CA ARCserve® Central Host-Based VM Backup

User Guide

r16

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

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

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

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

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication and High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Contact CA

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 Central Applications:

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:

- **Understanding your Support--**The following link provides information about maintenance programs and support offerings, including terms and conditions, claims, service-level objectives (SLO), and service hours.

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

- **Registering for Support--**The following 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--**The following link takes you to the One-Stop Product Support page for CA ARCserve Central Applications.

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

Documentation Changes

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

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

Update 7

- Updated Create Backup Policies (see page 72). This topic now includes the new Retention Setting feature where it lets you set the retention policy based on the number of recovery points to retain or the number of recovery sets to retain.
- Update Edit or Copy Backup Policies (see page 75). This topic now includes the new Retention Setting feature where it lets you set the retention policy based on the number of recovery points to retain or the number of recovery sets to retain.
- Added Merge Job Options (see page 49). This topic contains two new options: Pause Merge Job (see page 49) and Resume Merge Job (see page 50) on the Node screen. These topics describe how to pause or resume a merge job for a specific node.
- Updated Incremental Backup Jobs Process as Verify Backup Jobs (see page 136). This topic now describes how to correct incremental back jobs that run as verify backup jobs based the procedure described in a VMware Knowledge Base article.
- Added Recovering a Virtual Machine Uses a Different Transport Mode Than Specified (see page 143). This troubleshooting topic specifies the behavior of recovering a virtual machine when using a different transport mode than specified in the registry key.

Update 6

- Added Configure the CA ARCserve Central Protection Manager Server (see page 29). This configuration setting lets you change the current settings in CA ARCserve Central Host-Based VM Backup to CA ARCserve Central Protection Manager server settings. When the settings are configured, you can view the Host-Based VM Backup discovered nodes email alert information from CA ARCserve Central Reporting.
- Updated Configure Discovery Schedules (see page 31). This topic now includes a vCenter/ESX host list for you to view when setting up a schedule to discover nodes.
- Updated Configure Email and Alert Settings (see page 31). Renamed the title and updated this topic to include alerts on discovered nodes. A new Delete button is added to this screen t let you delete your saved settings. Deleting your saved settings prevents you from receiving email alert messages.

- Updated How to Manage Node Tasks for CA ARCserve Central Host-Based VM Backup (see page 39). The Node list now displays nodes that are unavailable when they are deleted or cannot be detected from the server. The Node list now displays the status of a policy deployment in the Policy column.
- Updated Update Nodes (see page 47). The topic describes how you can update multiple nodes simultaneously using the existing credentials or specifying new credentials. You can also force the server to manage the selected nodes.
- Updated Add Node Groups (see page 52). This topic replaces the "Unassigned" node group with "Nodes without a policy" and replaces the "Ungrouped" node group with "Nodes without a group".
- Updated Run a Backup Now (see page 62). This topic describes the priority level of backup jobs that are submitted when another backup job is waiting in the queue.
- Added Perform Full Disk Backups Containing Only Used Block Data (see page 69). This topic describes how to retrieve used block data after submitting a full disk backup job.
- Updated Create Backup Policies (see page 72). This topic now includes an email alert for failed and successful catalog jobs. This topic also includes email alerts for backup jobs that are waiting in the job queue, skipped, or replaced with another job.
- Added Define a Transport Mode for Backups (see page 84). CA ARCserve Central Host-Based VM Backup now lets you define a specific transport mode to use for D2D backup jobs that execute using Host-Based VM Backup.
- Updated Changed Block Tracking Backup Failures (see page 132). Removed references on resetting changed block tracking (CBT) when a backup job fails. CA ARCserve Central Host-Based VM Backup now automatically enables CBT on the virtual machine.

Update 5

- Add Node Groups (see page 52). Updated this topic to include Group and Node Name filters.
- Assign and Unassign Nodes from Backup Policies (see page 77). Updated this topic to include Group and Node Name filters.

Update 4

- Install CA ARCserve Central Host-Based VM Backup Silently. Removed the subtopic Silent Installation Product Codes and included it here.
- Uninstall CA ARCserve Central Host-Based VM Backup Silently. Removed the subtopic Silent Uninstallation Product Codes and included it here.
- How to use the CA ARCserve Central Host-Based VM Backup Home Page (see page 38). Removed Restore from the Navigation bar.
- Added Managing Node Tasks for CA ARCserve Central Host-Based VM Backup (see page 39). Created scenario-based content with a diagram on managing nodes.
- Added Managing Node Group Tasks for CA ARCserve Central Host-Based VM Backup (see page 51). Created scenario-based content with a diagram on managing node groups.
- Added Backing Up the Virtual Machine Environment (see page 57). Created scenario-based content with a diagram on backing up all virtual machines in your environment.
- Added Perform Preflight Checks for Your Backup Jobs (see page 58). This topic describes how a Preflight Check (PFC) is submitted.
- Added Solutions for Preflight Check Items (see page 59). This topic describes the error and warning messages you can receive when running a PFC and the solutions to resolve them.
- Added Run a Back Up Now (see page 62). Renamed the title from Submit a Backup Job to Run a Backup Now.
- Added View Job Status Information (see page 69). This topic describes how to view real-time information about in progress backup jobs.
- Host-Based VM Backup Monitoring Tasks (see page 70). Updated this topic to emulate the updated screen in the CA ARCserve Central Host-Based VM Backup application.
- Added How to Manage Policies for CA ARCserve Central Host-Based VM Backup (see page 71). Created scenario-based content with a diagram on creating, editing, assigning, unassigning backup policies.
- Restore and Recover Virtual Machines (see page 87). Revised all Restore-related topics with the new location of the Restore button on the screen.

Contents

Chapter 1: Introducing CA ARCserve Central Host-Based VM Backup 13

Chapter 2: Installing and Configuring CA ARCserve Central Host-Based VM Backup 17

Chapter 3: Using CA ARCserve Central Host-Based VM Backup 37

Chapter 6: Applying Best Practices 145

Appendix A: CA ARCserve D2D Procedures 173

Chapter 1: Introducing CA ARCserve Central Host-Based VM Backup

This section contains the following topics:

Introduction

CA ARCserve Central Applications combine core data protection and management technologies with an ecosystem of targeted applications that work in unison to facilitate on- and off-premises protection, copy, movement, and transformation of data across global environments.

CA ARCserve Central Applications are easy to use, manage, and install. It provides organizations with automated control of their information to make educated decisions about the access, availability, and security of their data, based on the overall business value.

About CA ARCserve Central Host-Based VM Backup

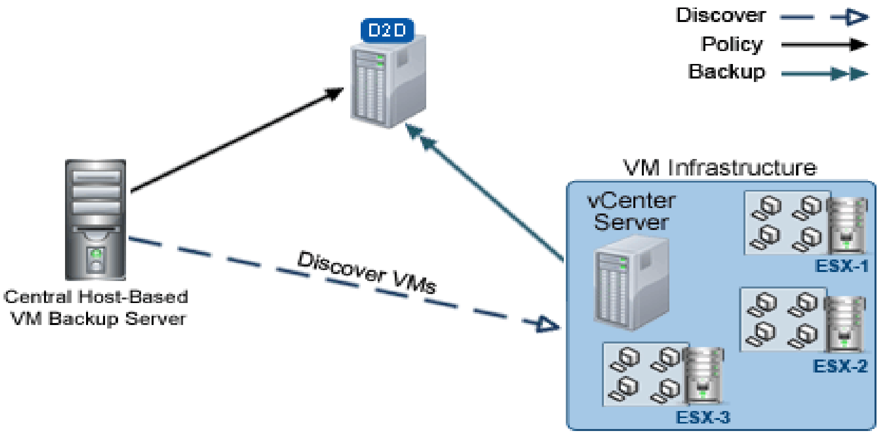
One of the CA ARCserve Central Applications is the CA ARCserve Central Host-Based VM Backup application. This application works with CA ARCserve D2D, which is a light-weight backup solution, and lets you protect multiple virtual machines without having to install the software or an agent on each individual virtual machine. This capability minimizes the adverse effects of running multiple backup operations on the same physical server and lets you perform file-level, application-level, or Bare Metal Recovery (BMR) from your virtual machine backups.

CA ARCserve Central Host-Based VM Backup scales easily so you can add virtual machines, as needed, without having to purchase additional licenses or install software on every virtual machine in your production environment.

How CA ARCserve Central Host-Based VM Backup Works

CA ARCserve Central Host-Based VM Backup lets you protect virtual machines running on an ESX or vCenter Server in a single pass using one instance of CA ARCserve D2D installed on a proxy. Use the following checklist to get started:

1. Install CA ARCserve D2D on one machine (physical or virtual) that acts as a backup proxy in your environment. For installation instructions, refer to the topic, Install CA ARCserve D2D, (see page 173) excerpted from the CA ARCserve D2D User Guide. Verify that the proxy is correctly configured.
2. Add nodes to manage. Specify an ESX server and the application detects the virtual machines running on it that meet requirements.
3. Create backup policies. In each policy, specify the backup proxy where you installed CA ARCserve D2D.
4. Assign backup policies to each VM so you can protect all VMs with the single CA ARCserve D2D instance running on the backup proxy.
5. Create node groups to better manage your virtual machine environment. For example, you can group nodes by business function or by installed application and then assign a policy configured to protect the nodes associated with a specific function or which are running a certain application.



CA ARCserve Central Applications Bookshelf

The topics contained in the CA ARCserve Central Applications Help system are also available as a User Guide in PDF format. The latest PDF version of this guide and Help System can be accessed from the CA ARCserve Central Applications Bookshelf.

The CA ARCserve Central Applications Release Notes files contain information relating to system requirements, operating system support, application recovery support, and other information you may need to know before installing this product. In addition, the Release Notes files contain a list of known issues that you should be aware of before you use CA ARCserve Central Applications. The latest version of the Release Notes can be accessed from the CA ARCserve Central Applications Bookshelf.

Chapter 2: Installing and Configuring CA ARCserve Central Host-Based VM Backup

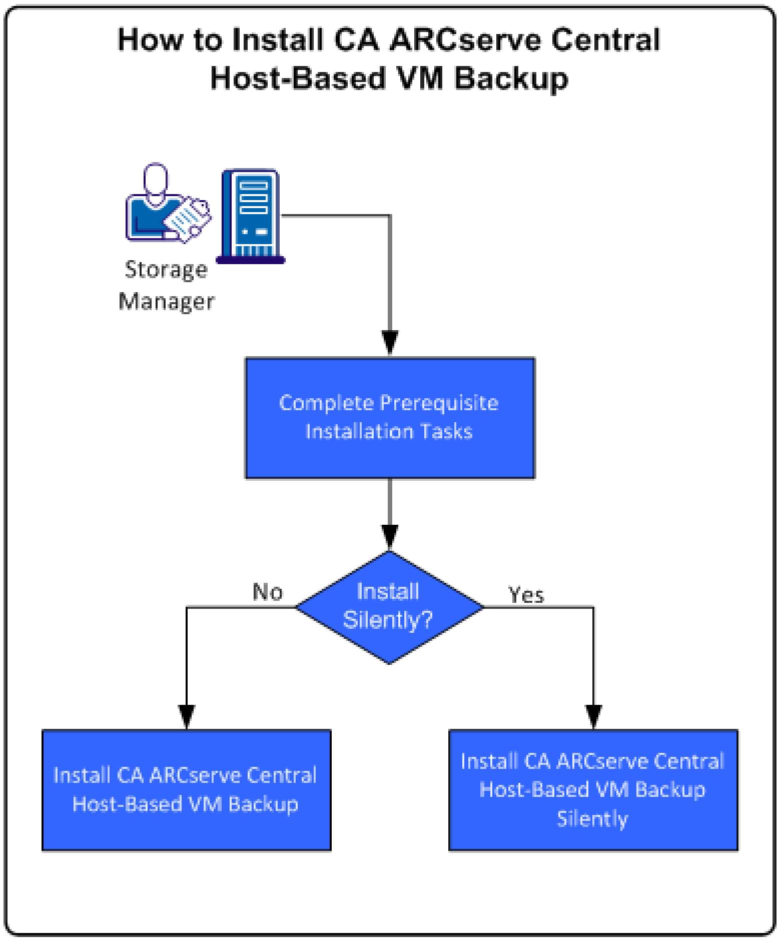
This section contains the following topics:

How to Install CA ARCserve Central Host-Based VM Backup

This scenario describes how Storage Managers can install CA ARCserve Central Host-Based VM Backup using the following methods:

- Standard installation--This method uses Installation Wizard to install the application.
- Silent installation--This method lets you perform an unattended installation using Windows Command Line.

The following diagram illustrates how to install the application:


How to Install CA ARCserve Central Host-Based VM Backup
Storage Manager
Complete Prerequisite Installation Tasks
Install Silently?
No
Yes
Install CA ARCserve Central Host-Based VM Backup
Install CA ARCserve Central Host-Based VM Backup Silently

The following table lists the topics that describe the tasks for installing CA ARCserve Central Host-Based VM Backup:

Task	See Topic
Perform prerequisite installation tasks and review installation considerations before you install the application.	Prerequisite Installation Tasks (see page 19)
Perform a standard installation using the Installation Wizard.	Install CA ARCserve Central Host-Based VM Backup (see page 21)
Perform a silent installation using the Windows Command Line.	Install CA ARCserve Central Host-Based VM Backup Silently (see page 23)

For information on updating various Windows Operating System Components after installing the application, see the Applying Best Practices section in the CA ARCserve Central Host-Based VM Backup User Guide.

Prerequisite Installation Tasks

Before you install the application, complete the following prerequisite tasks and review the installation considerations:

Prerequisite Tasks

- Review the Release Notes. The Release Notes contain a description of system requirements, supported operating systems, and a list of issues that are known to exist with this release of the application.
- Verify that your system meets the software and hardware requirements that are required to install the application.
- Verify that changed block tracking can be enabled and is enabled on the virtual machines that you are protecting.

  Note: For more information about the changed block tracking, see the following Knowledge Base document on the VMware website:

  http://kb.vmware.com/kb/1020128
- Verify that your Windows account has administrator privileges or any other equal privileges to install software on the computers where you plan to install CA ARCserve Central Host-Based VM Backup.
- Verify that your vCenter Server or ESX Server account has VMware and Windows administrative privileges. Assign the account to the Global License role on the vCenter Server system or ESX Server system to allow VDDK operations to complete successfully.

- Verify that you have the user names and passwords of the computers where you are installing the application in your possession.
- Verify that CA ARCserve D2D is installed on the backup proxy system that protects the virtual machines in your production environment.
- If you want granular restore capability from your VM backup, verify the following items:
  - Administrator credentials from any user with administrative privileges are provided to log in to the virtual machine guest operating system.
  - User Account Control (UAC) is disabled.

Installation Considerations

Before you install CA ARCserve Central Host-Based VM Backup, review the following installation considerations:

- The CA ARCserve Central Applications installation package installs a module named CA ARCserve Central Applications Server. The server is a module that is common to all applications. The module contains the web service, binaries, and configurations that let the application communicate with each other.

  When you install the application, the installation package installs the CA ARCserve Central Applications Server module before installing the product components. If it becomes necessary to apply a patch to the application, the patch updates the module before updating the product components.
- After CA ARCserve Central Applications is installed, download and install VMware VIX API version 1.10.1 or later on the backup proxy system for file level backup support.
- After CA ARCserve Central Host-Based VM Backup is installed, download and install VMware VIX API version 1.10.1 or later on the same computer which will be used for the preflight check later.
- CA ARCserve D2D installs VMware Virtual Disk Development Kit (VDDK) on all computers where you install CA ARCserve D2D. You do not need to download and install VDDK on your backup proxy systems.

  If you want to use a newer version of VDDK, download and install VDDK and then modify the value of the VDDKDirectory registry located at HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D to the installation folder where the new VDDK is installed.

  The default location for VDDK is as follows:

  - **x64 Operating System**

    ```
    c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit
    ```

    Note: Unzip the VDDK64.zip file from the VDDK installation directory to the VDDK64 folder.

For example, c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

- **x86 Operating System**

  c:\Program Files\VMware\VMware Virtual Disk Development Kit

- A local installation of CA ARCserve D2D is required to perform certain restore operations. For more information, see the topic, Restore Considerations (see page 96). Licenses for CA ARCserve D2D are included with CA ARCserve Central Host-Based VM Backup. To obtain the product installation files, visit CA support.
- Virtual compatibility for raw device mapping is supported but physical compatibility is not supported.

Install CA ARCserve Central Host-Based VM Backup

The installation wizard helps guide you through the process of installing one or more CA ARCserve Central Applications.

Note: Before you install an application, review the Release Notes file and verify that all of the tasks described in Prerequisite Tasks are complete.

To install CA ARCserve Central Host-Based VM Backup

1. Download the CA ARCserve Central Applications installation package to the computer where you want to install the application, and then double-click the Setup file.

   The installation package extracts its contents to your computer and then the Prerequisite Components dialog opens.

2. Click Install on the Prerequisites Components dialog.

   Note: The Prerequisite Components dialog opens only if Setup does not detect that the required prerequisite components are installed on your computer.

   After Setup installs the prerequisite components, the License Agreement dialog opens.

3. Complete the required options on the License Agreement dialog and click Next.

   The Configuration dialog opens.

4. On the Configuration dialog, complete the following:

   - **Components--**Specify the applications that you want to install.

     Note: If you are installing this application using the suite installation package, you can install multiple applications.

   - **Location--**Accept the default installation location or click Browse to specify an alternative installation location. The default location is as follows:

     C:\Program Files\CA\ARCserve Central Applications

   - **Disk Information--** Verify that your hard drive has sufficient free disk space to install the applications.

   - **Windows Administrator Name--**Specify the user name of the Windows Administrator account using the following syntax:

     Domain\User Name

   - **Password--**Specify the password for the user account.

   - **Specify Port Number--**Specify the port number that you want to use to communicate with the web-based user interface. As a best practice, you should accept the default port number. The default port number is as follows:

     8015

     Note: If you want to specify an alternative port number, the available port numbers are from 1024 through 65535. Before you specify an alternative port number, verify that the specified port number is free and available for use. Setup prevents you from installing the application using a port that is not available for use.

   - **Use HTTPS for web communication--**Specify to use HTTPS communication for data transmission. By default, this is not selected.

     Note: HTTPS (secure) communication provides a higher level of security than HTTP communication. HTTPS is recommended communication protocol if you transmit confidential information in your network.

   - **Allow Setup to register CA ARCserve Central Applications services and programs to the Windows Firewall as exceptions--**Verify that the check box next to this option is selected. Firewall exceptions are required if you want to configure and manage CA ARCserve Central Applications from remote computers.

     Note: For local users, you do not need to register firewall exceptions.

   Click Next.

   After the installation process is complete, the Installation Report opens.

5. The Installation Report dialog summarizes the installation. If you want to check for updates to the application now, click Check for updates and then click Finish.

The application is installed.

Install CA ARCserve Central Host-Based VM Backup Silently

CA ARCserve Central Applications lets you install CA ARCserve Central Host-Based VM Backup silently. A silent installation eliminates the need for user interaction. The following steps describe how to install the application using Windows Command Line.

To install CA ARCserve Central Host-Based VM Backup silently

1. Open the Windows Command Line on the computer where you want to start the silent installation process.
2. Download the CA ARCserve Central Applications self-extracting installation package to your computer.

   Start the silent installation process using the following Command Line syntax:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR> -Port:<PORT>
   -U:<UserName> -P:<Password> -Products:<ProductList>"
   ```

   Usage:

   s

   Lets you run the executable file package in silent mode.

   v

   Lets you specify additional command line options.

   q

   Lets you install the application in silent mode.

   -Path:<INSTALLDIR>

   (Optional) Lets you specify the target installation path.

   Example:

   ```
   -Path:\"C:\Program Files\CA\ARCserve Central Applications\"
   ```

   Note: If the value for INSTALLDIR contains a space, enclose the path with backslashes and quotation marks. Additionally, the path cannot end with a backslash character.

   -Port:<PORT>

   (Optional) Lets you specify the port number for communication.

   Example:

   ```
   -Port:8015
   ```

   -U:<UserName>

   Lets you specify the user name to use to install and run the application.

   Note: The user name must be an administrative account or an account with administrative privileges.

-P:<Password>

Lets you specify the password for UserName.

-Products:<ProductList>

(Optional) Lets you specify CA ARCserve Central Applications to install silently. If you do not specify a value for this argument, the silent installation process installs all components of CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

All CA ARCserve Central Applications

ALL

Note: The following examples describe the syntax that is required to install one, two, three, or all CA ARCserve Central Applications silently:

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

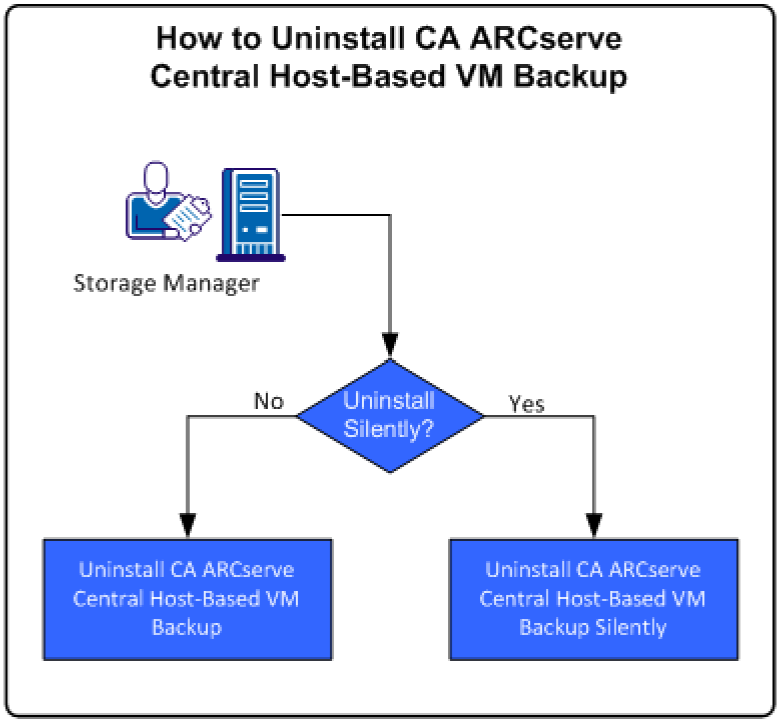
The application is installed silently.

How to Uninstall CA ARCserve Central Host-Based VM Backup

You can uninstall CA ARCserve Central Host-Based VM Backup using the following methods:

- Standard uninstallation--This method uses Windows Control Panel to uninstall the application.
- Silent uninstallation--This method lets you perform an unattended uninstallation using Windows Command Line.

The following diagram illustrates how to uninstall the application:


How to Uninstall CA ARCserve Central Host-Based VM Backup
Storage Manager
Uninstall Silently?
No
Yes
Uninstall CA ARCserve Central Host-Based VM Backup
Uninstall CA ARCserve Central Host-Based VM Backup Silently

Task	See Topic
Perform a standard uninstallation using Windows Control Panel.	Uninstall CA ARCserve Central Host-Based VM Backup (see page 26)
Perform a silent uninstallation using the Windows Command Line.	Uninstall CA ARCserve Central Host-Based VM Backup Silently (see page 26)

For information on updating various Windows Operating System Components after uninstalling the application, see the Applying Best Practices section in the CA ARCserve Central Host-Based VM Backup User Guide.

Uninstall CA ARCserve Central Host-Based VM Backup

You can uninstall the application using Programs and Features located in Windows Control Panel.

To uninstall CA ARCserve Central Host-Based VM Backup

1. From the Windows Start menu, click Start and click Control Panel.

   Windows Control Panel opens.

2. From Windows Control Panel, click the drop-down list next to View by and then click Large icons or Small icons.

   The icons for the Windows Control Panel applications appear in a grid layout.

3. Click Programs and Features.

   The Uninstall or change a program window opens.

4. Locate and click the application that you want to uninstall.

   Right-click the application and click Uninstall on the pop-up menu.

   Follow the on-screen instructions to uninstall the application.

The application is uninstalled.

Uninstall CA ARCserve Central Host-Based VM Backup Silently

CA ARCserve Central Applications lets you uninstall CA ARCserve Central Host-Based VM Backup silently. A silent uninstallation eliminates the need for user interaction. The following steps describe how to uninstall the application using Windows Command Line.

To uninstall CA ARCserve Central Host-Based VM Backup silently

1. Log in to the computer where you want to uninstall the application.

   Note: You must log in using an administrative account or an account with administrative privileges.

2. Open the Windows Command Line and execute the following command to start the silent uninstallation process:

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
   ```

