAN_RET_WEB_RUN 0xE0000004	Attempted to run this utility, but the CA ARCserve D2D web service is still running. The CA ARCserve D2D web service must be stopped before you can run the utility. Scan is aborted immediately when this error is encountered and the error message is displayed.
SCAN_RET_DATA_BAD 0xE0000005	The utility has detected data corruption while scanning the backup session. Scan is NOT aborted immediately when this error is encountered and continues until the scan of the entire session is completed. The error message is displayed and an entry is included in the activity log. For more detailed debugging information about this error, search for "<<!data corruption detected!>>" in the debug log.
SCAN_RET_INVALID_UUID 0xE0000006	Attempted to run this utility, but the specified UUID for the VM is invalid. Scan is aborted immediately when this error is encountered and the error message is displayed.
SCAN_RET_INVALID_DEST 0xE0000007	Attempted to run this utility, but failed to find a valid destination folder for the scan. Scan is aborted immediately when this error is encountered.
SCAN_RET_INVALID_CMD 0xDFFFFFFF	Attempted to run this utility, but an invalid parameter was input when running the tool and a help message is displayed.
Other non-0 value	For more detailed information about this error, check the AFUtil.log located in the Logs folder in the CA ARCserve D2D installation path. Scan is not aborted immediately when this value is returned.The scan will continue until all disks are scanned, regardless if successful or not.

Index