   Or,

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /ALL
   ```

   Example: The following syntax lets you uninstall CA ARCserve Central Host-Based VM Backup silently.

   ```
   "%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}
   ```

Usage:

<INSTALLDIR>

Lets you specify the directory where the application is installed.

Note: Execute the syntax that corresponds with the architecture of the operating system on the computer.

<ProductCode>

Lets you specify the application to uninstall silently.

Note: The silent uninstallation process lets you install one or more CA ARCserve Central Applications. Use the following product codes to uninstall CA ARCserve Central Applications silently:

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

The application is uninstalled silently.

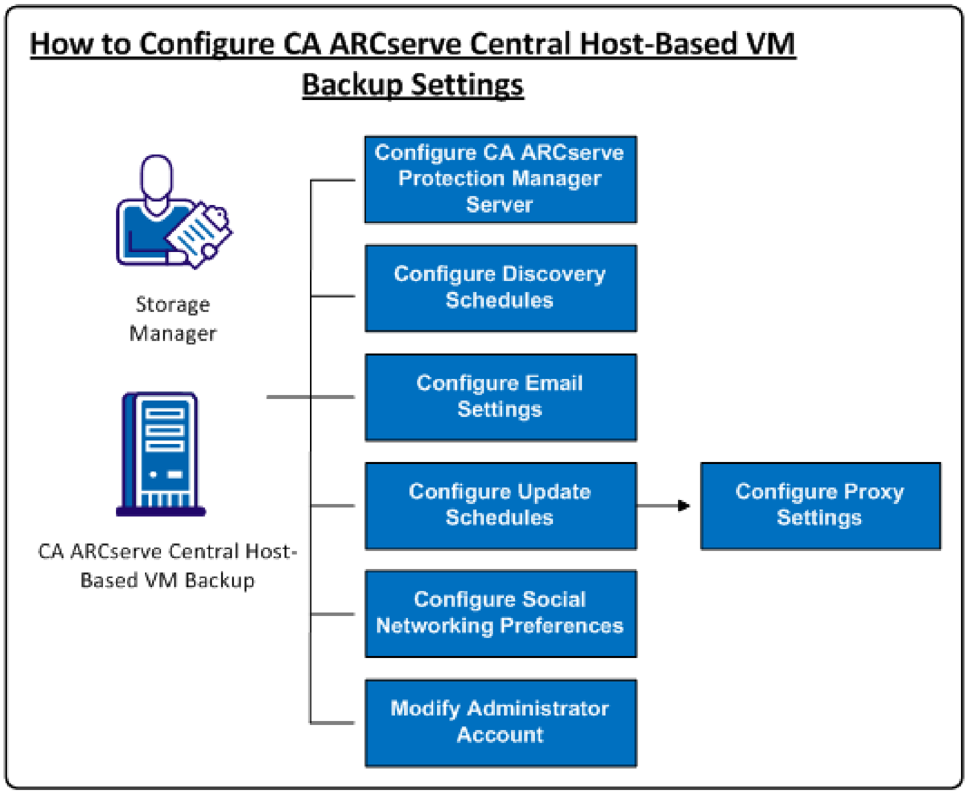
How to Configure CA ARCserve Central Host-Based VM Backup to Protect CA ARCserve D2D Nodes

The application lets you specify configuration settings for email alerts and schedules and how to update your CA ARCserve Central Host-Based VM Backup installation.

Before you start specifying your configuration settings, it is required that you first install CA ARCserve D2D on the server that performs your backup jobs. This peer, or proxy server, can be a single computer or multiple computers, depending on your needs. For instructions, refer to the topic, Install CA ARCserve D2D, (see page 173) excerpted from the CA ARCserve D2D User Guide.

You can install CA ARCserve Central Host-Based VM Backup on the same or a separate computer. The Installation procedure is wizard-based to make the setup easy. For more information, see Install CA ARCserve Central Host-Based VM Backup.

The following illustration describes the types of configurations you can set for your application:


How to Configure CA ARCserve Central Host-Based VM Backup Settings
Storage Manager
CA ARCserve Central Host-Based VM Backup
Configure CA ARCserve Protection Manager Server
Configure Discovery Schedules
Configure Email Settings
Configure Update Schedules
Configure Proxy Settings
Configure Social Networking Preferences
Modify Administrator Account

This scenario describes the following topics:

- Configure CA ARCserve Central Protection Manager Server (see page 29)
- Configure Discovery Schedules (see page 31)

- Configure Email Settings (see page 31)
- Configure Update Schedules (see page 32)
  - Configure Proxy Settings (see page 33)
- Configure Social Networking Preferences (see page 35)
- Modify Administrator Account (see page 36)

Configure the CA ARCserve Central Protection Manager Server

Configuring the CA ARCserve Central Protection Manager server lets you change the current settings in CA ARCserve Central Host-Based VM Backup to CA ARCserve Central Protection Manager server settings. When the settings are configured, you can view the Host-Based VM Backup discovered nodes email alert information from CA ARCserve Central Reporting.

Follow these steps:

1. Log in to the CA ARCserve Central Host-Based VM Backup server and click Configuration on the Navigation bar.

   The Configuration screen displays.

2. From the Configuration panel, click CA ARCserve Central Protection Manager Configuration.

3. Complete the following fields:

   - **CA ARCserve Central Protection Manager Server**

     Note: With CA ARCserve Central Protection Manager and CA ARCserve Central Host-Based VM Backup installed, the following fields default to the local CA ARCserve Central Protection Manager server. If CA ARCserve Central Protection Manager is not installed, the fields remain blank and it requires you to configure it manually. You can view the discovered nodes alert information from CA ARCserve Central Reporting.

    - **Machine Name**--The Host Name of the computer where CA ARCserve Central Protection Manager is installed.
    - **User Name**--The User Name that is required to log in to the computer where CA ARCserve Central Protection Manager is installed.
    - **Password**--The password for the user.
    - **Port**--The port number that you must use to communicate with the CA ARCserve Central Protection Manager Web Service.
    - **HTTPS**--This option is selected or unselected based on the connection configured in the CA ARCserve Central Protection Manager server.
  - **Detect Port and Protocol Automatically**--Lets you obtain the CA ARCserve Central Protection Manager Port and Protocol of the Protection Manager database and populates the previous fields.

    Note: This option is enabled only if the remote registry access of the CA ARCserve Central Protection Manager server is allowed.

    To verify if the remote registry is allowed or not, perform the following steps:

    1. Go to the CA ARCserve Central Protection Manager server where CA ARCserve Central Protection Manager is installed.

    2. Navigate to services.msc and verify that the 'Remote Registry' service has started.

    3. Set to 'Automatic'.
  - **Test--**Lets you verify that the access information for the CA ARCserve Central Protection Manager is correct.

4. Click Save.

Configure Discovery Schedules

You can configure the Discovery schedule for nodes on a repeating basis and on a scheduled time. By default, Discovery Configuration is disabled. To enable the configuration, click the Enable option to specify the type of repeating method that you want and a scheduled time for the node discovery to begin. You can specify the following parameters to configure your Discovery schedule:

- **Every number of days--**Lets you repeat this method on the number of days that are specified. (Default)
- **Every selected day of the week--**Lets you repeat this method on the days that are specified. Monday, Tuesday, Wednesday, Thursday, and Friday are the default days of the week.
- **Every selected day of the month--**Lets you repeat this method on the specified day of the month. 1 is the default option for the day of the month.

A vCenter/ESX Host list is displayed for you to view when setting up a schedule to discover nodes.

Configure the Email and Alert Settings

You can configure email and alert settings for use with your application to send alerts automatically under conditions you specify.

Follow these steps:

1. Log in to the application.

   From the Navigation bar on the home page, click Configuration to open the Configuration screen.

2. From the Configuration panel, click Email and Alert Configuration to open the Email and Alert Configuration options.

3. Complete the following fields:

   - **Service**--Specify the type of email service from the drop-down. (Google Mail, Yahoo Mail, Live Mail or Other).
   - **Mail Server**--Specify the host name of the SMTP server that you want CA ARCserve Central Applications to use to send email.
   - **Requires Authentication**--Select this option when the mail server that you specified requires authentication. The Account Name and Password are required.
   - **Subject**--Specify a default email subject.
   - **From**--Specify the email address the email is being sent from.
   - **Recipients**--Specify one or more email addresses, separated by a semicolon(;), the email is being sent to.
   - **Use SSL**--Select this option if the mail server you specified requires secure connection (SSL).
   - **Send STARTTLS**--Select this option if the mail server you specified requires STARTTLS command.
   - **Use HTML format**--Lets you send the email messages in HTML format. (selected by default)
   - **Enable Proxy Settings**--Select this option if there is a proxy server and then specify the proxy server settings.

4. Click Test Email to verify that the mail configuration settings are correct.
5. (Optional) From the Send Email Alerts section, click Discovered nodes to let the application send email alert messages when new nodes are discovered.
6. Click Save.

   Note: You can click Reset to revert to the previously saved values or click Delete to delete your saved settings. Deleting your email and alert settings prevents you from receiving email alert messages.

The email configuration is applied.

Configure Update Schedules

The application lets you set up a schedule that automatically downloads product updates from a CA Server or a local software staging server.

Follow these steps:

1. Log in to the application.
2. Click Configuration on the Navigation bar to open the Configuration screen.

3. From the Configuration panel, click Update Configuration.

   The update configuration options appear.

4. Select a Download Server.

   - **CA Server**--Click Proxy Settings for the following options:

     - **Use browser proxy settings--**Lets you use the credentials that provided for the browser proxy settings.

       Note: The Use browser proxy settings option affects Internet Explorer and Chrome.

     - **Configure proxy settings**--Specify the IP Address or Host Name of the proxy server and the port number. If the server you specified requires authentication, click Proxy server requires authentication and provide the credentials.

       Click OK to return to Update configuration.

   - **Staging Server--**If you select this option, click Add Server to add a staging server to the list. Enter its host name and Port number and click OK.

     If you specify multiple staging servers, the application tries to use the first server listed. If connection succeeds, the remaining servers listed are not used for staging.

5. (Optional) Click Test Connection to verify the server connection and wait until the test completes.

6. (Optional) Click Automatically check for updates, and then specify the day and time. You can specify a daily or weekly schedule.

Click Save to apply the Update configuration.

Configure Proxy Settings

CA ARCserve Central Applications let you specify a proxy server to communicate with CA Support to check for and download available updates. To enable this capability, you specify the proxy server that you want to communicate in behalf of the CA ARCserve Central Applications server.

Follow these steps:

1. Log in to the application and click Configuration on the Navigation bar.

   The Configuration options appear.

2. Click Update Configuration.

   The update configuration options display.

3. Click Proxy Settings.

   The Proxy Settings dialog opens.

4. Click one of the following options:

   - **Use browser proxy settings--**Lets the application detect and use the same proxy settings that are applied to the browser to connect to the CA Technologies server for update information.

     Note: This behavior applies to only Internet Explorer and Chrome browsers.

   - **Configure proxy settings--**Lets you define an alternative server that the application will use to communicate with CA Support to check for updates. The alternative server (proxy) can help ensure security, increased performance, and administrative control.

     Complete the following fields:

     - **Proxy Server--**Specify the host name or IP address of the proxy server.
     - **Port--**Specify the port number that the proxy server will use to communicate with the CA Support website.
     - **(Optional) Proxy server requires authentication--**If the login credentials for the proxy server are not the same as the credentials for the CA ARCserve Central Applications server, click the check box next to Proxy server requires authentication and specify the User Name and Password that is required to log in to the proxy server.

       Note: Use the following format to specify the user name: <domain name>/<user name>.

   Click OK.

The proxy settings are configured

Note: To help ensure that CA ARCserve Central Host-Based VM Backup can deploy policies to nodes and can protect CA ARCserve D2D nodes, verify that the Host-Based VM Backup server and the proxy server can communicate with each other using their host names. Perform the following steps:

1. From the CA ARCserve Central Host-Based VM Backup server, ping the proxy server using the host names of the server.
2. From the proxy server, ping the CA ARCserve Central Host-Based VM Backup server using the host name of the server.

Configure Social Networking Preferences

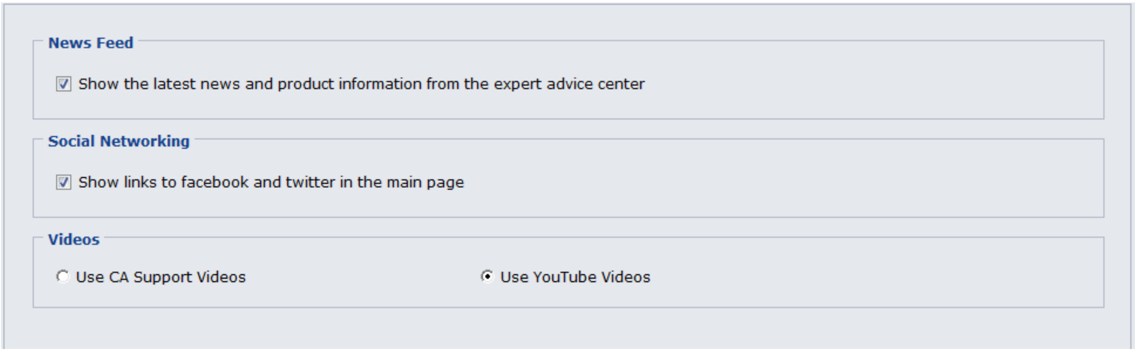
CA ARCserve Central Applications let you manage the social networking tools that can help you manage each application. You can generate news feeds, specify links to popular social networking websites, and select video source websites.

Follow these steps:

1. Log in to the application.

   From the Navigation bar on the home page, click Configuration to open the Configuration screen.

2. From the Configuration panel, click Preferences Configuration to open the Preferences options.



News Feed

☑ Show the latest news and product information from the expert advice center

Social Networking

☑ Show links to facebook and twitter in the main page

Videos

○ Use CA Support Videos ● Use YouTube Videos

3. Specify the options that you require:

   - **News Feed--**Lets the application display RSS feeds about CA ARCserve Central Applications and CA ARCserve D2D related news and product information (from the Expert Advice Center). The feeds appear on the home page.
   - **Social Networking--**Lets the application display icons on the home page for access to Twitter and Facebook for CA ARCserve Central Applications and CA ARCserve D2D related social networking websites.
   - **Videos**--Lets you select the type of video to view your CA ARCserve Central Applications and CA ARCserve D2D products. (Use YouTube Videos is the default video.)

   Click Save.

   The Social Networking options are applied

4. From the Navigation bar, click Home.

   The Home Page displays.

5. Refresh your browser window.

   The Social Networking options are applied.

Modify the Administrator Account

CA ARCserve Central Applications let you modify the user name, password, or both for the administrator account after you install the application. This administrator account is used only for the default display user name on the login screen.

Note: The user name specified must be a Windows administrative account or an account that has Windows administrative privileges.

Follow these steps:

1. Log in to the application and click Configuration in the Navigation bar.

   The configuration options appear.

2. Click Administrator Account
3. The Administrator account settings appear.
4. Update the following fields, as required:
   - User Name
   - Password

   Click Save

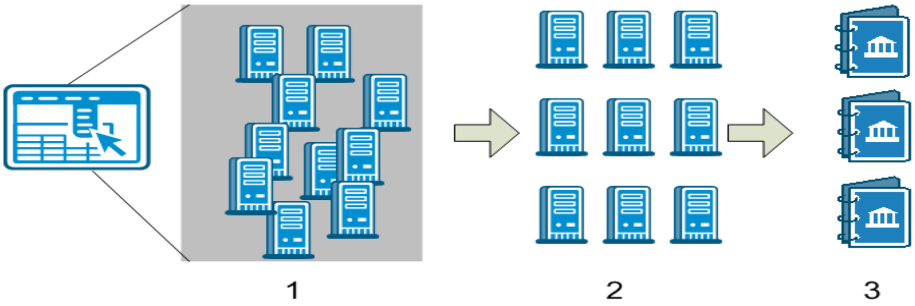
The administrator account is modified.

Chapter 3: Using CA ARCserve Central Host-Based VM Backup

This section contains the following topics:

How You Set Up Your Production Environment

Protecting your virtual machine environment requires a few basic activities:



1. Add the nodes to CA ARCserve Central Host-Based VM Backup. You can import all virtual machines hosted by an ESX or vCenter Server.

2. Group the nodes to make them easier to manage. For example, you can group nodes by business function, or by installed applications.

3. Create back up policies and assign a policy to a node. All nodes are backed up according to the policy you set.

How to Use the CA ARCserve Central Host-Based VM Backup Home Page

Launching the CA ARCserve Central Host-Based VM Backup opens a home page in your web browser. From the home page, you can perform the following tasks:

- **Left-side Navigation**:
  - **Node**--Node screen lets you view your virtual machine environment according to node groups, installed applications and vSphere Policy assigned.
  - **Policies**--vSphere Policies screen lets you create, edit, and assign backup policies to all nodes in your environment.
  - **Configuration**--Configuration screen lets you specify the email alerts and auto-update schedule for the application.
  - **View Logs**--View Logs screen lets you find specific issues: Information, Errors, or Warnings.
  - **Add New tab**--You can manually add the name and URL of any website you want to monitor.
  - **CA Support**--Lets you get access to various support and social network sites including Facebook and Twitter.

Log In to CA ARCserve D2D Nodes

From the Host-Based VM Backup home page, you can log in to CA ARCserve D2D nodes.

To log in to CA ARCserve D2D nodes

1. Open the application and click Nodes in the Navigation Bar.

   The Node screen displays.

2. From the Groups list, click All Nodes, or click the group that contains the CA ARCserve D2D node that you want to log in to.

   The nodes list displays all nodes associated with the specified group.

3. Browse to and click the node that you want to log in to and then click Login D2D from the pop-up menu.

   A CA ARCserve Central Host-Based VM Backup version of CA ARCserve D2D opens.

   Note: If a new browser window does not open, verify that the pop-up options for your browser allow all pop-ups or pop-ups only for this website.

You are logged in to the CA ARCserve D2D node.

Note: The first time that you log in to the CA ARCserve D2D node, an HTML page may open and display a warning message. This behavior can occur when using Internet Explorer. To correct this behavior, close Internet Explorer and repeat Step 3. You should then be able to log in to the CA ARCserve D2D node successfully.

How to Manage Node Tasks for CA ARCserve Central Host-Based VM Backup

This scenario explains how Storage Managers can manage nodes. For example, adding or discovering nodes, assigning nodes to node groups, and updating or deleting nodes from the Node screen.

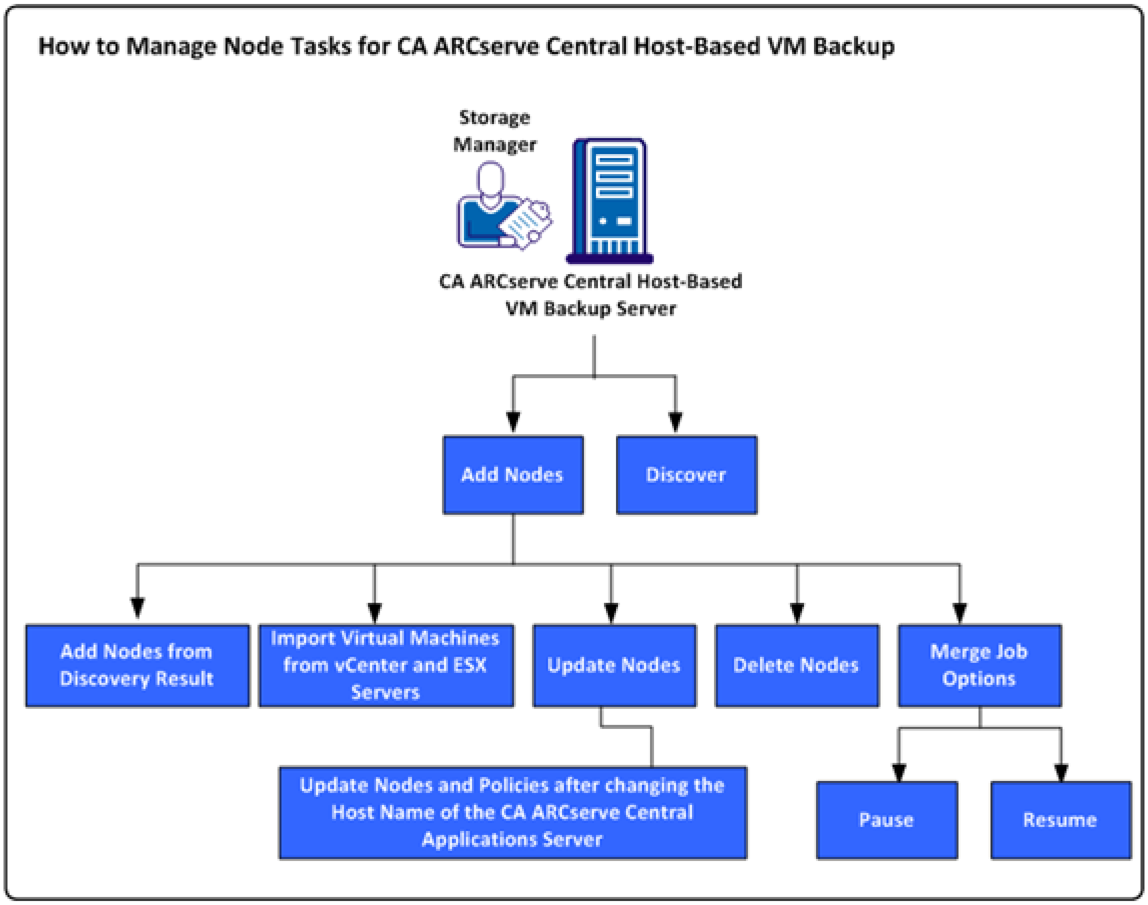
The following table describes the items that are displayed on the Node screen:

Column Name	Description
Node Name	Displays the name of the node. **Note**: Some nodes that are listed may not be enabled for you to select. The reason is because the node cannot be detected by the server. For example, the node can be deleted from the server.
Policy	Displays the name of the policy and the policy deployment status.
Virtual Machine Name	Displays the name of the virtual machine.
vCenter/ESX	Displays the server details that helps detect virtual machines.
Job (see page 69)	Displays the status of the backup job and links you to the Backup Status Monitor (see page 70) for more details.

Column Name	Description
Status	Displays the status of the node: ■ ❌ = Error/Failed ■ ❗ = Warning ■ ✅ = Successful If you hover your mouse over the icon, a Node Status Summary pop-up table appears with results for the following categories: ■ Last Backup - Displays the type, the date and time, and the status of the backup. ■ Recovery Points - Displays the number of recovery points for your monitored server. ■ Destination Capacity - Displays the amount of free space available at your backup destination.
Last Backup Result	Displays the status of the last backup job.
Last Backup Time	Displays the date and time of the last backup job.
PFC Status	Displays the status of the preflight check for your backup jobs: ■ ❌ = Error/Failed ■ ❗ = Warning ■ ✅ = Successful The icon determines whether a backup job can run or not for the specific node. If you hover your mouse over the icon, a Verification pop-up table appears with results for the following categories: ■ Changed Block Tracking (CBT) - Displays the CBT result for the backup. ■ VMware Tools - Displays whether the VMware tool is installed or not. ■ Disk - Displays the status of the disk. ■ Power State - Displays whether the virtual machine is powered on or off. ■ Credentials - Displays the status of the user credentials. ■ Applications - Displays the installation status of the application on the node. For more details, see topic Perform Preflight Checks for Your Backup Jobs (see page 58).

Column Name	Description
Applications	Displays what application the node is associated with.
OS	Displays what operating system the node is associated with.
Description	Displays a description of the node.

The following diagram illustrates the tasks that you can perform on Nodes.


How to Manage Node Tasks for CA ARCserve Central Host-Based VM Backup
Storage Manager
CA ARCserve Central Host-Based VM Backup Server
Add Nodes
Discover
Add Nodes from Discovery Result
Import Virtual Machines from vCenter and ESX Servers
Update Nodes
Delete Nodes
Merge Job Options
Update Nodes and Policies after changing the Host Name of the CA ARCserve Central Applications Server
Pause
Resume

This scenario describes the options that you can use when adding or updating nodes:

- Discover (see page 43)
- Add Nodes (see page 44)
  - Add Nodes from Auto Discovery Result Automatically (see page 45)
  - Import Virtual Machines from vCenter and ESX Servers (see page 46)
- Update Nodes (see page 47)
  - Update Nodes and Policies after changing the Host Name of the CA ARCserve Central Applications Server (see page 48)
- Delete Nodes (see page 48)
- Merge Job Options (see page 49)
  - Pause a Merge Job on a Node (see page 49)
  - Resume a Merge Job on a Node (see page 50)

Discover Nodes from CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based VM Backup lets you discover nodes automatically by adding vCenter Server and ESX Server systems to your environment. By adding them, the application can detect virtual machines that they host automatically.

Important! The process of discovering nodes requires you to specify the host name or IP address of the vCenter Server or ESX Server system. This information lets the discovery process discover virtual machines attached to vCenter Server and ESX Server systems. When you find it necessary to modify the host name or IP address of a vCenter Server or ESX Server system, repeat the steps in this topic and then redeploy the backup policy to create a new backup set with the updated host name or IP address.

Follow these steps:

1. Log in to the application and click Node on the Navigation bar to open the Node screen.
2. Click Discover on the toolbar to open Discover Nodes by vCenter/ESX server dialog.
3. On the Discover Nodes by vCenter/ESX server dialog, complete the following fields:
   - vCenter/ESX Host
   - User Name

     Note: The account that you specify must be an account with administrative privileges on the ESX Server or vCenter Server system.
   - Password
   - Port

   Click Add.

   Note: Repeat this step to add more vCenter/ESX Server systems.
4. Click Discover to start the discovery process.

   The Discovery Monitor opens, showing the discovery progress.
5. When the discovery process completes, a confirmation message appears: Do you want to continue to add nodes from Discovery Result?

   Click Yes and the Add nodes from the Discovery Result screen is displayed or click No if you have more hypervisors to add.

   Note: To detect the nodes automatically and add them to the Node Name list, see the topic Configure Discovery Schedules for more details.
6. From the Nodes Discovered list, click the nodes that you want to add and then click the right arrow. The nodes are added to the Nodes to Protect list.
7. Click Next to open the Node Credentials screen.

8. Provide a user name and password for each node you want to add or specify the appropriate global credentials.

   Click Finish.

   The nodes that you selected are added to the Node Names list on the Node screen for the Node Group selected.

9. (Optional) Click Refresh. The server that you added is now listed in the Groups list on the Node screen.

10. (Optional) Click Discover and repeat the previous steps until all servers are added.

Add Nodes

As your environment grows, you can use the Node screen to add nodes and then assign nodes to groups that you want to manage within the application. The application adds only virtual machines where:

- Guest OS is Windows
- VMware hardware version is 7 or greater.

You can add nodes using the following processes:

- Add nodes from Discovery Result (see page 45)--Discovery permits you to enter ESX and vCenter Server details, detect the virtual machines running on each server and then manually or automatically add the detected nodes to the application where they can be managed and protected.

  Servers added to the Discover list are scanned according to the schedule you specify on the Configuration screen until you remove them. You do not need to enter server details again. The Discover list displays only new virtual machines added to a server since the last scan. It does not show the VMs already managed in the application. You can also run Discover without waiting for the next scheduled scan.

- Import virtual machines from vCenter/ESX (see page 46)

  This option is a manual process. The process requires that you specify ESX or vCenter server details each time you launch it. You can add servers to the discovery list when you want to avoid re-entering server details. This option lists all the virtual machines that are detected on the specified server, even if they are already managed in the application.

Add Nodes from Discovery Result

This option lets you select the nodes that are automatically detected based on the settings you specified in the Discovery Configuration panel.

Follow these steps:

1. Log in to the application.

   Click Nodes on the Navigation bar to open the Nodes screen.

2. From the Node category, click Add and then click Add nodes from Discovery result on the pop-up menu.

   The Add nodes from Discovery result screen opens displaying a list of the discovered nodes.

3. From the Nodes Discovered list, select the nodes that you want to add and click the arrow to add them to the Nodes to Protect list. Click Next when you are finished.

   Note: You can filter the list by Node Name or Domain to minimize the list.

4. (Optional) Select one or more nodes and click Hide Selected Nodes to hide nodes you do not want to back up.

5. (Optional) Check the Show hidden nodes option to display any hidden nodes back on to the Nodes Discovered list. To hide the nodes again, uncheck the option.

6. On the Node Credentials screen, provide a User Name and Password for the node you want to add. You can specify global credentials or can apply credentials to the selected nodes.

7. Click Finish.

The nodes are added.

Import Virtual Machines from vCenter/ESX

You can add nodes using the Import virtual machines from the vCenter/ESX Server option. This task lets the application discover all of the virtual machines running on the specified host, but does not perform periodic automatic scans. If you add virtual machines later, repeat this procedure or the new virtual machines are not recognized.

Consider the following distinctions between this option and the Discover task:

- Specify ESX Server and vCenter Server details each time you launch this option.
- You have the option of adding any servers you specify to the Discover list so you do not have to enter credentials each time.
- All available virtual machines are listed every time that you use this option. Even the virtual machines that are managed by the application are listed.

Follow these steps:

1. Log in to the application.

   Click Node on the Navigation bar to open the Node screen.

2. Click Add on the toolbar and then click Import virtual machines from vCenter/ESX on the pop-up menu.

   The Discover Nodes dialog opens.

3. Complete the following fields on the Discover Nodes dialog:

   - vCenter/ESX Host

     Note: As a best practice, specify the host name of the vCenter Server system when you are running VMware Distributed Resource Scheduling (DRS) in your environment. This approach helps ensure that CA ARCserve Central Host-Based VM Backup can detect the virtual machines running in your environment and backups of DRS enabled virtual machines complete successfully. For more information about Distributed Resource Scheduling, see the VMware website.

   - User Name
   - Password
   - Port
   - Protocol

   Click Connect and wait until the scanning is complete.

4. (Optional) Enable the option Add vCenter/ESX server to Discovery list automatically.

5. Click Next to open the Node Credentials dialog.

6. On the Node Credentials screen, provide a global User Name and Password for all virtual machines that are detected and click the Apply to selected option. Or, click a VM to enter specific credentials.
7. Click Finish.

The virtual machines that you selected are added to the Node Group that you specified.

Note: CA ARCserve Central Host-Based VM Backup is unable to detect the host names of virtual machines that are in a powered off state or VMware Tools is not installed. Under these conditions, Unknown displays in the Host Name field on the Node screen after you import the nodes. In addition, the Node Name filter (on the Node screen) cannot filter nodes that are named using Unknown.

Update Nodes

CA ARCserve Central Host-Based VM Backup lets you update information about nodes that were added previously.

Follow these steps:

1. Log in to the application.

   From the Navigation Bar on the home page, select Node.

   The Node screen displays.

2. From the Groups bar, click the All Nodes group or click the group name containing the nodes that you want to update.

   The nodes that are associated with the group appear in the nodes list.

3. Click the nodes that you want to update and then right-click and click Update Node from the pop-up menu.

   The Update Node dialog opens.

   Note: To update all nodes in the node group, right-click the Node Group name and then click Update Node from the pop-up menu.

4. Update the node details as needed.

   Note: To update multiple nodes on the Node list, select the desired nodes, right-click any node, and click Update Node from the pop-up menu. The user name and password are the same for all selected nodes. By default, the Specify new credentials option and the Take control of the node check box is selected. You can specify a new user name and password for the selected nodes and can force this server to manage the nodes. In addition, you can select Use existing credentials to apply the current user name and password. The fields become disabled.

5. Click OK.

   The Update Node dialog closes and the nodes are updated.

Update Nodes and Policies After Changing the Host Name of the CA ARCserve Central Applications Server

After you change the host name of the CA ARCserve Central Host-Based VM Backup server, you update the nodes and the policies that are applied to the nodes. You perform these tasks to maintain the relationship between the server and the nodes that the server is protecting. The following table describes the possible scenarios and the corrective action for each scenario.

Scenario	Corrective Action
The node was added after the host name of the CA ARCserve Central Host-Based VM Backup server was changed.	No corrective actions are required.
The node was added before the host name of the CA ARCserve Central Host-Based VM Backup server was changed and a policy was not applied to the node.	Update the node. For more information, see Update Nodes (see page 47).
The node was added before the host name of the CA ARCserve Central Host-Based VM Backup server was changed and a policy was applied to the node.	Reapply the policy. For more information, see Assign Policies to Virtual Machines.

Delete Nodes

You may delete nodes as needed.

Follow these steps:

1. Log in to the application.

   Click Node on the Navigation bar to open the Node screen.

2. From the Groups bar, click the All Nodes group or click the group name containing the node that you want to delete.

   The nodes that are associated with the group appear in the nodes list.

3. Check one or more nodes that you want to delete and then click Delete on the toolbar.

   A confirmation message opens.

4. Do one of the following:

   - Click Yes to delete the node.
   - Click No if you do not want to delete the node.

Merge Job Options

CA ARCserve Central Host-Based VM Backup lets you pause and resume merge jobs for each node at any time. The process of pausing and resuming merge jobs does not affect in-progress jobs.

Pause a Merge Job on a Node

CA ARCserve Central Host-Based VM Backup lets you pause a merge job on a specific node.

For example, merge jobs can consume system resources and cause backup jobs to run slowly. Use the pause option to stop an in-progress merge job so that in-progress backup jobs can complete at their highest level of efficiency. After the backups complete, you can then resume the merge job.

Follow these steps:

1. From the CA ARCserve Central Host-Based VM Backup home page, click Node on the Navigation bar to open the Node screen.
2. Select the node group that contains the nodes with merge jobs you want paused.

   A list of nodes for the selected Node Group displays.
3. Click the nodes with merge jobs you want paused. Then right-click the selected nodes and click Pause Merge Job from the pop-up menu.

   Note: By default, the Pause Merge Job option is disabled. When the node is running a merge job, as indicated in the Job column, the Pause Merge Job option becomes enabled.

The merge job of the selected node is paused and can be verified on CA ARCserve D2D home page.

Resume a Merge Job on a Node

CA ARCserve Central Host-Based VM Backup lets you resume merge jobs that were paused for a specific node.

Follow these steps:

1. From the CA ARCserve Central Host-Based VM Backup home page, click Node on the Navigation bar to open the Node screen.
2. Select the node group that contains the nodes with merge jobs you want resumed.

   A list of nodes for the selected Node Group displays.
3. Click the nodes with merge jobs that are paused which you now want resumed. Then right-click the selected nodes and click Resume Merge Job from the pop-up menu.

   Note: The Resume Merge Job option is enabled when a backup job is not running and the merge jobs are paused.

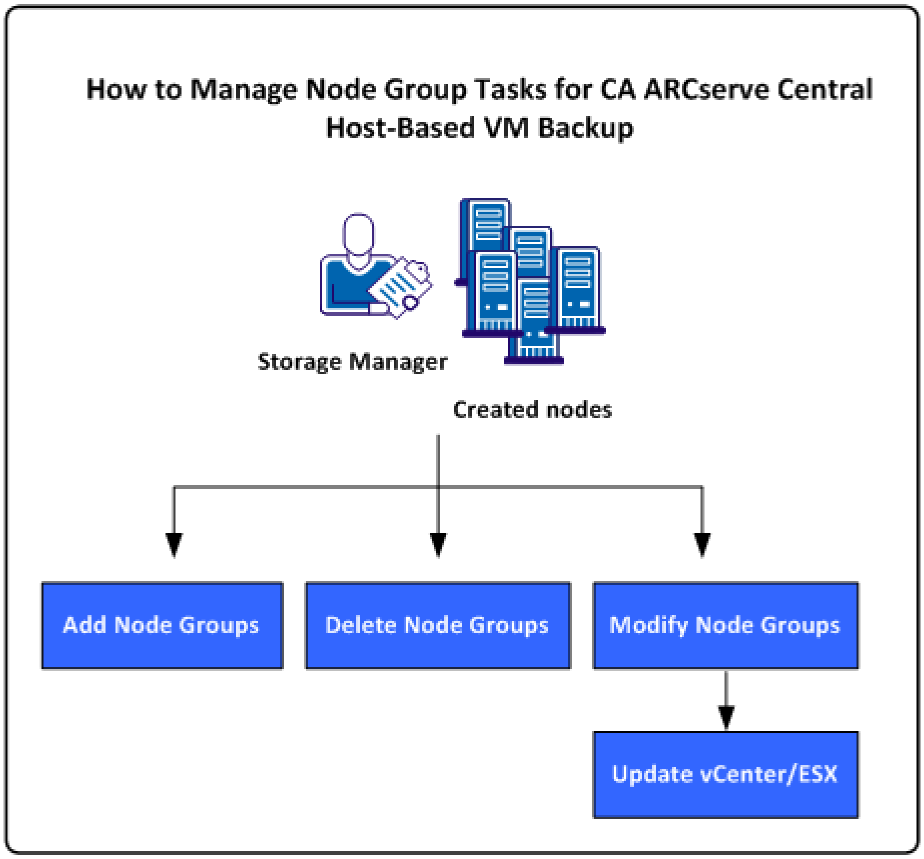
The merge job of the selected node is resumed and can be verified on CA ARCserve D2D home page.

How to Manage Node Group Tasks for CA ARCserve Central Host-Based VM Backup

With CA ARCserve Central Host-Based VM Backup, a Storage Manager can protect numerous virtual machines as easily as protecting one.

Start by adding nodes. You can group nodes by application or by their purpose. Creating node groups let you easily visualize your virtual machines environment. You can create backup policies and can assign a policy to nodes to simplify protection of your virtual environment. For more details, see How to Manage Policies for CA ARCserve Central Host-Based VM Backup (see page 71).

The following illustration describes the tasks that you can perform for Node Groups:



This scenario describes the following topics:

- Add Node Groups (see page 52)
- Delete Node Groups (see page 54)
- Modify Node Groups (see page 55)

Add Node Groups

When you first import a virtual machine from an ESX or vCenter Server host, a new node group is automatically added.

Node groups let you manage a collection of CA ARCserve D2D source computers based on common characteristics. For example, you can define node groups classified by the department they support: Accounting, Marketing, Legal, Human Resources, and so on.

The application contains the following node groups:

- **Default Groups:**
  - **All Nodes--**Contains all nodes associated with the application.
  - **Nodes without a Group**--Contains all nodes associated with the application that are not assigned to a node group.
  - **Nodes without a Policy**--Contains all nodes associated with the application that do not have a policy assigned.
  - **SQL Server--**Contains all nodes associated with the application and Microsoft SQL Server is installed on the node.
  - **Exchange--**Contains all nodes associated with the application and Microsoft Exchange Server is installed on the node.

  Note: You cannot modify or delete the default node groups.
- **Custom Groups--**Contains customized node groups.
- **vCenter/ESX Groups**--When you add a node from the "Import virtual machines from vCenter/ESX" option, the name of the vCenter/ESX server is added to this group.

Follow these steps:

1. Log in to the application.

   From the Navigation bar on the home page, click Node to open the Node screen.
2. Click Add on the Node Group toolbar.

   The Add Group dialog opens and nodes appear in the Available Nodes list.
3. Specify a Group Name for the node group.
4. Specify the following fields from the Add Group dialog:
   - **Group--**Select the group name containing the nodes that you want to assign.
   - **Node Name Filter--**Lets you filter the available nodes based on common criteria.

     Note: The Node Name filter field supports the use of wildcard characters.

     For example, Acc* lets you filter all nodes having a node name that begins with Acc. To clear the filter results, click X in the Filter field.

5. To add nodes to the node group, select the node or nodes that you want to add and click the single right arrow.

   The nodes move from the Available Node list to the Selected Nodes list, and are assigned to the node group.

   Note: To select and move all the nodes from the current group, click the double right arrow.

6. (Optional) To move nodes from the Selected Nodes list to the Available Nodes list, click the single left arrow.

   Note: To select and move all nodes in the current group, click the double left arrow.

7. Click OK.

The Node Group is added.

Delete Node Groups

You may delete a node group as needed. When you delete a group that was manually added, the virtual machines are not removed from the application. However, if you delete a group that was automatically created from an ESX or vCenter Server discovery, the group and all virtual machines are deleted from the application.

The application lets you delete the Node Groups that you created.

You cannot delete the following node groups:

- **All Nodes--**Contains all nodes associated with the application.
- **Nodes without a Group**--Contains all nodes associated with the application that are not assigned to a node group.
- **Nodes without a Policy**--Contains all nodes associated with the application that do not have a policy assigned.
- **SQL Server--**Contains all nodes associated with the application and Microsoft SQL Server is installed on the nodes.
- **Exchange--**Contains all nodes associated with the application and Microsoft Exchange Server is installed on the nodes.

Note: The process of deleting node groups does not delete individual nodes from the application.

Follow these steps:

1. Log in to the application.

   From the Navigation Bar on the home page, click Node to open the Node screen.

2. Click the node group that you want to delete and then click Delete in the Node Group toolbar.

   The Confirm message box dialog opens.

3. If you are sure that you want to delete the node group, click Yes.

   Note: Click No if you do not want to delete the node group.

The node group is deleted.

Modify Node Groups

The application lets you modify the node groups that you created. You can add and remove nodes from node groups and change the name of node groups.

Note: You cannot modify the following node groups:

- **All Nodes--**Contains all nodes associated with the application.
- **Nodes without a Group**--Contains all nodes associated with the application that are not assigned to a node group.
- **Nodes without a Policy**--Contains all nodes associated with the application that do not have a policy assigned.
- **SQL Server--**Contains all nodes associated with the application and Microsoft SQL Server is installed.
- **Exchange--**Contains all nodes associated with the application and Microsoft Exchange Server is installed.

Follow these steps:

1. Log in to the application.

   From the Navigation Bar on the home page, click Node.

   The Node screen displays.

2. Click the node group that you want to modify and then click Modify in the Node Group toolbar.

   The Modify Group dialog opens.

3. To modify the Group Name, specify a new name in the Group Name field.

4. To add nodes to the node group, select the node or nodes that you want to add to the node group and click the right arrow.

   The nodes move from the Available Node list to the Selected Nodes list, and are assigned to the node group.

   Note: To move all nodes from the Available Node list to the Selected Nodes list, click the double right arrow.

5. To remove nodes from the node group, click the left arrow or the double left arrow to remove one or all nodes respectively.

6. (Optional) To filter the available nodes based on common criteria, specify a filtering value in the Node Name Filter field.

   Note: The Filter field supports the use of wildcard characters.

   For example, Acc* lets you filter all nodes having a node name that begins with Acc. To clear the filter results, click the X in the Filter field.

7. Click OK.

The node group is modified.

Update vCenter and ESX Server Details

CA ARCserve Central Host-Based VM Backup lets you update the vCenter and ESX Server details that were added previously.

Follow these steps:

1. From the Node screen, expand the vCenter/ESX Groups from the Groups bar.
2. Select the vCenter/ESX group that you want to update the server details for and then right-click and click Update vCenter/ESX.

   The Update vCenter/ESX dialog opens.

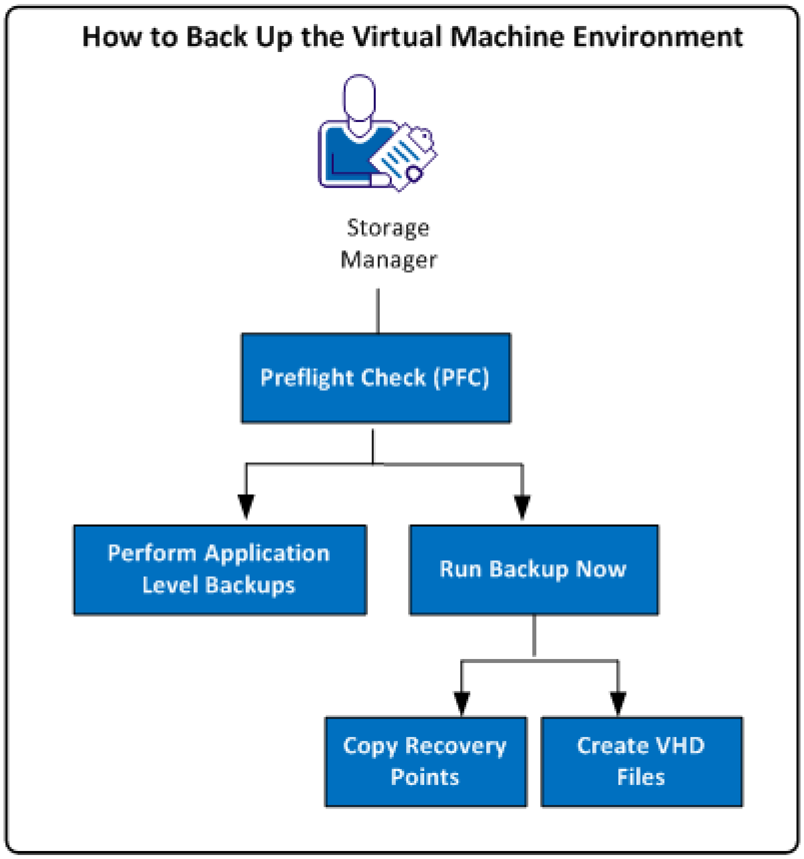
3. Update the vCenter/ESX Server details accordingly.
4. Click OK.

   The Update vCenter/ESX dialog closes and the node group is updated.

How to Back Up the Virtual Machine Environment

This scenario explains how a Storage Manager can back up and protect all virtual machines in your environment.

The following diagram illustrates how to back up the virtual machine environment.



The following list describes the processes that are illustrated in the diagram:

- Perform Preflight Checks for your Backup Jobs (see page 58)
- Run a Backup Now (see page 62)
  - Copy the Backup Recovery Points (see page 64)
  - Create VHD Files (see page 68)
- Perform Application Level Backups (see page 68)

Perform Preflight Checks for Your Backup Jobs

CA ARCserve Central Host-Based VM Backup features a utility called Preflight Check (PFC) which enables you to run vital checks on specific nodes to detect conditions that can cause backup jobs to fail. PFC runs automatically when you perform the following actions:

- Import virtual machines from a vCenter Server/ESX Server system
- Add nodes from the Discovery result
- Update a node

In addition, you can also perform a Preflight Check manually.

Follow these steps:

1. Log in to the application.

   Click Nodes on the Navigation bar to open the Nodes screen.

2. Do one of the following actions to specify the nodes that you want to run a preflight check from:

   - **Node level**: Click the group containing the nodes that you want to run a preflight check on and then click the check box next to the nodes. Then right-click the nodes and click Preflight Check from the context menu.
   - **Group level**: Right-click the group containing the nodes and click Preflight Check.

   A message is displayed, "Starting to preflight check the virtual machine."

3. Scroll to the PFC Status column and view the status of the Preflight Check.

The following table describes the checks that are performed by PFC:

Item	Description
Changed Block Tracking (CBT)	(CBT) is a feature that tracks disk sectors that are located on a virtual machine that have changed. This helps minimize the size of the backups. This item verifies that CBT is enabled.
VMware Tools	This item verifies that the VMware tools are installed on each virtual machine.
Disk	This item verifies the disks of the virtual machine.
Power State	This item verifies that the virtual machine is powered on.
Credentials	This item verifies that the user credentials are valid.

Item	Description
Applications	This item verifies whether Microsoft SQL Server and Microsoft Exchange Server are installed or not.

For more information on resolving errors and warnings for the Preflight Check results, see topic Solutions for Preflight Check Items (see page 59).

Solutions for Preflight Check Items

The following tables describe the solutions to help you resolve errors and warnings from your Preflight Check results:

Changed Block Tracking (CBT)

Status	Message	Solution
Warning	Changed Block Tracking is enabled with snapshots present. A full disk backup will be applied.	To apply the used block backup, perform the following steps: 1. Delete all the snapshots associated with the virtual machine. 2. Log in to the Host-Based VM proxy server. 3. Open the registry editor and locate the following key: HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\VM_InstanceUUID\<UUID> 4. Set registry key to "full disk backupForFullBackup"=0. 5. Create/set the registry to ResetCBT=1. 5. Submit the backup job.

VMware Tools

Status	Message	Solution
Warning	Out of date.	Install the latest version of VMware Tools.
Warning	Not installed or not running.	Install the latest version of VMware Tools and ensure that the tool is running.

Disk

Status	Message	Solution
Error	VM snapshots are not supported for the VM because it has a SCSI controller configured for bus-sharing configuration.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the VM.
Warning	The physical Raw Device Mapping (RDM) disk will not be backed up.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the VM.
Warning	The virtual Raw Device Mapping (RDM) disk will back up as a full disk.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the VM.
Warning	The independent disk will not be backed up.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the VM.
Warning	The application will back up the disk on the NFS data store as a full disk.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the VM.

Power State

Status	Message	Solution
Warning	Powered off	Power on the virtual machine.
Warning	Suspended	Power on the virtual machine.

Credentials

Status	Message	Solution
Warning	Incorrect credentials.	Provide valid user credentials.
Warning	Not provided.	Provide valid user credentials.

Applications

Status	Message	Solution
Warning	Application level restore is not supported because the VM has IDE disks.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the Microsoft SQL Server and Exchange Server data.
Warning	VMware VIX is not installed on the host server.	Download VIX from the VMware website and install it on the CA ARCserve Central Applications host server.
Warning	VMware VIX on the CA ARCserve Central Host-Based VM Backup server is out-of-date.	Download VIX from the VMware website and install it on the CA ARCserve Central Applications host server.
Warning	Application level restore is not supported because there is no ESX Server support.	Upgrade ESX Server to 4.1 or higher or use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the Microsoft SQL Server and Exchange Server data.
Warning	Application level restore is not supported because there are not enough SCSI slots available.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the Microsoft SQL Server and Exchange Server data.
Warning	The source resides on a dynamic disk. Application level restore is not supported.	Use CA ARCserve Central Protection Manager or CA ARCserve D2D to back up the Microsoft SQL Server and Exchange Server data. **Note**: VMware does not support application-level quiescing on virtual machines that are Windows Server 2008 or later with dynamic disks running on ESX Server 4.1 or later.
Warning	Unable to retrieve information about the application. This can prevent application level backups from completing successfully.	Disable UAC in the Windows operating system of the virtual machine.

Run a Back Up Now

Typically, backups are performed automatically and controlled by the schedule settings. However, there may be times when you need 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.

Follow these steps:

1. Log in to the application.
2. From the Navigation bar on the home page, click Node to open the Node screen.
3. Do one of the following actions to specify the nodes that you want to back up:
   - **Node level:** Click the group containing the nodes that you want to back up and then click the check box next to the nodes that you want to back up.
   - **Group level:** Click the group containing the nodes that you want to back up.
4. Then do one of the following actions to back up the node:
   - Click Backup on the toolbar.
   - Right-click the selected group or right-click the nodes and click Backup Now on the context menu.

5. On the Run a backup now dialog, specify a backup type by clicking one of the following types:

   - **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 since the previous backup.

     Note: 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. Be aware of the following advantages and disadvantages to performing Verify backups:
     - 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.

6. (Optional) Specify the Backup Name and click OK. If you do not specify a name, by default, it is named Customized/Full/Incremental/Verify Backup.

A confirmation screen appears, and the selected type of backup is launched immediately.

Be aware of the following behavior:

- All values specified in the Policy dialogs are applied to the job.
- If a custom (ad-hoc) backup job fails, no makeup job is created. A makeup job is only created for a failed scheduled job.
- CA ARCserve Central Host-Based VM Backup applies the following backup jobs in priority order:
  - Full
  - Verify
  - Incremental

  The following conditions occur when a Backup Now is submitted and a job is waiting in the queue:

  - When a Full Backup job is submitted and a Verify Backup job is waiting in the queue, the Full Backup job overwrites the job in the queue.
  - When a Full Backup job is submitted and an Incremental Backup job is waiting in the queue, the Full Backup job overwrites the job in the queue.
  - When a Verify Backup job is submitted and an Incremental Backup job is waiting in the queue, the Verify Backup job overwrites the job in the queue.
  - When a Verify Backup job is submitted and a Full Backup job is waiting in the queue, the Verify Backup job is skipped.
  - When an Incremental Backup job is submitted and a Full Backup job is waiting in the queue, the Incremental Backup job is skipped.
  - When an Incremental Backup job is submitted and a Verify Backup job is waiting in the queue, the Incremental Backup job is skipped.

Copy Recovery Points

Each time CA ARCserve D2D performs a successful backup, a point-in-time snapshot image of your backup is also created. This collection of recovery points allows you to locate and specify a backup image to copy. You can do the following to protect your backups:

- Copy/export recovery point information to store it safely off-site when a catastrophe occurs.
- Save your recovery points to multiple locations.
- Consolidate your backups if your destination is getting full and you still want to preserve all your recovery points.

When you select a recovery point to copy, you are also capturing all previous backup blocks that are needed to recreate a full and most recent backup image.

Follow these steps:

1. Log in to the application.

   Click Node on the Navigation bar to open the Node screen.

2. From the Groups list, click All Nodes, or click the group that contains the CA ARCserve D2D node with the recovery points you want to copy.

   The nodes list displays all nodes that are associated with the specified group.

3. Browse to and click the node that you want to log in to and then click Login D2D from the pop-up menu.

   The CA ARCserve D2D opens and you are logged in to the home page for the CA ARCserve D2D node.

   Note: Help ensure that the pop-up options on your browser window are enabled.

4. From the CA ARCserve D2D home page, select Copy Recovery Point.

   The Copy Recovery Point dialog opens.

5. In the Backup Location field, 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 User name and Password credentials to gain access to that location.

6. In the Virtual Machine field, click the drop-down list next to Select Virtual Machine to specify the virtual machine containing the recovery points that you want to copy.

   The calendar view highlights all dates during the displayed time period that contain recovery points for that backup source.

7. 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.

      Note: A clock icon with a lock symbol indicates that the recovery point contains encrypted information and requires a password for the restore.

   b. Select a recovery point that you want to copy.

      The corresponding backup content (including any applications) for that recovery point is displayed.

8. Click Next.

   The Copy Options dialog opens.

Note: Two password fields are displayed in this dialog. The Password field is for the password to decrypt the source session, and the Encryption Password field is used to encrypt the destination session.

a. If the exported recovery point was previously encrypted, a password is required.

   - If the exported recovery point is a backup session of the same machine running the copy recovery point job, the encryption password is saved and automatically populated.
   - If the exported recovery point is a backup session of another machine, an encryption password is required.

b. Select the destination.

   You can either specify a location or browse to the location where the copy of your selected recovery point is stored. You can click the green arrow icon button to verify the connection to the specified location. If necessary, enter the User name and Password.

c. Select the level of compression to perform.

   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 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 -** No compression is 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.
   - **Standard Compression -** Some compression is performed. This option provides a good balance between CPU usage and disk space usage. This option 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.

   Consider the following points:

   - If your backup image contains uncompressible data (such as JPG images, ZIP files), additional storage space is used to handle such data. As a result, if you select any compression option with uncompressible data in your backup, it can actually result in an increase in your disk space usage.
   - If you change the compression level from "No Compression" to "Standard Compression" or "Maximum Compression", or from "Standard Compression" or "Maximum Compression" to "No Compression", the first backup that is performed after this change automatically becomes a Full Backup. After the Full Backup is performed, all future backups (Full, Incremental, or Verify) will be performed as scheduled.

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

   You can change, add, or remove encryption for the copied recovery point.

   - Select the type of encryption algorithm that is used for the copy.

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

   - Provide (and confirm) an encryption password.

9. 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 only allows one recovery point copy job to run at the same time.

   The recovery point image is copied from the backup source to the copy destination.

Create VHD Files from CA ARCserve Central Host-Based VM Backup

This CA ARCserve D2D procedure lets you create a Virtual Hard Disk (VHD) file from the recovery point that is created after every successful backup. For more information, see the CA ARCserve D2D Appendix.

Follow these steps:

1. Perform the Copy Recovery Points (see page 64) procedure.
2. When the copy is finished, browse to the destination you specified and navigate to the CA ARCserve D2D host.
3. Open the folder, VStore\S0000000001.
4. Locate all files with a D2D extension and change each to VHD. After you rename all files, you can use them as regular VHD files.

Perform Application Level Backups

Generally, no special steps are required to protect Microsoft Exchange or SQL Server systems. However, depending on the way you perform a restore when a problem occurs enables certain options.

For example, enabling the Exchange Granular Catalog option on the Backup Settings/Advanced screen allows you to recover a specific mailbox or individual email message later. You can also restore folders or email messages directly from Windows Explorer.

To perform a full application backup, ensure that the following points are acknowledged:

- All application writers are in a stable state. Use *vssadmin* to see writer status.
- All databases that are backed up are in a healthy state. For example, for SQL Server, make sure that the database status is not *Restoring*.

You can also truncate transaction logs for SQL and Exchange Servers separately.

Note: When you upgrade to an ESX server, then upgrade the VMware tools inside the guest operating systems before performing application-level backups to avoid "out of date" errors.

Perform Full Disk Backups Containing Only Used Block Data

Retrieving used block data after performing full disk backups helps reduce the backup window and less space requirement from the backup destination.

Note: Due to VMware limitation, used blocks cannot be retrieved from virtual machines when recovery point snapshots are present. In such cases, a full disk backup is performed on the virtual machine.

After a full disk backup is submitted, perform the following steps to retrieve the used block data:

1. Delete all the snapshots that are associated with the virtual machine.
2. Log in to the CA ARCserve Central Host-Based VM Backup virtual machine.
3. Open the registry editor and locate the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFBackupDll\VM_InstanceUUID\<UUID>
4. Set the registry key "full disk backupForFullBackup" to 0.
5. Create or set the registry "ResetCBT" to 1.
6. Submit the backup job.

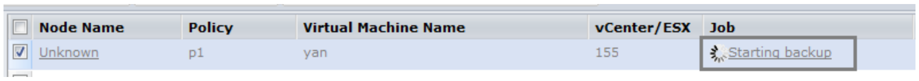
View Job Status Information

CA ARCserve Central Virtual Standby converts CA ARCserve D2D recovery points to recovery point snapshots. You can view status information about in-progress Host-Based VM Backup jobs.

When a job is running, you can view detailed information about the job. You can also stop the current job.

Follow these steps:

1. Log in to the application.
2. Click Nodes on the Navigation bar to open the Node screen.
3. If there are in-progress Host-Based VM Backup jobs, the phase of the job appears in the Job field as illustrated by the following screen:



□	Node Name	Policy	Virtual Machine Name	vCenter/ESX	Job
☑	Unknown	p1	yan	155	Starting backup

4. Click the phase to open the Backup Status Monitor dialog.

   Note: For information about the fields that appear on the Backup Status Monitor, see Backup Status Monitor (see page 70).

5. Do one of the following options:

   - Click Close to close the Backup Status Monitor dialog.
   - Click Cancel to stop the current job.

     Note: The Backup Status Monitor dialog closes shortly after you click Cancel.

More Information:

View Job Status Information (see page 69)

Host-Based VM Backup Monitoring Tasks

You can view the status of your virtual machine backups from the Node screen. Search for the node that has a job in progress from the Job field, click the link, and this dialog opens.

Virtual Machine backups are performed in two phases. First, the virtual hard disks are backed up and then, if successful, the catalog is generated. The catalog lets you restore files and folders as well as the entire virtual machine.

The monitor displays the following real-time information about the backup status job:

- **Phase--(Backup and Catalog Monitors)** Displays the current point in the process that is represented by the shaded portion of the progress bar.
- **Start Time--(Backup and Catalog Monitors)** Displays the date and time the operation was started based on policy configuration.
- **Elapsed Time--(Backup and Catalog Monitors)** Displays the difference between the Start Time and current time.
- **Estimated Time Remaining--(Backup Monitor only)** Displays the length of time that is estimated to complete the job.
- **Processing**--**(Catalog Monitor only)** Displays the volume drive letter or application for which the catalog is currently being generated.
- **Space Saved due to Compression--(Backup Monitor only)** Displays the portion of disk space that is saved if compression was specified in the backup operation policy.
- **Compression Level**--**(Backup Monitor only)** Displays the type of compression that is used for backups. The options can be No Compression, Standard Compression (default), or Maximum Compression.
- **Encryption--(Backup Monitor only)** Displays the encryption method that is selected when the backup job was configured.

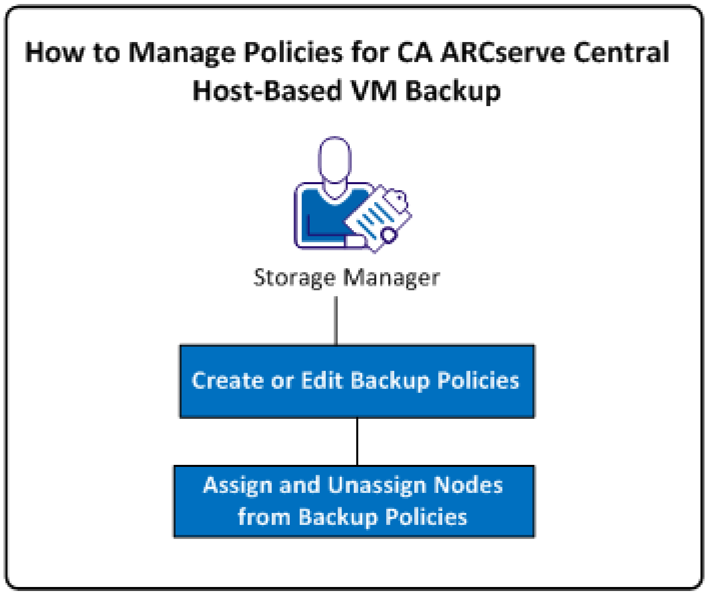
- **Write Speed Limit--(Backup Monitor only)** Displays the value if Throttle Backup was set on the Protection Settings screen of the backup policy.
- **Write Speed--(Backup Monitor only)** Displays the actual write speed in megabytes per minute.
- **Read Speed--(Backup Monitor only)** Displays the actual read speed in megabytes per minute.

How to Manage Policies for CA ARCserve Central Host-Based VM Backup

Backup policies define how and when to back up nodes that are imported from the vCenter/ESX Server. Storage Managers can create and edit backup policies and then assign and unassign them from nodes.

Note: You can assign a policy to one or more nodes. However, you cannot assign one or more policies to a node.

The following diagram illustrates the process of administering backup policies.


How to Manage Policies for CA ARCserve Central Host-Based VM Backup
Storage Manager
Create or Edit Backup Policies
Assign and Unassign Nodes from Backup Policies

The following list describes the processes that are illustrated in the diagram:

- Create Backup Policies (see page 72)
- Edit Backup Policies (see page 75)
- Assign and Unassign Nodes from Backup Policies (see page 77)

Create Backup Policies

The process of creating backup policies uses the CA ARCserve D2D interface for configuring backup settings, with a few distinctions. You can create policies that are based on similar backup needs, for example, by installed application or by schedule.

The following procedure summarizes the steps that are required for creating a simple CA ARCserve D2D backup job policy. For complete details on creating CA ARCserve D2D backup policies, see the appropriate CA ARCserve D2D topics in the Appendix.

Note: During a host-based backup operation, the following message appears if you are using hotadd as the transport mode:

You need to format the disk in drive <driveLetter> before you can use it. Do you want to format it?

Click Cancel to ignore this message. The message occurs when the operating system detects that the virtual hard disk was added to the backup proxy server. The operating system assumes that the virtual hard disk is a new device that requires formatting. If you click Format Disk in error, no damage occurs since the virtual hard disk is read-only.

Follow these steps:

1. Log in to the application.

   Click Policies on the Navigation bar to open the Policies screen.

2. Click New on the toolbar to open the New Policy dialog.

3. Enter a Policy Name that appropriately describes the policy.

4. On the Backup Settings tab, click Protection Settings and specify the following information:

   - **Backup Destination**--Specify the local volume or remote shared folder where you want to save your backup sessions.
   - **CA ARCserve D2D VM Backup Proxy**--Specify the Hostname or IP address of the server where CA ARCserve D2D has been installed. If CA ARCserve D2D is not already installed, you can use CA ARCserve Central Protection Manager to deploy it. Provide the appropriate credentials for this server. The Port number defaults to 8014. If you changed this default during CA ARCserve D2D installation, specify the correct port number.
   - **Retention Setting**--You can set the retention policy that is 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 incrementals). The default option is Retain Recovery Points. For more details, see Specify Protection Settings from the CA ARCserve Central Protection Manager User Guide.
   - **Compression**--Select a compression level. The default value is Standard. You can specify no compression or Maximum compression.
   - **Encryption**--Specify an encryption level. The default value is no encryption. When specifying an encryption level, provide an encryption password that is used to restore encrypted data.
   - **Throttle Backup**--Enter the rate at which backups are written to disk. Lower this rate to reduce CPU or network load but note that doing so increases backup times. This option is disabled by default.

5. Click Schedule and complete the following information:

   - **Start date and time**--Specify the date and time you want to begin your backup jobs.
   - **Incremental Backup**--Define a repeat schedule for your incremental backup jobs. The default value is to repeat Incremental Backups once a day.
   - **Full Backup**--Define a repeat schedule for your full backup jobs. By default, this value is set to Never Repeat.
   - **Verify Backup**--Define a repeat schedule for verify backup jobs. By default, this value is set to Never Repeat.

6. Click Advanced and enable the following options if you want to truncate application log files:

   - **SQL Server**--Specify a daily, weekly, or monthly truncation schedule.
   - **Exchange Server**--Specify a daily, weekly, or monthly truncation schedule.

7. Click Pre/Post Backup Settings and specify any desired pre/post-backup commands. If needed, provide the proper credentials:

   - **Run a command before backup is started**--Enter the script command to run before starting the backup job.
   - **On exit code**--Enable this option if you want to trigger the script command on a specific exit code.
   - **Run Job**--If selected, the software continues running the job if the specified exit code is returned.
   - **Fail Job**--If selected, the software aborts the backup job if the specified exit code is returned.
   - **Run a command after snapshot is taken**--Enter the script command to run after the snapshot is taken.
   - **Run a command after backup is over**--Enter the script command to run after backup completes.

8. (Optional) Click the Preferences tab. Configure any of the following email alerts, as needed:

   - Missed Jobs
   - vCenter/ESX cannot be reached (before backup)
   - License failure
   - Backup, Catalog, Restore or Copy job failure/crash/cancel
   - Backup, Catalog, Restore or Copy job success
   - Destination free space is less than
   - Merge failure

     Note: A merge failure can occur for the following reasons:

     - The session is mounted.

       To solve the problem, dismount the session.

     - A catalog job locks the session.

       The next backup job automatically merges this session.

     - The session is locked due to other reasons.

   - Skip/Merge job waiting in the job queue

If you enable these options, click Email Settings to configure your email server. Provide the Service type, Mail Server, and Port. If authentication is required, enable that option and provide credentials.

- Specify the Subject to appear in the email, for example, CA ARCserve Central Host-Based VM Backup Alert.
- Specify a From value, for example, CA ARCserve Central Host-Based VM Backup.
- Specify an email address for all Recipients. Separate each address with a semi-colon (;).

You can enable the Proxy Settings by providing the Proxy Server name, Port, and the required credentials.

Click OK.

9. Click Save.

Edit or Copy Backup Policies

CA ARCserve Central Host-Based VM Backup lets you edit or copy CA ARCserve D2D backup policies after they are created.

Follow these steps:

1. Log in to the application.

   Click Policies on the Navigation bar to open the Policies screen.

2. From the Policies screen, click the check box next to a policy and do one of the following:

   - Click Edit on the toolbar and edit the selected policy.
   - Click Copy on the toolbar to copy and create a new policy from the selected policy.

     Note: When you copy a policy, the Copy Policy dialog opens. Specify a name for the new policy and click OK.

   The Edit Policy dialog opens.

3. If you want to change the name of the policy name, specify a name in the Policy Name field.

4. On the Backup Settings tab, click Protection Settings and complete the following information:

   - **Backup Destination**--Specify a remote shared folder where you want to save your backup sessions.
   - **CA ARCserve D2D VM Backup Proxy**--Specify the host name or IP address of the server where CA ARCserve D2D has been installed. If CA ARCserve D2D is not already installed, you can use CA ARCserve Central Protection Manager to deploy it. Provide the appropriate credentials for this server. The Port number defaults to 8014. If you changed this default during CA ARCserve D2D installation, specify the correct port number.
   - **Retention Setting**--You can set the retention policy that is 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 incrementals). The default option is Retain Recovery Points. For more details, see Specify Protection Settings from the CA ARCserve Central Protection Manager User Guide.
   - **Compression**--Select a compression level. The default value is Standard. You can specify no compression or Maximum.
   - **Encryption**--Specify an encryption level. The default value is no encryption. When specifying an encryption level, provide an encryption password that is used to restore encrypted data.
   - **Throttle Backup**--Enter the rate at which backups are written to disk. Lower this rate to reduce CPU or network load but note that doing so increases backup times. This option is disabled by default.

5. Click Schedule and complete the following information:

   - **Start date and time**--Specify the date and time you want to begin your backup jobs.
   - **Incremental Backup**--Define a repeat schedule for your incremental backup jobs. The default value is to repeat Incremental Backups once a day.
   - **Full Backup**--Define a repeat schedule for your full backup jobs. By default, this value is set to Never Repeat.
   - **Verify Backup**--Define a repeat schedule for verify backup jobs. By default, this value is set to Never Repeat.

6. Click Advanced and enable the following options if you want to truncate application log files:

   - **SQL Server**--Specify a daily, weekly, or monthly truncation schedule.
   - **Exchange Server**--Specify a daily, weekly, or monthly truncation schedule.

7. Click Pre/Post Backup Settings and specify any required pre/post-backup commands. If needed, provide the proper credentials:

   - **Run a command before backup is started**--Enter the script command to run before starting the backup job.
   - **On exit code**--Enable this option if you want to trigger the script command on a specific exit code.
   - **Run Job**--If selected, the software continues running the job if the specified exit code is returned.
   - **Fail Job**--If selected, the software aborts the backup job if the specified exit code is returned.
   - **Run a command after snapshot is taken**--Enter the script command to run after the snapshot is taken.
   - **Run a command after backup is over**--Enter the script command to run after backup completes.

8. (Optional) Click the Preferences tab. Configure any desired email alerts, as needed. If you enable these options, click Email Settings to configure your email server.
9. Click Save.

The policy is edited or copied.

Assign and Unassign Nodes from Backup Policies

To protect multiple virtual machines, select the policy that you wish to use and then assign it to one or more nodes.

Follow these steps:

1. Log in to the application.

   Click Policies on the Navigation bar to open the Policies screen.

2. From the Policies screen, click the Policy Assignment tab.
3. From the Policies list, select the policy that you want to assign.

   Click Assign and Unassign to open the Assign/Unassign Policy dialog.

4. Specify the following fields from the Assign/Unassign Policy dialog:

   - **Group--**Lets you select the group name containing the nodes that you want to assign.
   - **Node Name Filter--**Lets you filter the available nodes based on common criteria.

     Note: The Node Name field lets you filter nodes using wildcard characters.

     For example, Acc* lets you filter all nodes having a node name that begins with Acc. To clear the filter results, click X in the Filter field.

5. Do one of the following actions:

   - **Assign nodes to policies--**Select the nodes that you want to add and click the single right arrow.

     The nodes move from the Available Nodes list to the Selected Nodes list.

     Note: To select and move all nodes, click the double right arrow.

   - **Unassign nodes from policies--**Select the nodes that you want to unassign and click the single left arrow.

     The nodes move from the Selected Nodes list to the Available Nodes list.

     Note: To select and move all nodes, click the double left arrow.

   Click OK.

6. If necessary, provide a global user name and password and apply them to the selected nodes.

   Click OK.

   The selected nodes are added to the Policy Assignment list with a Deploy Status of [Assigned] Pending.

   Note: You can also view the Deploy Status on the Node screen.

7. Click Deploy Now to apply the assigned policy to the specified nodes immediately. Use the Refresh button to update the status.

On the Node screen, the status for the nodes you specified on the Policy Assignment list now shows the assigned policy in the Policy column. Click the Node Name and click Login D2D to verify the status of your backup jobs.

View CA ARCserve Central Host-Based VM Backup logs

The View Log contains comprehensive information about all the operations performed by your application. 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 may occur.

To view CA ARCserve Central Host-Based VM Backup logs

1. From the home page, click View Logs in the navigation bar.

   The View Logs screen appears.

2. From the drop-down lists, specify log information that you want to view.

   - **Severity--**Lets you specify the severity of the log that you want to view. You can specify the following severity options:

     - **All--**Lets you view all logs, regardless of the severity.
     - **Information--**Lets you view only logs that describe general information.
     - **Errors--**Lets you view only logs that describe severe errors that occurred.
     - **Warnings--**Lets you view only logs that describe warming errors that occurred.
     - **Errors and Warnings--**Lets you view only severe errors and warning errors that occurred.

- **Module--**Lets you specify the module for which you want to view logs. You can specify the following module options:
  - **All--**Lets you view logs about all application components.
  - **Common--**Lets you view logs about common processes.
  - **Import Nodes from Auto Discovery**--Lets you view logs on nodes that were imported only from Auto Discovery.
  - **Import Nodes from Hypervisor**--Lets you view logs on nodes that were imported only from Hypervisor.
  - **Policy Management--**Lets you view only logs about managing policies.
  - **Updates--**Lets you view only logs about updating the application.
  - **Preflight Check**--Lets you view only logs that ran the Preflight Check status for each node.
  - **Submit VM Backup Jobs**--Lets you view only logs where nodes were submitted for virtual machine backup jobs.
- **Node Name--**Lets you view only logs for a specific node.

  Note: This field supports the wildcard '*' and '?'. For example, enter 'lod*' to return all activity logs for the machine name that begins with 'lod'.

Note: The Severity, Module, and Node Name options can be applied collectively. For example, you can view Errors (severity) that relate to Updates (Module) for Node X (Node Name).

The logs display based on the view options specified.

Note: The displayed Time in the log is based on the time zone of your application's database server.

View Activity Log Information for a Specific Node

CA ARCserve Central Host-Based VM Backup lets you view activity log information for a specific CA ARCserve D2D node. The Activity Log provides an audit trail of every job that ran (with the most recent activities listed first) and can be helpful in troubleshooting any problems that occur.

To view Activity Log information for a specific node

1. Open the application and click Node in the Navigation bar.

   The Node screen displays.

2. From the Groups list, click All Nodes, or click the group that contains the CA ARCserve D2D node that you want to log in to.

   The nodes list displays all nodes associated with the specified group.

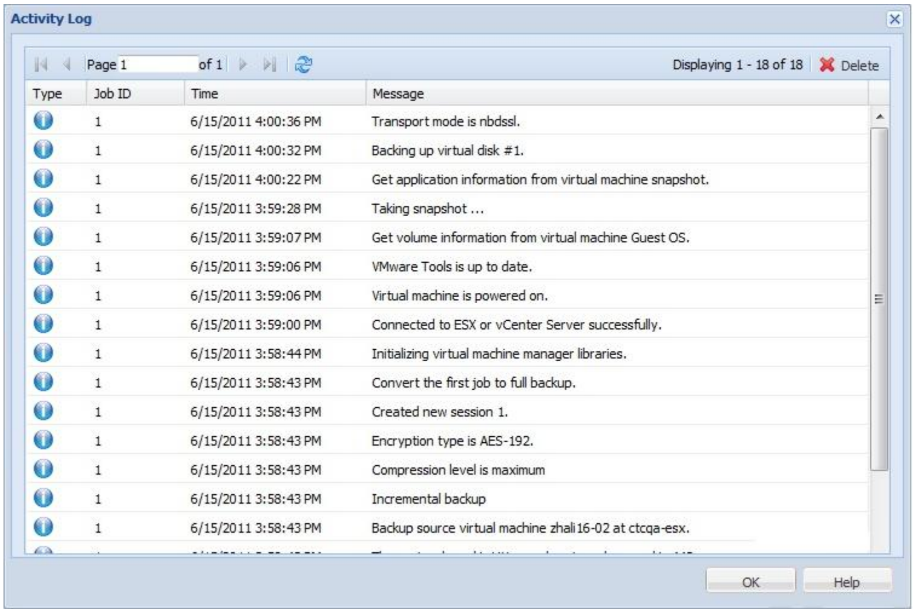
3. Browse to and click the node that you want to log in to and then click Login D2D from the pop-up menu.

   The CA ARCserve D2D opens and you are logged in to the home page for the CA ARCserve D2D node.

   Note: If a new browser window does not open, verify that the pop-up options for your browser allow all pop-ups or pop-ups only for this website.

4. Click View Logs on the Tasks list.

   The Activity Log opens as illustrated by the following:



Type	Job ID	Time	Message
ℹ	1	6/15/2011 4:00:36 PM	Transport mode is nbdssl.
ℹ	1	6/15/2011 4:00:32 PM	Backing up virtual disk #1.
ℹ	1	6/15/2011 4:00:22 PM	Get application information from virtual machine snapshot.
ℹ	1	6/15/2011 3:59:28 PM	Taking snapshot ...
ℹ	1	6/15/2011 3:59:07 PM	Get volume information from virtual machine Guest OS.
ℹ	1	6/15/2011 3:59:06 PM	VMware Tools is up to date.
ℹ	1	6/15/2011 3:59:06 PM	Virtual machine is powered on.
ℹ	1	6/15/2011 3:59:00 PM	Connected to ESX or vCenter Server successfully.
ℹ	1	6/15/2011 3:58:44 PM	Initializing virtual machine manager libraries.
ℹ	1	6/15/2011 3:58:43 PM	Convert the first job to full backup.
ℹ	1	6/15/2011 3:58:43 PM	Created new session 1.
ℹ	1	6/15/2011 3:58:43 PM	Encryption type is AES-192.
ℹ	1	6/15/2011 3:58:43 PM	Compression level is maximum
ℹ	1	6/15/2011 3:58:43 PM	Incremental backup
ℹ	1	6/15/2011 3:58:43 PM	Backup source virtual machine zhali16-02 at ctcqa-esx.

   The Activity Log provides the following information:

   - **Type--**Specifies the severity of the activity, which includes Information, Warnings, and Errors.
   - **Job ID--**Specifies the job for which the activity applies.
   - **Time--**Specifies the data and time for which the activity applies.
   - **Message--**Describes the activity.

5. Click OK to close the Activity Log.

Add Links to the Navigation Bar

Each of the CA ARCserve Central Applications has an Add New Tab link in the Navigation bar. Use this feature to add entries in the Navigation bar for additional web-based applications you would like to manage. However, for every application that is installed, a new link is automatically added to the Navigation bar. For example, if you installed CA ARCserve Central Reporting and CA ARCserve Central Virtual Standby on "Computer A" and then launch CA ARCserve Central Reporting, CA ARCserve Central Virtual Standby is automatically added to the Navigation bar.

Note: Every application that is installed is detected only if other CA ARCserve Central Applications are on the same computer.

Follow these steps:

1. From the Navigation bar of the application, click the Add New Tab link.
2. Specify the Name and URL of the application or website you want to add. For example, www.google.com.

   Optionally, specify the location of an icon.
3. Click OK.

   The new tab is added to the bottom of the Navigation bar.

Be aware of the following considerations:

- The CA Support link is added by default for your convenience.

You can remove the new tab by highlighting the tab and click the Remove link.

Integrate CA ARCserve Central Host-Based VM Backup With CA ARCserve Central Applications

If you installed CA ARCserve Central Protection Manager and CA ARCserve Central Reporting, you can centrally monitor the status of your host-based backups.

Considerations for Protecting Raw Device Mappings

Consider the following behavior when protecting raw device mappings (RDM):

- The application does not support protecting physical compatibility mode raw device mappings (disks of this type are physical devices). The application omits physical compatibility mode raw device mappings from the backup source during the backup process. A solution to this behavior is to install CA ARCserve D2D inside the guest operating system and perform backups in the same manner as you would back up physical disks.

- The application supports protecting virtual compatibility mode raw device mappings. However, consider the following limitations:
  - In regard to full backups, the application lets you back up complete virtual compatibility mode RDM disks. However, if you do not use data compression, the backup datasets can be the same size as the source disk.
  - CA ARCserve Central Host-Based VM Backup restores virtual compatibility mode RDM disks as normal virtual disks. After the recovery process completes, the disk is no longer configured as or behaves as a virtual RDM.
  - An alternative approach to backing up virtual compatibility mode RDMs is to install CA ARCserve D2D inside the guest operating system and back up the RDMs in the same manner as you would back up physical machines.

Change Server Communication Protocol

By default, CA ARCserve Central Applications use the Hypertext Transfer Protocol (HTTP) for communication among all of its components. If you are concerned about the security of passwords that are communicated between these components, you can change the protocol being used to Hypertext Transfer Protocol Secure (HTTPS). When you do not need this extra level of security, you can change the protocol being used to HTTP.

Follow these steps:

1. Log in to the computer where the application is installed using an administrative account or an account with administrative privileges.

   Note: If you do not log in using an administrative account or an account with administrative privileges, configure the Command Line to run using the Run as Administrator privilege.

2. Open Windows Command Line.

3. Do one of the following:

   - **To change the protocol from HTTP to HTTPS:**

     Launch the "changeToHttps.bat" utility tool from the following default location (the location of the BIN folder can vary depending upon where you installed the application):

     C:\Program Files\CA\ARCserve Central Applications\BIN

     When the protocol has been successfully changed, the following message displays:

     The communication protocol was changed to HTTPS.

   - **To change the protocol from HTTPS to HTTP:**

     Launch the "changeToHttp.bat" utility tool from the following default location (the location of the BIN folder can vary depending upon where you installed the application):

     C:\Program Files\CA\ARCserve Central Applications\BIN

     When the protocol has been successfully changed, the following message displays:

     The communication protocol was changed to HTTP.

4. Restart the browser and reconnect to CA ARCserve Central Applications.

   Note: When you change the protocol to HTTPS, a warning displays in the web browser. This behavior occurs because of a self-signed security certificate that prompts you to ignore the warning and proceed or add that certificate to the browser to prevent the warning from coming back in future.

Define a Transport Mode for Backups

You can define a specific transport mode (transfer data) to use for D2D backup jobs that execute using Host-Based VM Backup. By default, Host-based VM backup uses a mode that lets Host-Based VM Backup to optimize the performance (increase the speed) of the backup operation. However, when you want to specify a particular transport mode for backup operations, you configure the registry key described in this topic.

Host-Based VM Backup can execute backups using the following transport modes:

- HOTADD transport mode (see page 237)
- NBD transport mode (see page 237)
- NBDSSL transport mode (see page 237)
- SAN transport mode (see page 238)

Be aware of the following considerations:

- This is an optional configuration task. By default, Host-Based VM Backup executes backups using a transport mode that optimizes the performance of the backup operation.
- When you configure this registry key to use a specific transport mode and the mode is not available, Host-Based VM Backup uses an available default transport mode for the backup operation.

Follow these steps:

1. Log in to the CA ARCserve D2D backup proxy system for the virtual machines.

   Open Windows Registry Editor and browse to the following key:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D\AFBackupDll\{VM-InstanceUUID}].
   ```

2. Right-click VM-InstanceUUID and select New and click String Value on the pop-up menu.

   Name the new string value as follows:

   ```
   EnforceTransport
   ```

3. Right-click EnforceTransport and click Modify on the pop-up menu to open the Edit String dialog.
4. In the Value Data field, specify the transport mode that you want to use during the backup job. Specify one of the following values:

   hotadd

   HOTADD transport mode (see page 237)

   nbd

   NBD transport mode (see page 237)

   nbdssl

   NBDSSL transport mode (see page 237)

   san

   SAN transport mode (see page 238)

5. Click OK to apply the value and close the Edit String dialog.

The transport mode is defined and is used the next time that a job runs.

Chapter 4: Restore and Recover Virtual Machines

The restore and recovery options available depend on how your system was backed up. For example, you cannot use backup sessions that are created with CA ARCserve Central Host-Based VM Backup to perform Application Level or Microsoft Exchange granular restore operations but can do so using sessions created with CA ARCserve Central Protection Manager or CA ARCserve D2D. Certain restore options available with CA ARCserve D2D may not be available with this application. For example, Restore to Original Location is not possible with the application's backups because the location of the proxy server is different from the location of the backup source virtual machine.

For more information, see Restore Considerations (see page 96) to help you determine when to use the available Restore Methods (see page 87).

This section contains the following topics:

Restore Methods

How your backup session was created determines which restore methods can be used. For example, some restore methods are only possible if performed with a locally installed version of CA ARCserve D2D. Other methods require the virtual machine powered on at backup time.

Browse Recovery Points

Lets you find available recovery points (successful backups) from a calendar view. Use this method to restore files, folders, or perform the application level restore process.

Backups created with CA ARCserve D2D, CA ARCserve Central Host-Based VM Backup, or CA ARCserve Central Protection Manager can be restored with this method.

Find Files/Folders to Restore

Lets you find specific files or folders to restore.

Backups created with CA ARCserve D2D can be restored with this method. It is also available to restore backups created with CA ARCserve Central Host-Based VM Backup and CA ARCserve Central Protection Manager when the virtual machine was powered on at the time of backup.

Recover VM

Lets you browse all available virtual machine recovery points (successful backups) from a calendar view. You can then specify the virtual machine you want to recover.

This method is available to restore backups created with CA ARCserve Central Host-Based VM Backup and first provisions a virtual machine and then restores the OS, applications and data from the recovery point you specified.

Application Restore

To restore a Microsoft Exchange or SQL Server completely without having to rebuild it, click the Browse Recovery Points method from a locally installed version of CA ARCserve D2D.

Bare Metal Recovery

Bare Metal Recovery (BMR) is the process of restoring a computer from bare metal including its operating system, software applications, settings and data. BMR requires you to have a Windows image or boot kit and at least one full backup. Backups created with CA ARCserve D2D, CA ARCserve Central Host-Based VM Backup, CA ARCserve Central Virtual Standby, and CA ARCserve Central Protection Manager can be restored with this method. However, if the virtual machine was powered down during backup, BMR is not possible.

Restore from Recovery Points

The Browse Recovery Points restore method lets you find successful backups (named recovery points) from a calendar view. You can then browse for and select the backup content, including applications, you want to restore. The procedure for restoring with the Browse Recovery Points method is the same as if using CA ARCserve D2D, with one exception. To restore virtual machine recovery points, you cannot use the restore to original location option.

Follow these steps:

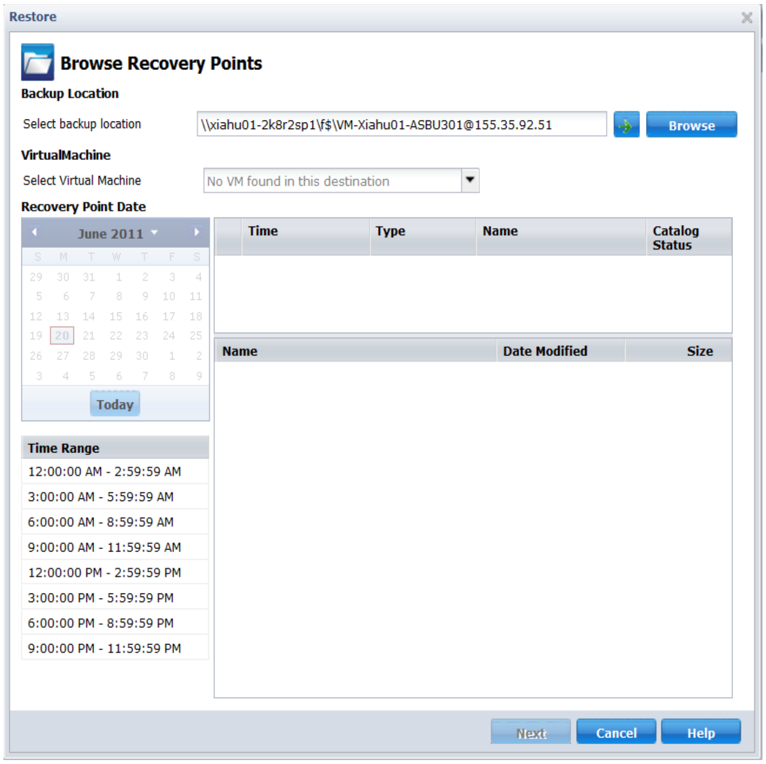
1. Log in to the application and click Node on the Navigation bar.

   From the Node screen, expand the group containing the node that you want to restore.

   Click the check box next to the node that you want to restore and then click Restore on the toolbar.

2. From the Restore dialog, click Browse Recovery Points.

   The Restore dialog opens and the Backup Location is provided for you based on the node you selected. If desired, change it to another backup destination and provide the user credentials.



Restore

Browse Recovery Points

Backup Location

Select backup location: \\xiahu01-2k8r2sp1\f$\VM-Xiahu01-ASBU301@155.35.92.51

VirtualMachine

Select Virtual Machine: No VM found in this destination

Recovery Point Date

June 2011

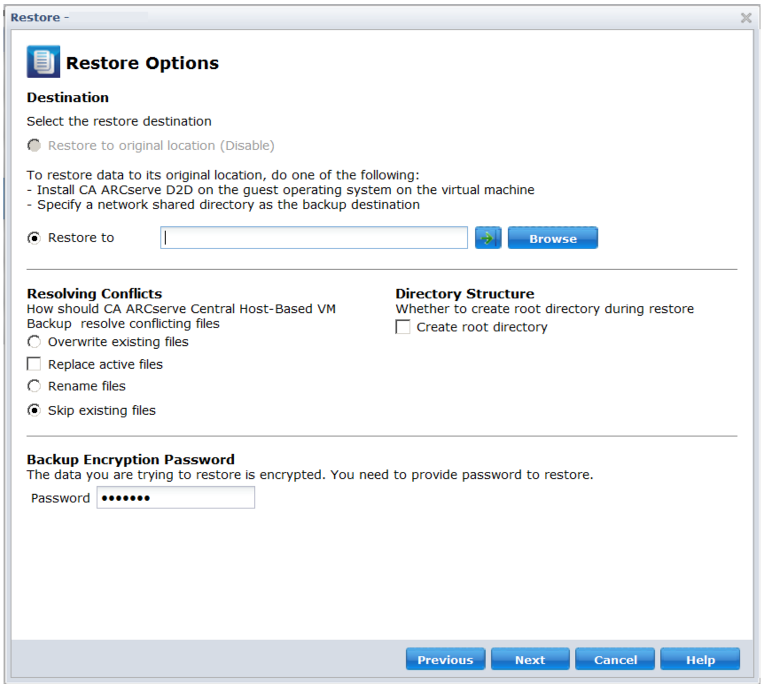
S	M	T	W	T	F	S
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

Time	Type	Name	Catalog Status

Time Range
12:00:00 AM - 2:59:59 AM
3:00:00 AM - 5:59:59 AM
6:00:00 AM - 8:59:59 AM
9:00:00 AM - 11:59:59 AM
12:00:00 PM - 2:59:59 PM
3:00:00 PM - 5:59:59 PM
6:00:00 PM - 8:59:59 PM
9:00:00 PM - 11:59:59 PM

Name	Date Modified	Size

3. Click the recovery point date and then click a recovery point time. Select the content that you want to restore. Select an entire volume or a file, folder, database, or application. Solid green boxes next to a selection indicate that it is selected for restore. Click Next when done.



Restore -

Restore Options

Destination

Select the restore destination

○ Restore to original location (Disable)

To restore data to its original location, do one of the following:
- Install CA ARCserve D2D on the guest operating system on the virtual machine
- Specify a network shared directory as the backup destination

● Restore to

Resolving Conflicts

How should CA ARCserve Central Host-Based VM Backup resolve conflicting files

○ Overwrite existing files

□ Replace active files

○ Rename files

● Skip existing files

Directory Structure

Whether to create root directory during restore

□ Create root directory

Backup Encryption Password

The data you are trying to restore is encrypted. You need to provide password to restore.

Password •••••••

4. On the Restore Options dialog, specify the restore destination.

   - **Restore to original location (disable)**--for CA ARCserve Central Host-Based VM Backup sessions, you cannot restore to the original location. To restore files or folders to their original location in the Guest OS of a VM, you need to either install CA ARCserve D2D in the guest OS of the VM or restore to a network shared folder on the VM.
   - **Restore to**--specify the destination you want to restore to.
   - **Overwrite existing files--**Replaces files located at the destination.
   - **Replace active files--**Replaces files in use or being accessed at reboot time.
   - **Rename files--**Creates a new file if the file name exists. This option copies source files to the destination with the same file name but a new extension. Data is restored to the file with the new extension.
   - **Skip existing files--**Skips over and does not replace existing files that are located on the destination. This is the default setting.
   - **Create root directory--**Recreates the same root directory structure on the destination found in the backup image.

5. Click Next. On the Restore Summary screen, verify that all options are correct. If not, click Previous to go back. If yes, click Finish to launch the restore process.

Restore by Mounting a Recovery Point

The Mount Recovery Point restore method lets you mount a recovery point to the backup proxy system. To mount a recovery point, you would have to log in to the CA ARCserve D2D user interface.

Follow these steps:

1. Log in to CA ARCserve Central Host-Based VM Backup and click Node on the Navigation bar.
2. From the Node screen, expand the group containing the node that you want to restore.

   Click the check box next to the node that you want to restore and then click Restore on the toolbar.

   A CA ARCserve Central Host-Based VM Backup version of CA ARCserve D2D opens.

   Note: Verify that the pop-up options for your browser allow all pop-ups or pop-ups only for this website, so that a new browser can open.

For more details on the Mount Recovery Point dialog, click Help on the dialog screen from the CA ARCserve D2D home page.

Restore Data Using Find Files/Folders to Restore

Each time the application performs a successful backup, all backed up files or folders are included in the snapshot image of your backup. This restore method allows you to specify exactly which file or folder you want to restore.

Follow these steps:

1. Log in to the application and click Node on the Navigation bar.

   From the Node screen, expand the group containing the node that you want to restore.

   Click the check box next to the node that you want to restore and then click Restore on the toolbar.
2. From the Restore dialog, click Find Files/Folders to Restore.
3. On the Find Files/Folders to Restore dialog, specify or browse to the Backup Location. If you are restoring from a CA ARCserve Central Host-Based VM Backup session, you cannot specify a File Copy Location. File Copy restore is permitted only if you are restoring from CA ARCserve Central Protection Manager or CA ARCserve D2D backup sessions.

4. Specify the 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.

5. (Optional) Specify a path name to further filter your search and select whether to include or not include subdirectories or files and folders.

6. Click Find to launch the search.

   The results of the search are displayed. If the search discovers multiple occurrences (recovery points) of the same searched file, it lists all occurrences sorted by date (with the most recent listed first).

7. Select the version that you want to restore from the list and click Next.

   The Restore Options dialog is displayed. You may restore to an alternate location only. Specify or browse to the location where you want the backup image stored. Click the green arrow to verify the connection. Provide user credentials, if needed.

8. Select the conflict resolution options:

   Overwrite existing files

   Overwrites (replaces) any existing files that are located 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, the software discovers that the existing file is currently in use or being accessed and it does not immediately replace that file, but instead to avoid any problems, it delays the replacement of the active files until the next time that you reboot the computer. (The restore occurs immediately, but the replacement of any active files is done during the next reboot).

   Note: If this option is not selected, then any active file is skipped from the restore.

   Rename files

   Creates a new file if the file name 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 does not overwrite (replace) any existing files that are located at the restore destination. Only objects that do not currently exist on your computer are restored from the backup files.

   By default, this option is selected.

9. (Optional) Select Create root directory from the Directory Structure.

   This option recreates the same root directory structure on the restore destination path.

   Note: If this option is not selected, the file or folder is restored directly to the destination folder.

10. Enter the backup encryption password to restore the encrypted data and then click Next.

    The Restore Summary dialog is displayed.

11. 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.

Recover an Entire Virtual Machine

You can recover an entire virtual machine from a CA ARCserve Central Host-Based VM Backup session.

This backup method is similar to performing BMR. With this method you can recover the Windows guest operating system, applications, and data.

Follow these steps:

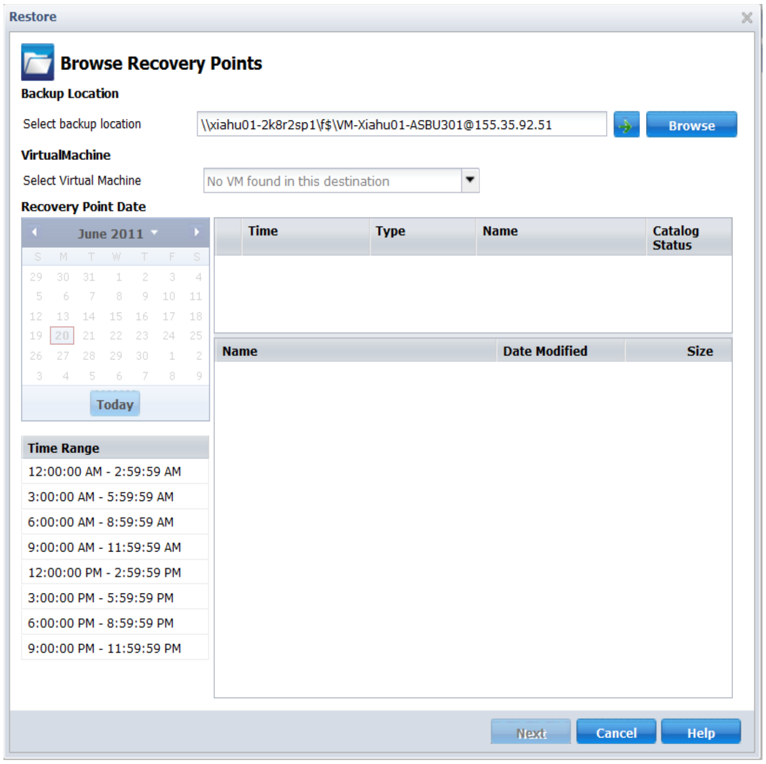
1. Log in to the application and click Node on the Navigation bar.

   From the Node screen, expand the group containing the node that you want to restore.

   Click the check box next to the node that you want to restore and then click Restore on the toolbar.

2. From the Restore dialog, click Recover VM.

3. The Restore dialog opens. The Backup Location and Virtual Machine fields are populated based on the VM that you selected from the Node screen. If desired, change these values.



Restore

Browse Recovery Points

Backup Location

Select backup location: \\xiahu01-2k8r2sp1\f$\VM-Xiahu01-ASBU301@155.35.92.51

VirtualMachine

Select Virtual Machine: No VM found in this destination

Recovery Point Date

Specify the source where your virtual machine backup sessions are stored. Enter user credentials if prompted.

The drop-down menu lists all the virtual machines at the location in the Backup Location field.

4. From the calendar, click the date for the virtual machine image you want to recover. From the Time Range list, click the backup image to recover. The content that corresponds with your selection is displayed for your reference. You cannot select individual volumes, folders, or files. The entire virtual machine is restored.

5. Click Next. On the Restore Options dialog, specify a destination.
   - Restore to Original Location--Restores the virtual machine to the vCenter/ESX server where the backup image was captured.
   - Restore to Alternate Location--Restores the virtual machine to a new location.
6. Specify the conflict resolution and post recovery options. By default, these options are not selected.
   - Overwrite existing Virtual Machine--Replaces any existing virtual machine images on the vCenter/ESX server.
   - Power on Virtual Machine--Starts the virtual machine after the restore process finishes.
7. Click Next. Enter vCenter/ESX Server credentials for the backup source, if prompted and click OK.
8. On the Restore Summary dialog, verify that all options are correct. If not, click Previous to go back. If yes, click Finish to launch the recovery process.

Restore Considerations

Use the following table to help you determine what restore method to use under the listed conditions.

Restore Method:	When you want to:	Considerations:
Browse Recovery Points (Use this method for performing application level restores.) Find Files/Folders to Restore	Restore a file, folder, database, or application that is now corrupt.	■ **CA ARCserve Central Host-Based VM Backup**: To restore files or folders, the VM must be powered on at time of backup. Restore to original location is not possible. Map a network drive to the original location or access it as a share, restore to the mapped or shared location. Install CA ARCserve D2D in the Guest OS of a new VM and restore an application database. For more information, see the topic, Perform Application Level Restores. ■ **CA ARCserve D2D or CA ARCserve Central Protection Manager**: See the application User Guide.
Recover VM	Provision a new VM, restore the OS, applications, and data	■ **CA ARCserve Central Host-Based VM Backup**: Recommended ■ **CA ARCserve D2D or CA ARCserve Central Protection Manager**: Not Supported

Recovery is also possible using the BMR and Application Level Restore processes. For more information, see the topic, Restore Methods (see page 87).

Application Level Restores

CA ARCserve Central Applications let you protect and recover data, but also help you get applications that use that data back up and running. Application Level Restores use the Browse Recovery Points restore method. During the application level restore process, you can recover Microsoft Exchange or SQL Servers without having to perform a full disaster recovery.

Before you begin the application level restore process, you may need to perform the following tasks:

- Provision a new virtual machine with a Windows Guest OS
- Install CA ARCserve D2D in the Guest OS.
- For Exchange Server application restore operations:
  - Verify that the account has Exchange Full Administrator role privileges for Exchange Server 2003, or Exchange Organization Administrator or Server Administrator role privileges for Exchange Server 2007/2010.
  - When you are restoring Exchange Server 2007 databases to Recovery Storage Groups, create the Recovery Storage Groups on the protected server. Similarly, when you are restoring Exchange Server 2010 databases to Recovery Databases, create the Recovery Databases on the protected server.
  - Review the complete Application Level Restore procedure provided in the CA ARCserve D2D User Guide and excerpted in CA ARCserve D2D Procedures (see page 173).

Restore Exchange Server Data

You can perform application level restores of Microsoft Exchange Server data with the following:

- Exchange Server 2003: Single Server Environment. Cluster Environment is not supported.
- Exchange Server 2007: Single Server Environment, Local Continuous Replication (LCR), and Cluster Continuous Replication (CCR) environment. For Exchange Server 2007 CCR, install CA ARCserve D2D locally on both the active and passive nodes. You can perform backup operations from either the active or passive node, but you can perform restore operations only on the active node. Single Copy Cluster (SCC) is not supported.
- Exchange Server 2010: Single Server Environment and Database Availability Group (DAG) environment. For a DAG environment, verify CA ARCserve D2D is installed on all servers in the DAG. You can perform backup operations from any server for both active and passive database copies, but restore operations can only be performed to an active database copy.

You can restore Microsoft Exchange Server data to the following levels:

- Microsoft Exchange Writer Level: Restores all Exchange Server data.
- Storage Group Level: Restores a specific Storage Group (does not apply to Microsoft Exchange Server 2010).
- Mailbox Store Level: Restores a specific mailbox store (applies only to Microsoft Exchange Server 2003).
- Mailbox Database Level: Restores a specific mailbox database (applies to Exchange Server 2007 and 2010).

Note: Before you begin, perform the necessary prerequisites in Application Level Restores (see page 97).

Important! Microsoft Exchange Server granular restore is not supported from CA ARCserve Central Host-Based VM Backup backup sessions. To restore Microsoft Exchange Server data at a granular level, back up the Exchange Server data using CA ARCserve Central Protection Manager or CA ARCserve D2D.

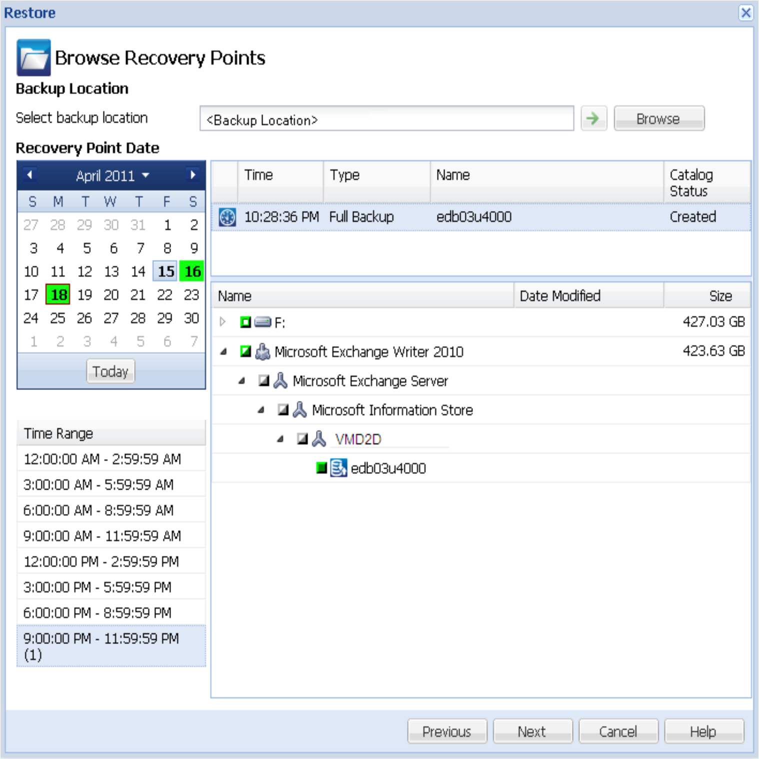
To restore Exchange Server data

1. Verify that CA ARCserve D2D is installed on the guest operating system.
2. Log in to the guest operating system on the virtual machine where you want to restore Exchange Server data.
3. Start CA ARCserve D2D and then click Restore on the CA ARCserve D2D Navigation panel to open the Restore dialog.
4. Click Browse Recovery Points to open the Browse Recovery Points dialog.

5. In the Select backup location field on the Browse Recovery Points dialog, specify the path to the backup session on the Host-Based VM Backup virtual machine that you want to restore Exchange Server data from. The following path is an example of the path to the backup session on the Host-Based VM Backup virtual machine:

   https://<server name>/<share name>/vm@<host name or IP address of the ESX Server system>

6. On the calendar, click a recovery point date and time.



Restore

Browse Recovery Points

Backup Location

Select backup location <Backup Location>

Recovery Point Date

April 2011

S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Time	Type	Name	Catalog Status
10:28:36 PM	Full Backup	edb03u4000	Created

Time Range
12:00:00 AM - 2:59:59 AM
3:00:00 AM - 5:59:59 AM
6:00:00 AM - 8:59:59 AM
9:00:00 AM - 11:59:59 AM
12:00:00 PM - 2:59:59 PM
3:00:00 PM - 5:59:59 PM
6:00:00 PM - 8:59:59 PM
9:00:00 PM - 11:59:59 PM (1)

Name	Date Modified	Size
F:		427.03 GB
Microsoft Exchange Writer 2010		423.63 GB
Microsoft Exchange Server		
Microsoft Information Store		
VMD2D		
edb03u4000		

7. Click Next to open the Restore Options dialog.

8. 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.

9. Click Next to open the Restore Summary dialog.
10. 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.

Restore SQL Server Data

You can perform application level restores of Microsoft SQL Server data with the following:

- Microsoft SQL Server 2005 Express, Standard, Workgroup, and Enterprise
- Microsoft SQL Server 2008, SQL Server 2008 R2 Express, Web, Standard, Workgroup, and Enterprise

Note: Before you begin, read the prerequisites in Application Level Restores (see page 97).

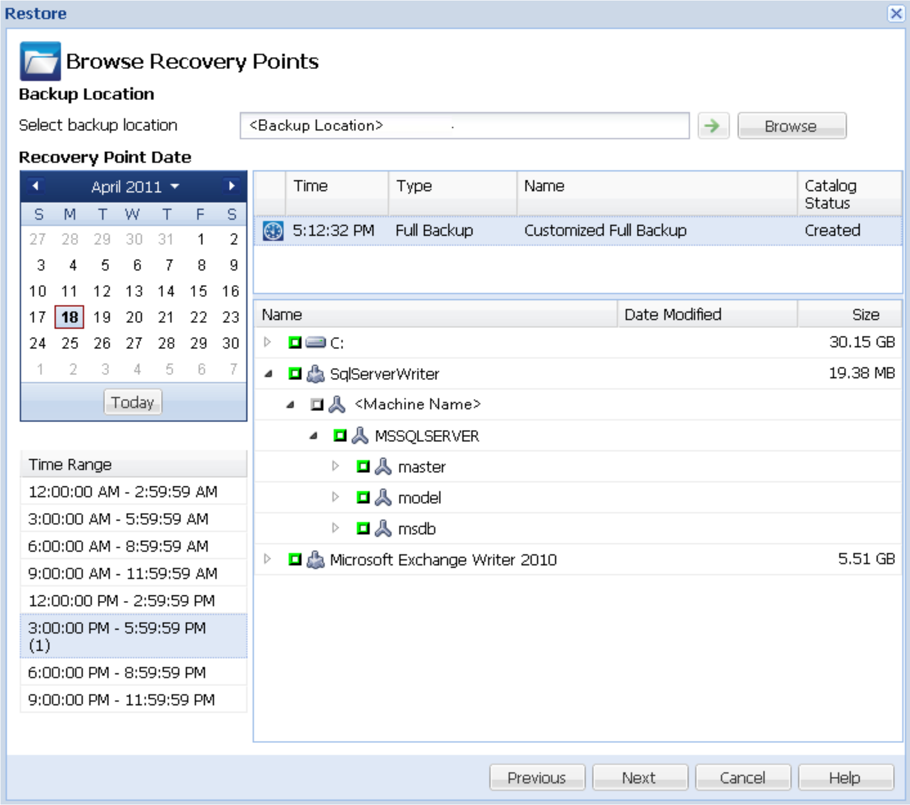
Important! Microsoft SQL Server granular restore is not supported from CA ARCserve Central Host-Based VM Backup backup sessions. To restore Microsoft SQL Server data at a granular level, back up the SQL Server data using CA ARCserve Central Protection Manager or CA ARCserve D2D.

To restore SQL Server data

1. Verify that CA ARCserve D2D is installed on the guest operating system.
2. Log in to the guest operating system for the virtual machine where you want to restore Exchange Server data.
3. Start CA ARCserve D2D and then click Restore on the CA ARCserve D2D Navigation panel to open the Restore dialog.
4. Click Browse Recovery Points to open the Browse Recovery Points dialog.
5. In the Specify backup location field on the Browse Recovery Points dialog, specify the path to the backup session on the Host-Based VM Backup virtual machine that you want to restore Exchange Server data from. The following path is an example of the path to the backup session on the Host-Based VM Backup virtual machine:

   ```
   https://<server name>/<share name>/vm@<host name or IP address of the ESX Server system>
   ```

6. Select the recovery point (date and time) and then select the Microsoft SQL Server database to be restored.



Backup Location

Select backup location <Backup Location>

Recovery Point Date

April 2011

S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Time Range
12:00:00 AM - 2:59:59 AM
3:00:00 AM - 5:59:59 AM
6:00:00 AM - 8:59:59 AM
9:00:00 AM - 11:59:59 AM
12:00:00 PM - 2:59:59 PM
3:00:00 PM - 5:59:59 PM (1)
6:00:00 PM - 8:59:59 PM
9:00:00 PM - 11:59:59 PM

Time	Type	Name	Catalog Status
5:12:32 PM	Full Backup	Customized Full Backup	Created

Name	Date Modified	Size
C:		30.15 GB
SqlServerWriter		19.38 MB
<Machine Name>		
MSSQLSERVER		
master		
model		
msdb		
Microsoft Exchange Writer 2010		5.51 GB

7. Click Next to open the Restore Options dialog.

   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.

   Restore to original location

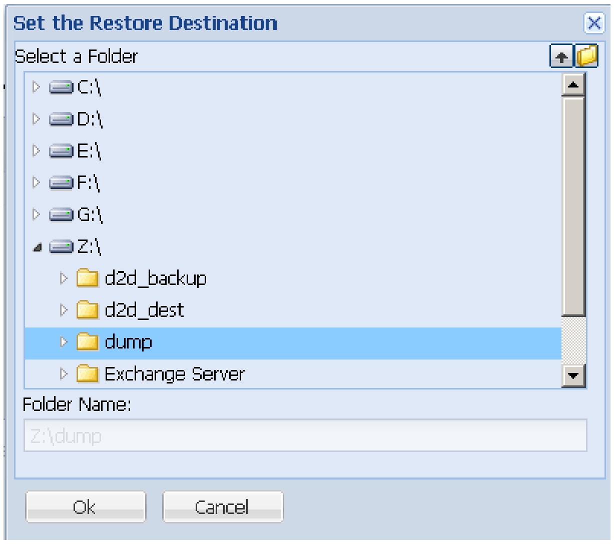
   Restores to the original location from where the backup image was captured.

   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.

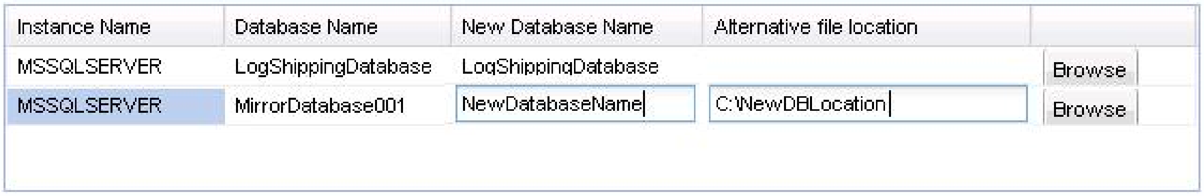
   When you select this option, you can then specify or browse to the folder location where the dump file will be restored to.



Folder Name: Z:\dump

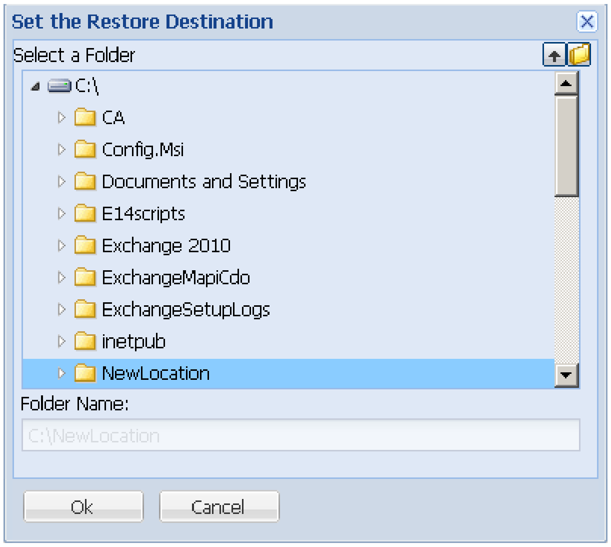
   Restore to alternate location

   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.



Folder Name: C:\NewLocation

8. Click Next to open the Restore Summary dialog.

9. 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.

Chapter 5: Troubleshooting CA ARCserve Central Host-Based VM Backup

This section provides troubleshooting information to help you identify and resolve problems that you can encounter when using CA ARCserve Central Host-Based VM Backup.

This section contains the following topics:

Cannot Connect to Specified Server Messages Appear when Attempting to Add Nodes

Valid on Windows platforms.

Symptom:

The following message appears when you to try to add or connect to nodes from the Node screen.

```
Cannot connect to specified server.
```

Solution:

If the above message appears when you try to add nodes from the Node screen, the following corrective actions can help you solve the problem:

- Verify that the Windows Server service is running on the CA ARCserve Central Host-Based VM Backup server and the source virtual machine (node).
- Verify that a Windows Firewall exception is applied to the Windows File and Printer Sharing service on the CA ARCserve Central Host-Based VM Backup server and the source virtual machine (node).
- Verify that a Windows Firewall exception is applied to the Windows Netlogon service only if the node is not a member of a domain. Perform this task on the CA ARCserve Central Host-Based VM Backup server and the source virtual machine (node).
- Verify that the value applied to the Sharing and Security model for local account is Classic. To apply the Classic value, do the following:

  Note: Perform the following steps on the CA ARCserve Central Host-Based VM Backup server and the source virtual machine (node).

  1. Log in to the CA ARCserve Central Host-Based VM Backup server and open Control Panel.
  2. From the Control Panel, open Administrative Tools.
  3. Double-click Local Security Policy.

     The Local Security Policy window opens.

4. From the Local Security Policy window, expand Local Policies and expand Security Options.

   The Security Policies appear.

5. Right-click Network access: Sharing and security model for local accounts and click Properties on the pop-up menu.

   The Network access: Sharing and security model for local accounts properties dialog opens.

6. Click Local Security Setting.

   From the drop-down list, select Classic - local users authenticate as themselves.

   Click OK.

- Verify that the value applied to the Local Policies for the LAN manager authentication level is set to send LM & NTLMv2 – use NTLMv2 session security if negotiated. To apply the value, do the following:

  1. Log in to the CA ARCserve Central Host-Based VM Backup server and open the command prompt.

     Execute the following command

     ```
     secpol.msc
     ```

     The Local Security Settings dialog opens.

  2. Select local policies and click security options.

     Search for Network security: LAN manager authentication level.

     Double-click the option.

     The Properties dialog opens

  3. Select the following option and click OK.

     ```
     send LM & NTLMv2 – use NTLMv2 session security if negotiated
     ```

  4. From the command prompt, execute the following command:

     ```
     gpupdate
     ```

  The value is applied.

Blank Webpages Appear or Javascript Errors Occur

Valid on Windows Server 2008 and Windows Server 2003 operating systems.

Symptom:

When you open CA ARCserve Central Applications websites using Internet Explorer, blank web pages appear or Javascript errors occur. The problem occurs when opening Internet Explorer on Windows Server 2008 and Windows Server 2003 operating systems.

This problem occurs under the following conditions:

- You are using Internet Explorer 8 or Internet Explorer 9 to view your application, and the browser does not recognize the URL as a trusted site.
- You are using Internet Explorer 9 to view your application, and the communication protocol in use is HTTPS.

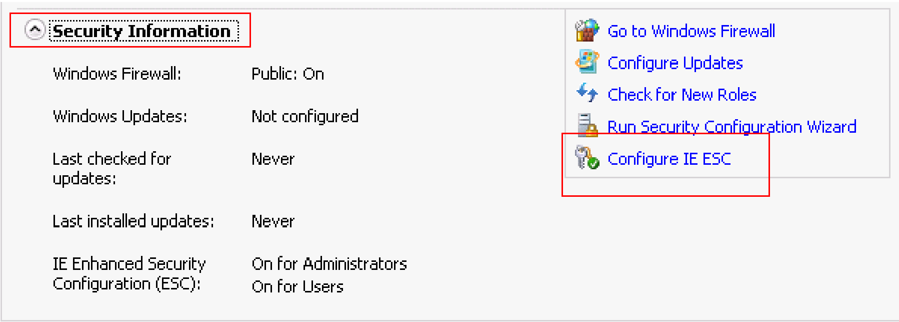
Solution:

To correct this problem, disable Internet Explorer Enhanced Security on the computers that you use to view your application.

To disable Internet Explorer Enhanced Security on Windows Server 2008 systems, do the following:

1. Log on to the Windows Server 2008 computer that you use to view reports using the Administrator account or an account that has administrative privileges.
2. Right-click Computer on the desktop and click Manage to open the Server Manager window.
3. From the Server Manager window, click Server Manager (Server Name).

   From the Server Summary section, open Security Information and click Configure IE ESC as illustrated by the following:



Security Information

Windows Firewall:	Public: On
Windows Updates:	Not configured
Last checked for updates:	Never
Last installed updates:	Never
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users

   The Internet Explorer Enhanced Security Configuration dialog opens.

4. On the Internet Explorer Enhanced Security Configuration dialog, do the following:

   - Administrators--Click Off
   - Users--Click Off.

   Click OK.

The Internet Explorer Enhanced Security Configuration dialog closes and Internet Explorer Enhanced Security is disabled.

To disable Internet Explorer Enhanced Security on Windows Server 2003 systems, do the following:

1. Log on to the Windows Server 2003 computer that you use to view reports using the Administrator account or an account that has administrative privileges.
2. Open Windows Control Panel and then open Add or Remove Programs.
3. From the Add or Remove Programs dialog, click the Add/Remove Windows Components option to access the Windows Components Wizard screen.

   Clear the checkmark next to Internet Explorer Enhanced Security Configuration.

   Click Next.

   Follow the on-screen instructions to complete the configuration and then click Finish.

Internet Explorer Enhanced Security is disabled.

Web Pages Do Not Load Properly When Logging in to CA ARCserve D2D Nodes

Valid on Windows platforms.

Symptom:

Web pages in browser windows do not load properly, display error messages, or both when logging in to CA ARCserve D2D nodes from the Nodes screen.

Solution:

This behavior affects mainly Internet Explorer browsers. Web pages may not load properly when Active scripting, ActiveX controls, or Java programs are disabled on your computer or blocked on your network.

You can correct the problem by refreshing your browser window. However, if refreshing your browser window does not correct the problem, do the following:

1. Open Internet Explorer.

   From the Tool menu, click Internet Options.

   The Internet Options dialog opens.

2. Click the Security tab.

   The Security options display.

3. Click Internet zone.

   The Internet Zone options display.

4. Click Custom Level.

   The Security Settings - Internet Zone dialog opens.

5. Scroll to the Scripting category.

   Locate Active scripting.

   Click the Enable or Prompt option.

6. Click OK on the Security Settings - Internet Zone dialog.

   The Security Settings - Internet Zone dialog closes.

7. Click OK on the Internet Options dialog.

   The Internet Options dialog closes and the Active scripting option is applied.

Note: If this solution does not correct the problem, consult your systems administrator to verify that other programs, such as antivirus or firewall programs, are not blocking Active scripting, ActiveX controls, or Java programs.

How to Troubleshoot Page Loading Problems

Valid on Windows platforms.

Symptom:

The following error messages appear in browser windows when you log in to CA ARCserve Central Applications, CA ARCserve D2D nodes, and monitoring servers.

Message 1:

Errors on this webpage might cause it to work incorrectly.

Message 2:

!

Solution:

Web pages do not load properly for many reasons. The following table describes common reasons and the corresponding corrective actions:

Reason	Corrective Action
There are problems with the underlying HTML source code.	Refresh the webpage and try again.
Your network blocks Active scripting, ActiveX, or Java programs.	Allow your browser to use Active scripting, ActiveX, or Java programs.
Your antivirus application is configured to scan temporary Internet files and downloaded programs.	Filter your antivirus application to allow Internet-related files associated with CA ARCserve Central Applications webpages.
The scripting engine installed on your computer is corrupt or outdated.	Update the scripting engine.
The video card drivers installed on your computer are corrupt or outdated.	Update the video card drivers.
The DirectX component installed on your computer is corrupt or outdated.	Update the DirectX component.

Garbage Characters Appear in Browser Windows When Accessing CA ARCserve Central Applications

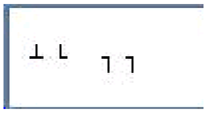
Valid on all Windows operating systems. All browsers affected.

Symptom:

When you log in to CA ARCserve Central Applications, garbage characters appear in the content area of your browser window.

Solution:

This problem occurs when you install CA ARCserve Central Applications using HTTPS communication and then try to access CA ARCserve Central Applications using HTTP communication. The underlying CA ARCserve Central Applications web services component does not support the capability to convert HTTP URLs to HTTPS URLs. As a result, garbage characters appear in your browser window. For example:



To correct this problem, access CA ARCserve Central Applications using HTTPS when you install or configure the applications to communicate using HTTPS.

Access Denied Errors Occur when Updating Nodes

Valid on all Windows operating systems that support User Account Control (UAC).

Note: Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7 support UAC.

Symptom 1:

When you provide a Windows user account that is a member of the administrators group, the following messages displays when applying the password on the Node Credentials dialog of the Import Virtual Machines from vCenter/ESX dialog:

Administrator Privileges are required.

The result is that you cannot apply the node credentials.

Symptom 2:

When you import nodes but do not provide node credentials during the import operation, the following message displays when you try to perform the Update Node operation using a Windows user account that is a member of the administrators group:

Access is denied. Verify user has administrator privilege and the remote registry access is not restricted by local security policy of the added machine.

The result is that you cannot update the node.

Solution:

You can expect this behavior when UAC is enabled on computers running a Windows operating system that supports UAC. UAC is a Windows feature that allows only the Administrator account to log in to the computer from a remote location. The solution to this behavior is to complete the following steps:

Follow these steps:

1. Log in to the computer using the Administrator account.
2. Open Windows Control Panel.
3. Open User Accounts.

4. From the Make changes to your user account screen, click Change User Account Control Settings and then do one of the following:

   - **Windows Vista and Windows Server 2008:** On the Make changes to you user account screen, click Turn User Account Control on or off. Then on the Turn on User Account Control (UAC) to make your computer more secure screen, clear the check box next to Use User Account Control (UAC) to help protect your computer, and click OK.

     Restart your computer to apply the changes to UAC.

   - **Windows Server 2008 r2 and Windows 7:** On the Choose when to be notified about changes to your computer screen, move the slider from Always notify to Never notify. Click OK, close Windows Control Panel.

     Restart your computer to apply the changes to UAC.

5. After the computer restarts, verify that the following configurations are applied to the guest operating system on the virtual machine:

   - The Windows Server service is running.
   - The File and Printer Sharing service is allowed to communicate through the Windows firewall.
   - When the node is not required to join a domain, the Netlogon Service is allowed to communicate through the Windows firewall.
   - The value of Local Security Policy, Local Policies, Security Options, Network access: Sharing and security model for local accounts is Classic.

6. Verify the following configuration is applied on the Host-Based VM Backup server:

   - The value of Local Security Policy, Local Policies, Security Options, Network security: LAN Manager authentication level is Send LM & NTLM - use NTLMv2 session security if negotiated.

Certificate Error Appears When You Log In to the Application

Valid on Windows platforms.

Symptom:

The following message appears in your browser window when you log in to the application:

- Internet Explorer:

  ```
  There is a problem with this website's security certificate.
  ```

- Firefox:

  ```
  This connection is untrusted.
  ```

- Chrome:

  ```
  This site's security certificate is not trusted!
  ```

If you specify an option that lets you continue to the website, you can log in to the application successfully. However, you encounter this behavior every time you log in to the application.

Solution:

This behavior occurs when you specify to use HTTPS as the communication protocol. To correct this problem temporarily, click the link in your browser window that lets you continue to the website. However, the next time that you log in to the application, you will encounter the message again.

HTTPS communication protocol provides a higher level of security than HTTP communication protocol. If you want to continue to communicate using HTTPS communication protocol, you can purchase a security certificate from VeriSign and then install the certificate on the application server. Optionally, you can change the communication protocol used by the application to HTTP. To change the communication protocol to HTTP, do the following:

1. Log in to the server where you installed the application.
2. Browse to the following directory:

   ```
   C:\Program Files\CA\ARCserve Central Applications\BIN
   ```

3. Execute the following batch file:

   ```
   ChangeToHttp.bat
   ```

4. After the batch file executes, open Windows Server Manager.

   Restart the following service:

   ```
   CA ARCserve Central Applications Service
   ```

Backups Fail with Snapshot Creation Errors

Valid on Windows platforms.

When you submit backups of VMware based virtual machines, the following symptoms occur:

Symptom 1

Backup jobs fail and the following message appears in the Activity Log:

```
Failed to take snapshot. ESX/vCenter report error. A general system error occurred. Protocol error from VMX.
```

Solution 1

This error is a VMware issue. To correct this problem, uninstall and then reinstall VMware Tools inside the guest operating system and then resubmit the job.

Symptom 2

Backup jobs fail and the following message appears in the Activity Log:

```
Could not take snapshot of the virtual machine. ESX Server/vCenter Server reported the following error: Cannot create a quiesced snapshot because the create snapshot operation exceeded the time limit for holding off I/O in the frozen virtual machine..
```

Solution 2

This error occurs when VSS encounters errors when creating snapshots. VSS can encounter errors under the following conditions:

A VSS writer is in an unstable state.

To determine the source and correct this behavior, perform the following remedial actions:

1. Run the command "vssadmin list writers" from the command line on the guest operating system on the virtual machine.
2. Verify that all VSS writers are in a healthy state.
3. For writers that are in the following states, contact Microsoft or the vendor of the writer for information about how to fix the errors.

   ```
   state=Stable
   Last Error=No Error
   ```

   Note: Restarting writers usually solves the problem.

VSS encountered errors when creating snapshots.

To determine the source and correct this behavior, perform the following remedial actions:

1. Review the Windows event log in the guest operating system. Check for errors that are related to the VSS components about the time the backup started.
2. When VSS reports errors due to insufficient disk space, free disk space on the volume that is associated with the error.
3. When VSS or the Windows Volsnap driver generates time-out errors, the applications running inside the virtual machine are in a highly active state. The highly active state prevents VSS from creating consistent snapshots. To remedy this condition, schedule backups at times when the applications perform fewer input and output operations to the volume.
4. When the Windows Event Log indicates that the VolSnap driver encountered errors, see the article Volume Snapshot Driver Integrity at the Microsoft Technet Library for information about how to correct VolSnap driver errors.

Recover VM Operations Fail with Unknown Errors

Valid on Windows operating systems.

Symptom:

Recover VM jobs fail. You can submit the Recover VM job, however, the following message appears in the Activity Log:

```
Failed to recover virtual disks.
```

In addition, VDDK reports the following error message:

```
Unknown Error.
```

Solution 1:

To correct this problem, consider the following solutions:

- Recover VM jobs can fail when there is not enough free disk space on the original datastore. VDDK returns the message because the VDDK API (currently) does not support the capability to detect the amount of free disk space on the original datastore. (The datastore is the location where you specified to recover the virtual machine.) To correct this problem, free the amount of disk space on the original datastore that is required to complete the operation and then resubmit the job.
- Network disturbance and high network traffic can cause Recover VM jobs to fail. To correct this problem, verify that the proxy server and the ESX Server system or the vCenter Server system can communicate with each other though the network, then resubmit the job.
- Multiple concurrent connections consisting of backup or recover VM jobs to the ESX Server system or the vCenter Server system, which includes vSphere SDK connections through the VMware vSphere Client, can cause the jobs to fail. To correct this problem, close all unnecessary connections and then resubmit the job. For information about the maximum quantity of concurrent connections that are allowed, see Cannot Open VMDK File (see page 137).
- Examine the Tasks and Events sections of the VMware vSphere Client log to discover internal errors for the specific virtual machine. Correct the internal errors and then resubmit the job.

  Example: Another application or operation is using the VMDK file. To correct this problem, release the file and resubmit the job.

Solution 2:

This problem can occur under the following conditions:

- VDDK did not process a snapshot properly.
- VDDK did not delete a snapshot manually or internal to the virtual machine.

To correct this problem, resubmit the job. If the job fails again, delete the recovered virtual machine and resubmit the job.

Backup and Recovery Operations Using the hotadd Transport Mode Cannot Mount Disks

Valid on Windows platforms.

Symptom:

Backup and recovery jobs that use the hotadd transport mode cannot mount disks to the proxy system.

Solution:

To correct this problem, do the following:

1. Open VMware vSphere Client.

   Log in to the ESX Server system or the vCenter Server system using administrative credentials.

2. Select the proxy virtual machine and edit the settings for the proxy virtual machine.
3. Remove the hotadd disks that are attached to the source virtual machine or the proxy virtual machine.
4. Resubmit the job.

Recovery Operations Fail When Recovering Data Using the HOTADD or SAN Transport Mode

Valid on Windows platforms.

Symptom:

Recovery operations fail when recovering data using the HOTADD or SAN transport mode. The following message appears in the Activity Log:

An unknown error has occurred. Contact Technical Support.

Solution:

Recovery operations fail using the HOTADD transport mode (see page 237) or SAN transport mode (see page 238) when the disk settings are not configured properly.

To configure the disk, perform the following steps:

1. Log in to the backup proxy system using an account with administrative privileges.
2. Open Windows Command Line.

3. From the command line, type the following command:

   ```
   diskpart
   ```

   Press Enter.

4. Type SAN and then press Enter.

   The current SAN policy displays.

5. Type the following command:

   ```
   SAN POLICY = OnlineAll
   ```

   Press Enter.

   The SAN policy is configured as do not automatically mount SAN hosted volumes.

6. To clear the read-only attribute of the specific SAN disk, select the disk from the disk list and type the following command:

   ```
   attribute disk clear readonly
   ```

   Press Enter

7. Type exit and then press Enter.

The disk is configured and you can resubmit the job.

If the job fails again, mount the HOTADD disks manually using disk management on the proxy system.

To mount the disks manually, perform the following steps:

1. Log in to the backup proxy system using an account with administrative privileges.
2. Open Windows Control Panel and double-click Administrative Tools.

   The Administrative Tools window opens.

3. From the Favorites list, double-click Computer Management.

   The Computer Management opens.

4. Expand Storage and click Disk Management.

   The disks display.

5. Right-click the disk that you want to mount and click Online.

The disk is mounted and you can resubmit the job.

Operating System Not Found Errors Occur

Valid on Windows platforms.

Symptom 1

The following message appears when you try to start the guest operating system on a virtual machine after you recovered the virtual machine using the Restore to Alternate Location option:

```
Operating System Not Found.
```

Solution 1

The above behavior can occur on virtual machines that contain SCSI and IDE devices. If this problem occurs, examine how disks are configured on your virtual machine and verify that the boot sequence of the recovered virtual machine is the same as the source virtual machine. If the boot sequence is different, you must update the BIOS on the recovered virtual machine to match that of the source.

Note: The first IDE disk should use (0:1).

Symptom 2

The following message appears when you try to start the guest operating system on a virtual machine after you recovered virtual machine:

```
Operating System Not Found.
```

Solution 2

If the above problem occurs, examine how disks are configured on the virtual machine and verify that the boot sequence on the Replica virtual machine is the same as the source virtual machine.

MAC Address Changes are Not Retained After VM Recovery

Valid on Windows platforms.

Symptom:

The MAC addresses of virtual machines are not retained after recovering virtual machines.

Solution:

MAC addresses are not retained during recovery, to prevent duplicates. To retain MAC address information, set the following registry key on the proxy server:

```
Location: SOFTWARE\CA\CA ARCSERVE D2D
Key Name: RetainMACForVDDK
Value Type: String
Key Value: 1
```

On virtual machines with two NIC cards, set the RetainMACForVDDK registry key if you wish to set one as Manual. Otherwise, all cards are set to Automatic after recovery.

CA ARCserve D2D Web Service Fails on CA ARCserve D2D Nodes

Valid on Windows platforms.

Symptom:

The web service running on CA ARCserve D2D nodes starts and fails or cannot start.

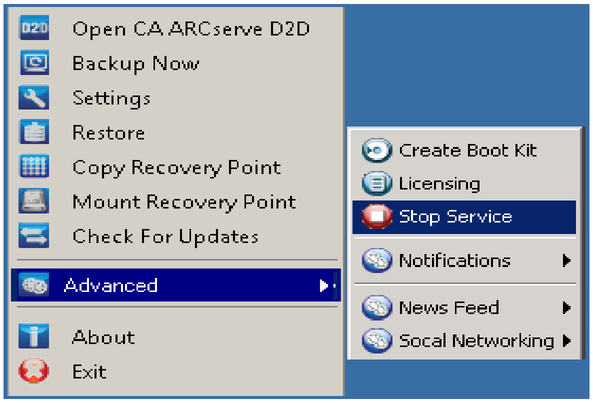
Solution:

This problem occurs when the port used by the CA ARCserve D2D web service is the same as the port used by the VMware vCenter web service (Tomcat).

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.

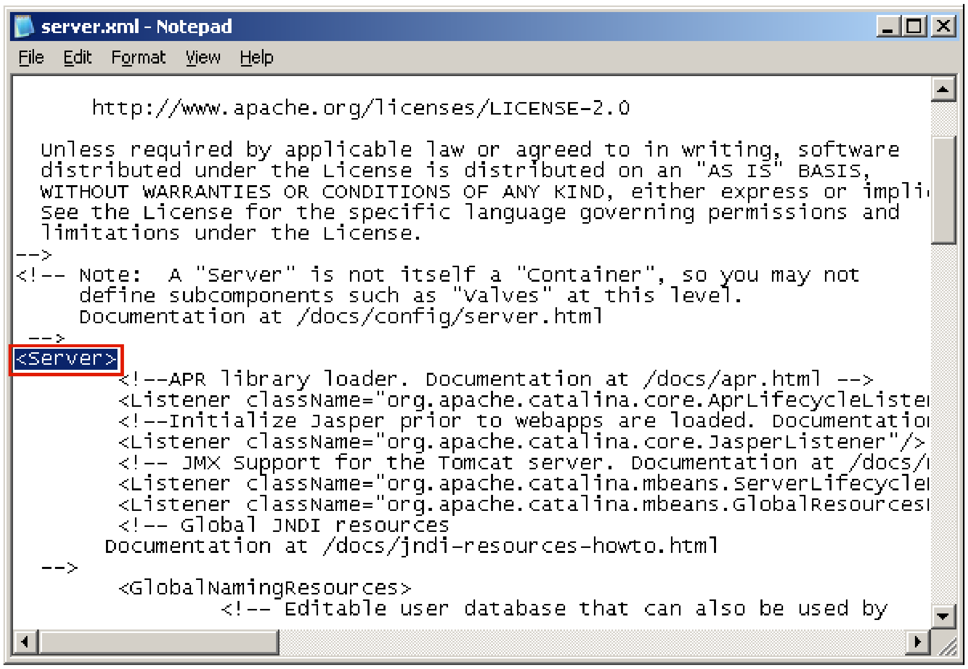
   

2. Access the Tomcat server.xml file to edit/configure the behavior of Tomcat.

   The Tomcat server.xml file is located in the following folder structure:

   C:\Program Files\CA\ARCserve Central Applications\TOMCAT\conf

3. Locate the <Server> tag inside the server.xml file.



```
      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or impli
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<!-- Note:  A "Server" is not itself a "Container", so you may not
     define subcomponents such as "Valves" at this level.
     Documentation at /docs/config/server.html
 -->
<Server>
        <!--APR library loader. Documentation at /docs/apr.html -->
        <Listener className="org.apache.catalina.core.AprLifecycleListe
        <!--Initialize Jasper prior to webapps are loaded. Documentatio
        <Listener className="org.apache.catalina.core.JasperListener"/>
        <!-- JMX Support for the Tomcat server. Documentation at /docs/
        <Listener className="org.apache.catalina.mbeans.ServerLifecycle
        <Listener className="org.apache.catalina.mbeans.GlobalResources
        <!-- Global JNDI resources
       Documentation at /docs/jndi-resources-howto.html
  -->
        <GlobalNamingResources>
                <!-- Editable user database that can also be used by
```

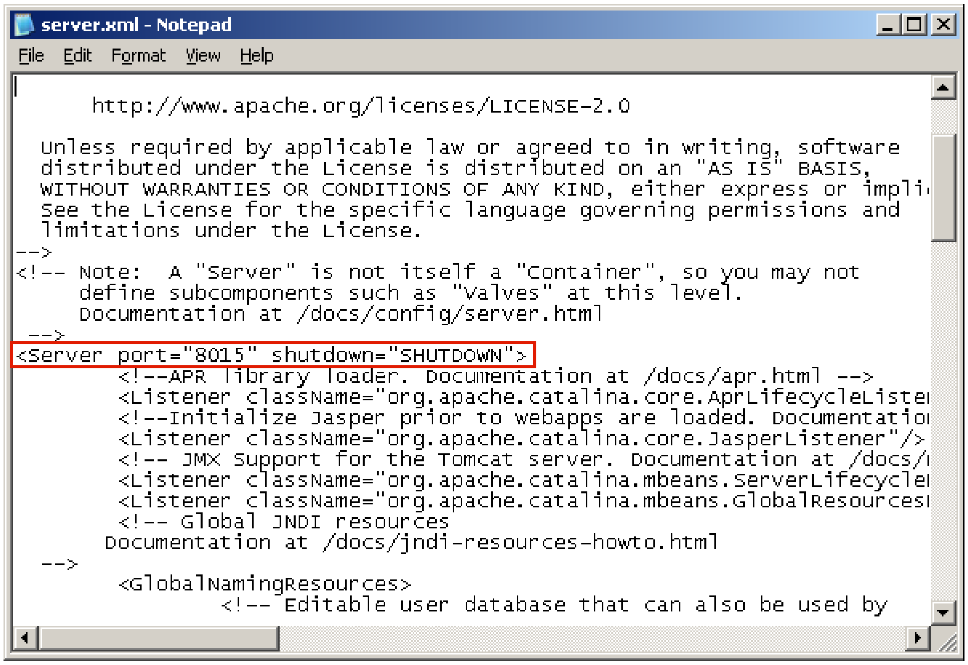
4. Edit the <Server> tag as follows:

   From:

   <Server>

   To:

   <Server port="8015" shutdown="SHUTDOWN">



```
      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or impli
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<!-- Note:  A "Server" is not itself a "Container", so you may not
     define subcomponents such as "Valves" at this level.
     Documentation at /docs/config/server.html
 -->
<Server port="8015" shutdown="SHUTDOWN">
        <!--APR library loader. Documentation at /docs/apr.html -->
        <Listener className="org.apache.catalina.core.AprLifecycleListe
        <!--Initialize Jasper prior to webapps are loaded. Documentatio
        <Listener className="org.apache.catalina.core.JasperListener"/>
        <!-- JMX Support for the Tomcat server. Documentation at /docs/
        <Listener className="org.apache.catalina.mbeans.ServerLifecycle
        <Listener className="org.apache.catalina.mbeans.GlobalResources
        <!-- Global JNDI resources
       Documentation at /docs/jndi-resources-howto.html
  -->
        <GlobalNamingResources>
                <!-- Editable user database that can also be used by
```

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.

CA ARCserve Central Host-Based VM Backup Cannot Communicate with the CA ARCserve D2D Web Service on Remote Nodes

Valid on Windows operating systems.

Symptom:

CA ARCserve Central Host-Based VM Backup cannot communicate with the CA ARCserve D2D web service on remote nodes.

Solution:

The following table describes reasons why CA ARCserve Central Host-Based VM Backup cannot communicate with the CA ARCserve D2D web service on remote nodes and the corresponding corrective action:

Cause	Corrective Action
The network was not available or not stable when applying policies.	Verify that the network is available and stable and then try again.
The CA ARCserve D2D computer could not handle the load when the application tried to communicate with the node.	Verify that the CPU on the remote CA ARCserve D2D node is in a normal state and then try again.
The CA ARCserve D2D service on the remote node was not running when applying policies.	Verify that the CA ARCserve D2D on the remote node is running and then try again.
The CA ARCserve D2D service was not communicating properly.	Restart the CA ARCserve D2D service on the remote node and then try again.

The CA ARCserve D2D Web Service Runs Slowly

Valid on Windows operating systems.

Symptom 1:

The CA ARCserve D2D web service on CA ARCserve D2D systems runs slowly. You can detect other symptoms such as:

- The CA ARCserve D2D web service stops responding or occupies 100 percent of the CPU resources.
- CA ARCserve D2D nodes perform poorly or cannot communicate with the web service.

Solution 1:

In various environmental configurations, you can discover that the CA ARCserve D2D web service occupies too much CPU time, or the response is slow. By default, Tomcat is configured to allocate a limited amount of memory to the nodes, which may not be suitable for your environment. To verify this problem, review the following log files:

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log
```

Search for the following message:

```
java.lang.OutOfMemoryError
```

To correct this problem, increase the amount of allocated memory.

To increase the memory, do the following:

1. Open Registry Editor and access the following key:
   - x86 Operating Systems:

     HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java
   - x64 Operating Systems:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

2. Do one of the following:

   - If the message in the log file is the following:

     ```
     java.lang.OutOfMemoryError: PermGen space
     ```

     Append the following to the value of Options.

     ```
     -XX:PermSize=128M -XX:MaxPermSize=128M
     ```

     Note: You may need to increase the value of -XX:MaxPermSize to suit your environment.

   - If the message in the log file is one of the following:

     ```
     java.lang.OutOfMemoryError: Java heap space
     java.lang.OutOfMemoryError: GC overhead limit exceeded
     ```

     Increase the value of the following DWORD:

     ```
     JvmMx
     ```

3. Restart the CA ARCserve D2D web service.

Symptom 2

Scheduled backups are skipped and stop running.

Solution 2

When you configure the MAX value as 20 or less than 20 for concurrent backups, do the following:

1. Increase the value of the following DWORD:

   ```
   JvmMx=256
   ```

   Note: This DWORD is referenced in Solution 1.

2. Append the following to the value of Options.

   ```
   -XX:MaxPermSize=128M
   ```

   Note: This DWORD is referenced in Solution 1.

When you configure the MAX value as more than 20 but less than 50 for concurrent backups, do the following:

1. Increase the value of the following DWORD:

   ```
   JvmMx=512
   ```

   Note: This DWORD is referenced in Solution 1.

2. Append the following to the value of Options.

   ```
   -XX:MaxPermSize=256M
   ```

   Note: This DWORD is referenced in Solution 1.

Changed Block Tracking Failures

Valid on Windows.

Symptom:

Virtual machine backups fail and changed block tracking is enabled on the virtual machines.

Solution:

The following table describes environmental conditions that can cause virtual machine backups with changed block tracking enabled to fail:

Condition	Solution
User generated snapshots are present on the virtual machines, and changed block tracking is disabled.	Enable or reset changed block tracking to allow the full backup job to continue. **Note**: The full backup job continues with used and unused blocks of data from the VMDK files.
The incorrect version of VMware hardware is installed on the virtual machine.	Verify that VMware hardware version 7.0 or later is installed on the virtual machine.
The incorrect version of ESX Server is installed on the virtual machine.	Verify that ESX Server version 4.0 or later is installed on the virtual machine.
The ESX Server system encountered a hard shutdown. Hard shut downs can cause changed block tracking backups to fail.	CA ARCserve Central Host-Based VM Backup automatically enables changed block tracking on the virtual machine.
The ESX Server system encountered a (clean) reboot while the virtual machine was in powered on state.	CA ARCserve Central Host-Based VM Backup automatically enables changed block tracking on the virtual machine.
The virtual machine was moved using Storage vMotion.	CA ARCserve Central Host-Based VM Backup automatically enables changed block tracking on the virtual machine.

Backups Fail Due to ESXi License

Valid on Windows platforms.

Symptom:

CA ARCserve D2D full, incremental, and verify backup jobs fail. The following message appears in the CA ARCserve D2D Activity Log:

```
VM server <server_name> does not have a paid ESX license
```

Solution:

Due to a VMware limitation, virtual machines running on ESXi servers with a free license cannot be backed up. To protect these VMs, apply a purchased license.

Backup Fails Because VM Has Snapshots

Valid on Windows platforms.

Symptom:

CA ARCserve D2D full, incremental, and verify backup jobs fail. The following message appears in the CA ARCserve D2D Activity Log:

```
The application cannot enable changed block tracking on the virtual machine because there are snapshots on the virtual machine. To correct this problem, delete the snapshots and then resubmit the backup.
```

Solution:

If you disabled the Changed Block Tracking (CBT) feature and manually created a snapshot perhaps to test a condition directly from vCenter Server, the next scheduled backup job fails because the application does not recognize manually created snapshots due to a disabled Changed Block Tracking (CBT) feature. Delete the snapshot and resubmit the backup job. CA ARCserve Central Host-Based VM Backup automatically enables CBT. If you create manual snapshots with CBT enabled, backups will not fail.

Note: You can manually enable the CBT feature from the vSphere Client.

Backups Fail and Event 1530 is Logged in the Event Log on the Backup Proxy System

Valid on Windows Platforms.

Symptom:

CA ARCserve Central Host-Based VM Backup jobs fail. Event 1530 is logged in the Application Event log on the backup proxy system.

Environment/Steps to Reproduce:

- Microsoft SQL Server or Microsoft Exchange Server is installed on the virtual machine.
- The user logs in to or is already logged in to the CA ARCserve Central Host-Based VM Backup proxy server using the Administrator account or an account that is a member of the Administrators group.
- After the backup job starts, the user logs out of the proxy server.
- The backup job fails. Event 1530 is logged in the Application Event log.

  Warning ... Microsoft-Windows-User Profiles Service 1530 None Windows detected your registry file is still in use by other applications or services. The file will be unloaded now. The applications or services that hold your registry file may not function properly afterwards.

Cause:

Windows Server 2008 contains a User Profile Service that unloads user profiles when users log out of the computer. As a result, COM objects may not be created, which prevents Host-Based VM Backup from calling its COM modules.

Solution:

To prevent backup jobs from failing, complete the following steps:

Note: For this solution to work, all the symptoms listed above must be present.

1. Log in to the Host-Based VM Backup proxy server using the Administrator account or an account that is a member of the Administrators group.
2. Start the Local Group Policy Editor by typing gpedit.msc in the Run dialog.
3. From the Local Group Policy Editor, expand Computer Configuration, Administrative Templates, System, and User Profiles.
4. From the User Profile directory, double-click **Do not forcefully unload the user registry at user logoff** to open the **Do not forcefully unload the user registry at user logoff** dialog.
5. From the **Do not forcefully unload the user registry at user logoff** dialog, click Enabled and then click OK.

   Note: The value DisableForceUnload is now added to the Registry.
6. Restart the Host-Based VM Backup server.

Backups Complete Using the NBD Transport Mode When the hotadd Transport Mode was Specified

Valid on Windows platforms.

Symptom:

Virtual machine backups complete using the NBD transport (see page 237) mode when the hotadd transport mode (see page 237) was specified for the backup.

Solution:

CA ARCserve Central Host-Based VM Backup lets you back up virtual machines that reside on ESX Server systems. When you back up virtual machines using the hotadd transport mode, you can connect maximum 15 virtual disks to each SCSI controller on the CA ARCserve D2D virtual machine proxy server. When you submit a backup that includes more than 15 virtual disks and there is only one SCSI controller on the CA ARCserve D2D virtual machine proxy server, the single SCSI controller cannot accommodate all of the virtual machines. As a result, CA ARCserve Central Host-Based VM Backup backs up the data of the NBD transport mode.

To prevent this behavior from occurring, verify that there are a sufficient quantity of SCSI controllers on the CA ARCserve D2D virtual machine proxy server that can accommodate all the virtual machines in the backup job.

Incremental Backup Jobs Process as Verify Backup Jobs

Valid on Windows.

Symptom:

When you submit or schedule incremental backup jobs that process using the Hotadd transport mode, the following behavior occurs:

- The incremental jobs convert to verify backup jobs. The Activity Log entry for the job indicates that the incremental backup job was converted to a verify backup job.
- The Snapshot Manager in the VI Client for the virtual machine that was backed up contains a consolidated helper snapshot.
- The Edit Settings dialog in the VI Client for the affected virtual machine indicates that there are erroneous disks attached to the backup proxy system. The VMDK URLs associated with the erroneous disks are not the same as the VMDK URLs that are associated with the backup proxy system.

Solution:

To correct this behavior, remove the erroneous VMDK files (disks) from the backup proxy system using the guidelines described in VMware Knowledge Base article 1003302. In addition, VMware recommends that the amount of free space on the datastore be twice the cumulative size of the virtual machine's files.

Backup Jobs Fail Because the Blocks Cannot Be Identified

Valid on Windows.

Symptom:

For a particular virtual machine, all backup jobs fail and the following message appears in the Activity Log:

```
The application was unable to identify the blocks that were used or changed on the virtual machine. This problem can occur when the ESX Server system restarts while the virtual machine is running. The next time a backup job runs, the application will reset changed block tracking and perform a verify backup operation.
```

Solution:

To correct this behavior, perform a disk consolidation operation on the virtual machine. To perform disk consolidation, follow these steps.

1. Open the VMware VI Client.
2. Expand the ESX Server system for the affected virtual machine.
3. Right-click the affected virtual machine, select Snapshot and then click Consolidate on the pop-up menu to consolidate the disks.
4. Resubmit the backup.

Cannot Open VMDK File

Valid on Windows platforms.

Symptom:

Multiple concurrent backup jobs fail in NBD (or LAN) transport mode. The following message appears in the Activity Log:

```
Cannot open VMDK File
```

Solution:

This is a VMware connection limitation. The following Network File Copy (NFC) protocol limits apply:

- ESX 4: 9 direct connections, maximum
- ESX 4 through vCenter Server: 27 connections, maximum
- ESXi 4: 11 direct connections, maximum
- ESXi 4 through vCenter Server: 23 connections, maximum

Connections cannot be shared across disks. The maximum limits do not apply to SAN or hotadd connections. If the NFC client fails to shut down properly, connections can remain open for ten minutes.

Nodes Do Not Appear on the Node Screen After Changing the Name of the Node

Valid on Windows platforms.

Symptom:

The host name of the node was changed after it was added to the Node screen. The node no longer appears on the Node screen.

Solution:

This behavior is expected. CA ARCserve Central Host-Based VM Backup retains the name of the node as it was added from the node screen. When you rename the node, the application cannot detect the node. As such, the node does not appear on the node screen.

To display renamed nodes on the node screen, do the following:

1. Rename the node.
2. Open the Node screen and delete the node (see page 48) that was renamed.
3. Add the node using its new name.

Multiple Connections Error Occurs When Saving or Assigning a Policy to a CA ARCserve D2D Server

Valid on all Windows platforms.

Symptom:

When you try to save or assign a policy to a CA ARCserve D2D server, the following error message appears:

```
Validate backup destination failed. Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.
```

Solution:

If the preceding message appears when you try to save or assign a policy to a CA ARCserve D2D server, the following corrective actions can help you solve the problem:

- Specify the User Name field with "machine (or domain) name\username".
- Go to the remote server where the shared folder is hosted and delete all sessions from the CA ARCserve Central Applications Server or CA ARCserve D2D Server. Do one of the following to delete the sessions:
  - Run the following command line:

    ```
    net session \\machinename /delete
    ```

  - Go to the following directory to disconnect the session:

    Compmgmt.msc > System Tools > Shared Folders > Sessions > Disconnect session
- Confirm that you are using the same user name to access the remote shared folder.
- Save and deploy the policy again.

Virtual Machine Backups Fail Because the ESX Server is Not Accessible

Valid on Windows platforms.

Symptom:

Virtual machine backups fail. The following message appears in the Activity Log:

```
Failed to create virtual machine snapshot.
```

Solution:

Virtual machine backups can fail when multiple backups run concurrently on one ESX Server system. The problem does not occur when multiple backups run concurrently on multiple ESX Server systems. To back up the virtual machines, CA ARCserve Central Host-Based VM Backup takes a snapshot of the data that resides on the virtual machines. When multiple snapshot operations run concurrently on one system, the ESX Server system can stop responding. Although the time in which the ESX Server system stops responding is temporary, the backup operation is interrupted, which causes the backup operation to fail.

To prevent backups from failing, use the solution that suits your environment:

- Reduce the quantity of virtual machines that you are backing up concurrently. For example, if you are backing up eight virtual machines concurrently, reduce the quantity to seven virtual machines, resubmit the backup, and then analyze the results. If necessary, reduce the quantity of virtual machines that are backed up until backups do not fail or the above message does not appear in the Activity Log.

  To reduce the quantity of virtual machines in a backup, you unassign virtual machines from the policy. For more information, see Unassign Policies from Virtual Machines.

- Define a limit to the quantity of concurrent backups. This approach helps you control the quantity of backup jobs that can run concurrently in your environment. For more information, see Define a Limit to the Quantity of Concurrent Backups (see page 165).

Add New Tab Link Not Launching Properly for Internet Explorer 8, 9, and Chrome

Valid on Windows

Symptom:

When I add a new tab link to the Navigation bar specifying an HTTPS URL, the following error messages appear when I click the new tab:

- Internet Explorer 8 and 9:

  Content was blocked because it was not signed by a valid security certificate.

- Chrome:

  The webpage is not available.

Solution:

To correct this problem for Internet Explorer, do the following:

- Internet Explorer 8:

  Click on the message bar and select "Display Blocked Content".

- Internet Explorer 9:

  Click the "Show content" button from the message bar at the bottom of the page. The page refreshes and the added tab link opens successfully.

To correct this problem for Chrome, perform the following steps:

Step 1 - Export Certificate:

1. Open a new tab in Chrome and enter the HTTPS URL.

   A warning message appears, "The site's security certificate is not trusted!"

2. From the address bar, click the lock with the 'X'.

   A pop-up window opens with a Certification Information link.

3. Click the Certificate Information link.

   The Certificate dialog opens.

4. Click the Details tab and then click Copy to File, to save the certificate to your local computer.

   The Certificate Export Wizard dialog opens.

5. Click Next to select the format you want to use to export the file.

   Note: DER encoded binary X.509 (.CER) is selected by default.

6. Click Next to browse to a location where you want to save the certificate.
7. Click Next to complete the Certificate Export Wizard and then click Finish.

The certificate exports successfully.

Step 2 - Import Certificate:

1. Open the Tools Options from Chrome.

   The Options screen opens.

2. Select the Under the Hood option and click Manage Certificates from HTTPS/SSL.

   The Certificates dialog opens.

3. Click Import.

   The Certificate Import Wizard dialog opens.

4. Click Next to browse for the certificate you saved on your local computer.

5. Click Next to open the Certificate Store.

   The Certificate Store dialog opens.

6. Click Browse to open the Select Certificate Store dialog.

   The Select Certificate Store dialog opens.

7. Select Trusted Root Certification Authorities from the file list and click OK.

   The Certificate Store dialog appears.

8. Click Next to complete the Certificate Import Wizard and then click Finish.

   A Security Warning dialog opens stating that you are about to install a certificate.

   Click Yes to agree on the terms.

The certificate imports successfully.

Add New Tab Link, RSS Feeds, and Social Networking Feedback Not Launching Properly on Internet Explorer 8 and 9

Valid on Windows

Symptom:

For an HTTPS CA ARCserve Central Applications URL:

When I add a new tab link to the Navigation bar specifying an HTTP URL, the following error message appears when I click the new tab and the Feedback link:

```
Navigation to the webpage was canceled.
```

In addition, the RSS Feeds are not displayed.

Note: The Feedback link also displays the error message even if you do not select the new added tab link.

Solution:

To correct this problem, do the following:

- Internet Explorer 8:

  After you log in, click No on the pop-up security warning message, "Do you want to view only the webpage content that was delivered securely?" By clicking No allows the delivery of unsecured content to your webpage.

- Internet Explorer 9:

  Click the "Show all content" button on the message bar displayed at the bottom of the page. The page refreshes and the added tab link opens successfully.

Cannot Specify an Asterisk or Underscore as a Wildcard in Filter Fields Using Japanese Keyboards

Valid on Windows

Symptom:

Because of the different keycodes between the US and Japanese keyboards, the Japanese keyboard does not allow you to enter the wildcard character "*" and other special characters, such as the underscore character "_", into the following filter fields:

- Occurs only on Firefox:
  - Node > Add Group - Node Name Filter field
  - Policies > Policy Assignment tab > Assign and Unassign Policy - Node Name Filter field
  - Restore > Node Explorer - Node Name field
  - Node > Add Node from Auto Discovery result > Nodes to Protect - Node Name field

Solution:

To prevent this from occurring, open a text editing application such as Notepad. Type the special characters, such as "*" and "_", in the text editor. Then copy the characters from the text editor into the the field.

Recovering a Virtual Machine Uses a Different Transport Mode Than Specified

Valid on Windows platforms.

Symptom:

Virtual machine recovery uses a different transport mode than what is specified in the registry key.

Solution:

This behavior affects thin disks. To correct this problem, follow these steps:

1. Log in to the CA ARCserve Central Host-Based VM Backup virtual machine.
2. Open the registry editor and locate the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D\AFRestoreDll
3. Set the registry key "EnforceTransportForRecovery" to one of the following transport modes:
   - NBD
   - NBDSSL
4. Submit the recovery for the virtual machine.

Chapter 6: Applying Best Practices

This section contains the following topics:

Perform Bare Metal Recovery of a Virtual Machine

Bare Metal Recovery is supported when a virtual machine is powered on at the time the backup job is performed.

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.

Videos

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:

- One of the following things:
  - A customized Windows PE image (D2DBMR.ISO) which is released with the CA ARCserve D2D product.
  - A BMR USB stick which is created from the boot kit wizard, with the Windows 7/Windows Vista/Windows 2008/Windows 2008R2 installation media (CD/DVD). (You can also use the USB stick with the Windows PE image instead of the installation media to load the necessary drivers during BMR, if necessary).

    Note: If you are using a USB stick you can add additional drivers to it, which you cannot do with the Windows PE image.
- 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.

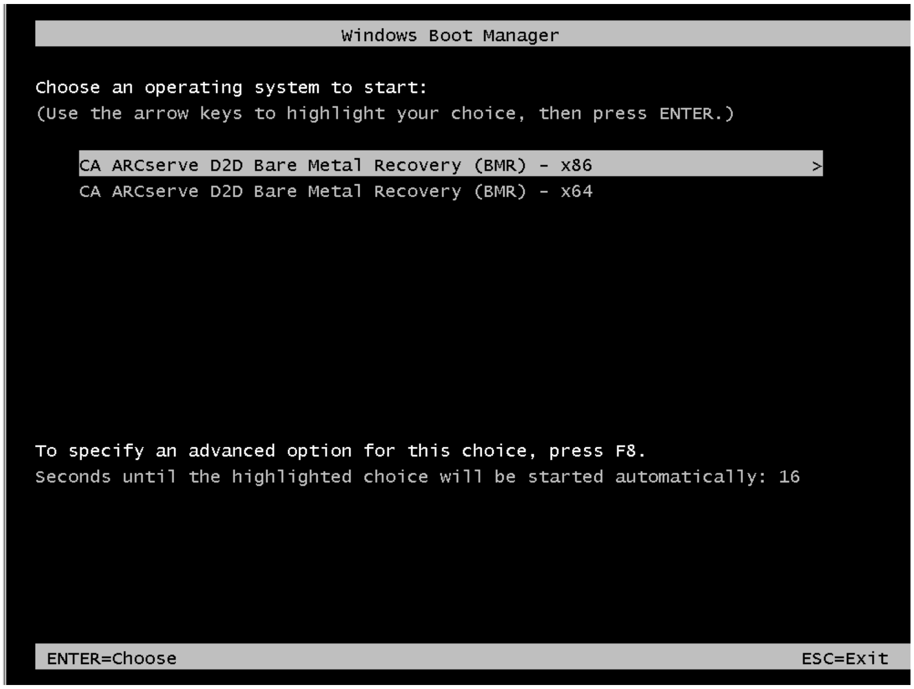
To restore data using bare metal recovery:

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.

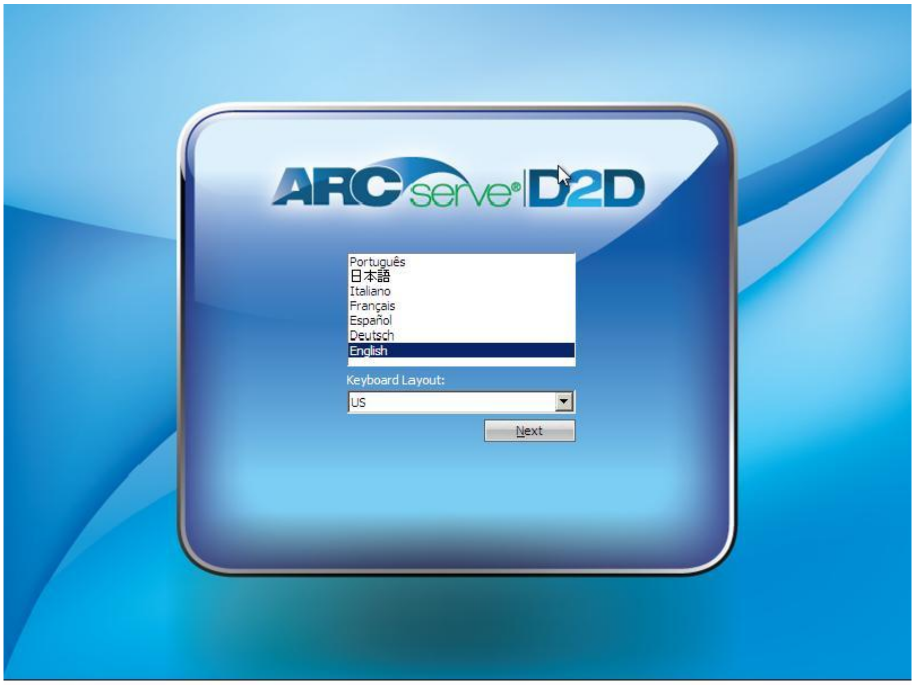
   Note: If you are using Windows PE image to perform BMR, select an architecture (x86/x64) and press Enter to continue.



```
                         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
```

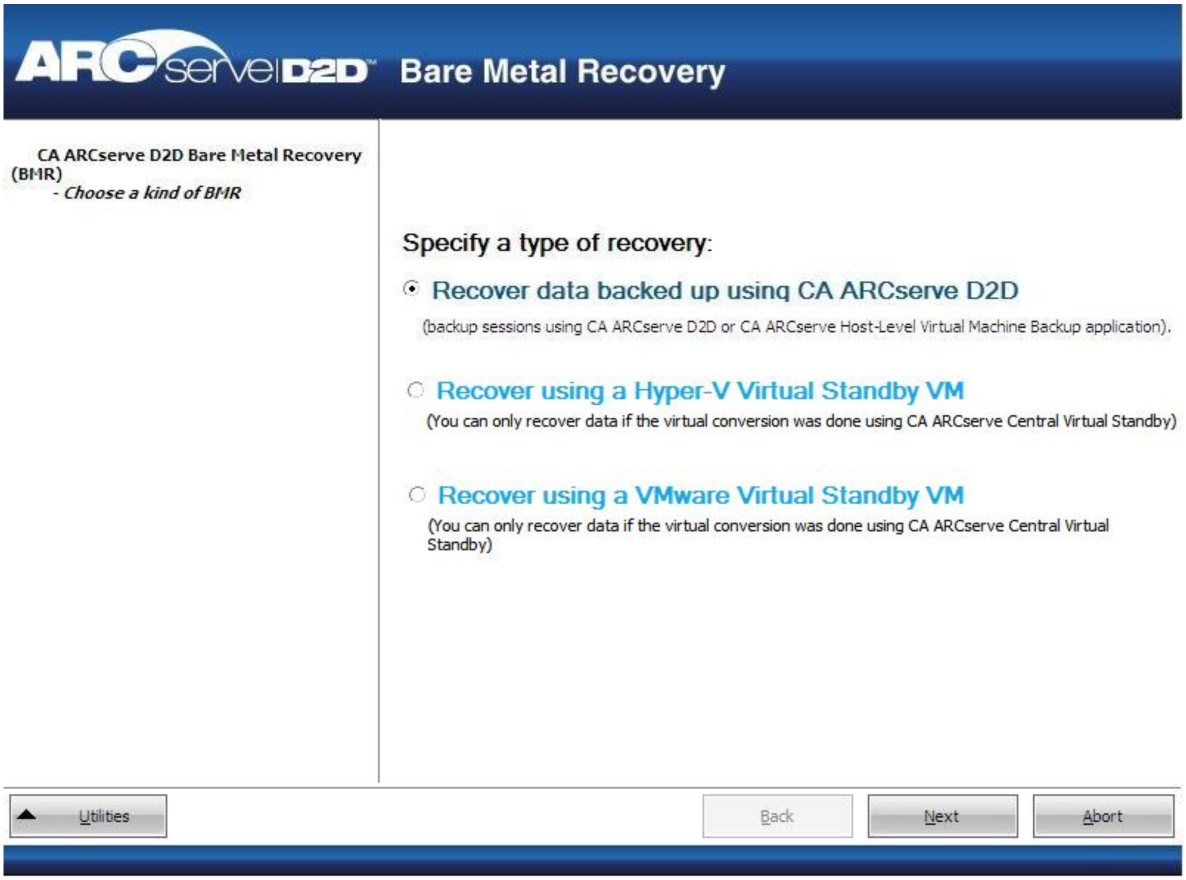
3. The CA ARCserve D2D language select screen is displayed. Select a language and press "Next" to continue.

   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.



Keyboard Layout: US

The Bare Metal Recovery process is initiated and the initial BMR wizard screen is displayed.



Specify a type of recovery:

● Recover data backed up using CA ARCserve D2D

(backup sessions using CA ARCserve D2D or CA ARCserve Host-Level Virtual Machine Backup application).

○ Recover using a Hyper-V Virtual Standby VM

(You can only recover data if the virtual conversion was done using CA ARCserve Central Virtual Standby)

○ Recover using a VMware Virtual Standby VM

(You can only recover data if the virtual conversion was done using CA ARCserve Central Virtual Standby)

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 to continue this procedure.

   - **Recover using a VMware Virtual Standby VM**

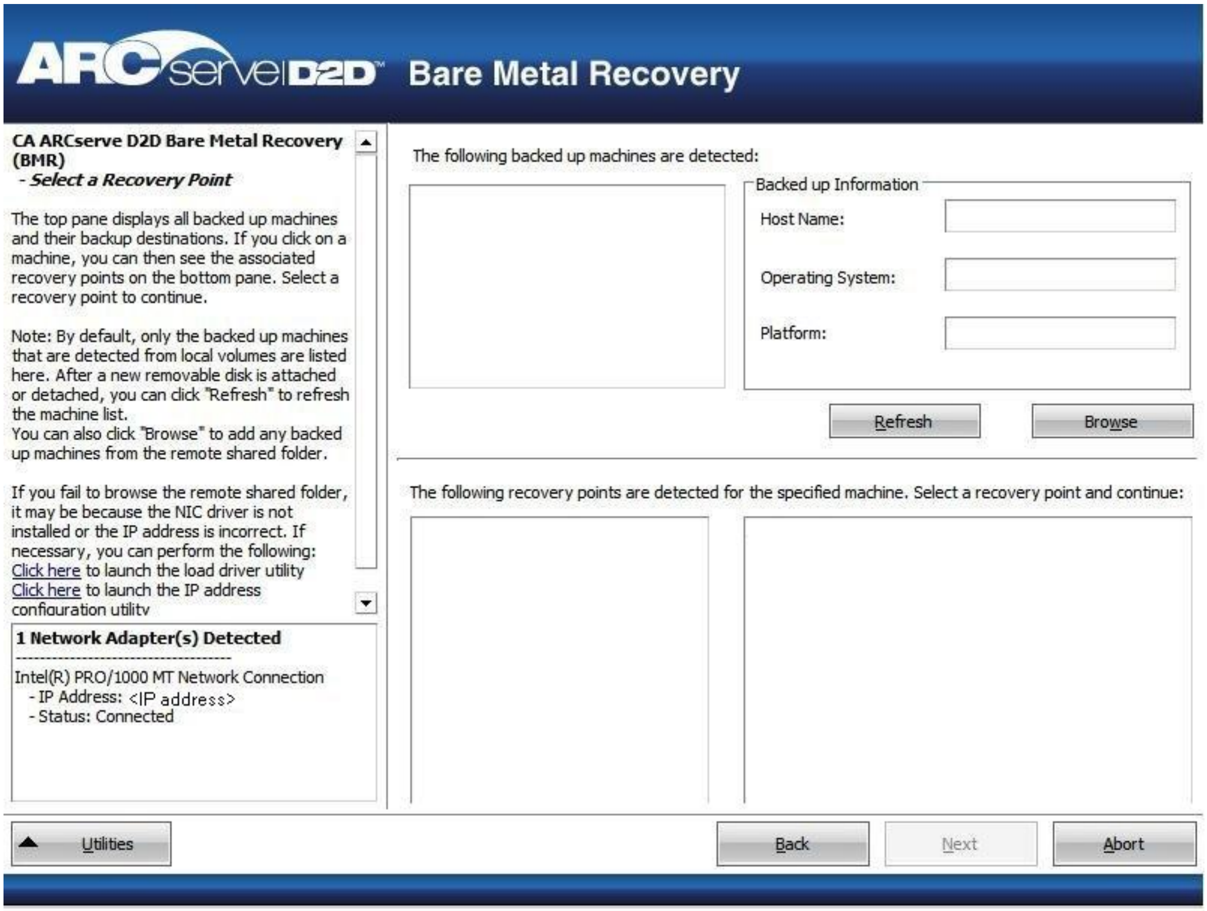
     Lets you recover data for a machine for which virtual conversion is done to a VMware virtual machine. This option is used in connection with the CA ARCserve Central Virtual Standby application.

     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 to continue this procedure.

5. Click Next.

   The Select a Recovery Point wizard screen is displayed.



CA ARCserve D2D Bare Metal Recovery (BMR)
- Select a Recovery Point

The top pane displays all backed up machines and their backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a recovery point to continue.

Note: By default, only the backed up machines that are detected from local volumes are listed here. After a new removable disk is attached or detached, you can click "Refresh" to refresh the machine list.
You can also click "Browse" to add any backed up machines from the remote shared folder.

If you fail to browse the remote shared folder, it may be because the NIC driver is not installed or the IP address is incorrect. If necessary, you can perform the following:
Click here to launch the load driver utility
Click here to launch the IP address configuration utility

1 Network Adapter(s) Detected

Intel(R) PRO/1000 MT Network Connection
- IP Address: <IP address>
- Status: Connected

The following backed up machines are detected:

The following recovery points are detected for the specified machine. Select a recovery point and continue:

6. From the Select a Recovery Point wizard screen, select the machine (or volume) which contains recovery points for your backup image.

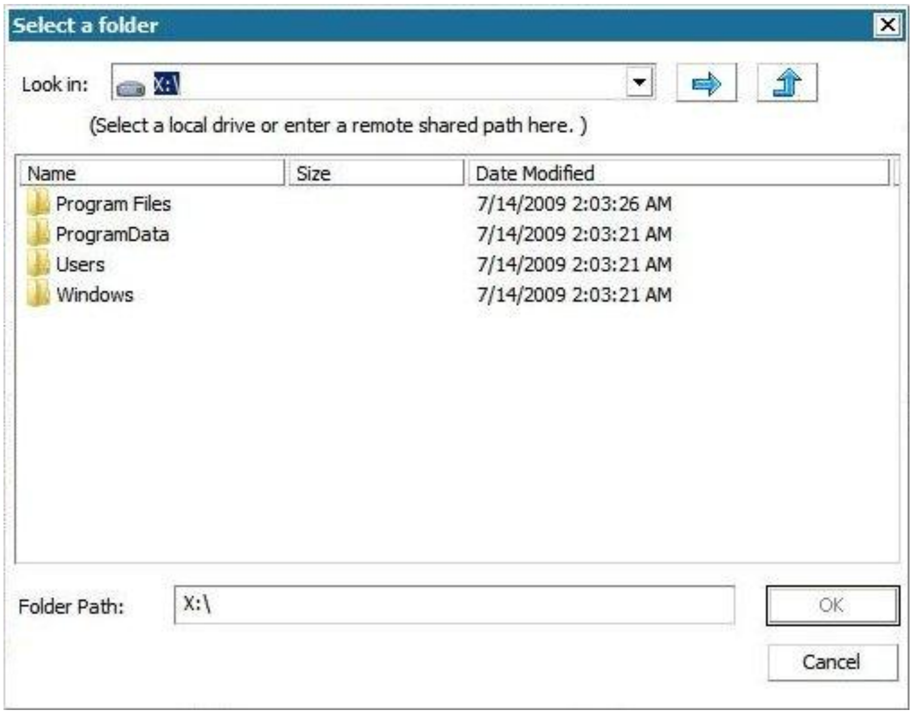
   CA ARCserve D2D lets you recover from any local drive or from a network share.

   - 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.



Look in: X:\

(Select a local drive or enter a remote shared path here.)

Name	Size	Date Modified
Program Files		7/14/2009 2:03:26 AM
ProgramData		7/14/2009 2:03:21 AM
Users		7/14/2009 2:03:21 AM
Windows		7/14/2009 2:03:21 AM

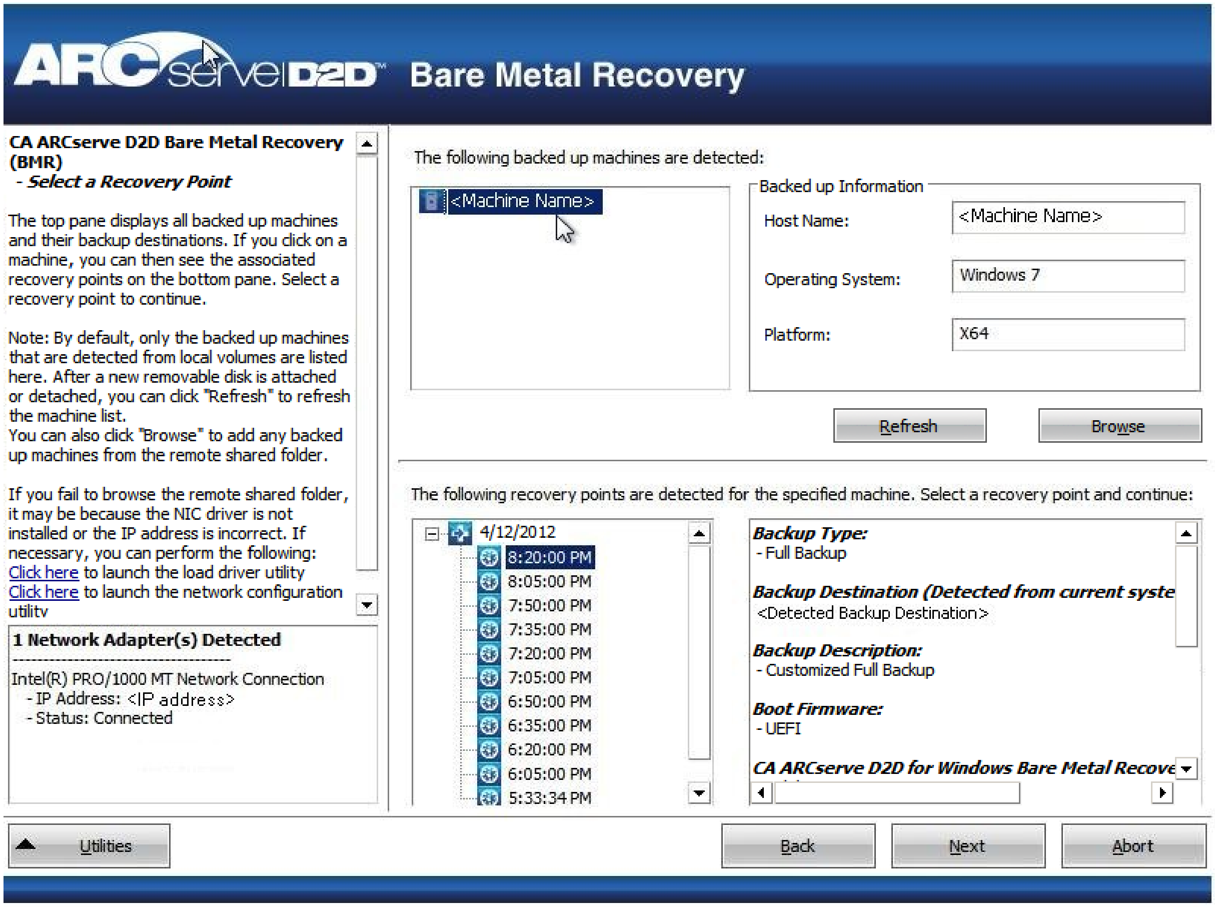
Folder Path: X:\

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.



CA ARCserve D2D Bare Metal Recovery (BMR)
- Select a Recovery Point

The top pane displays all backed up machines and their backup destinations. If you click on a machine, you can then see the associated recovery points on the bottom pane. Select a recovery point to continue.

Note: By default, only the backed up machines that are detected from local volumes are listed here. After a new removable disk is attached or detached, you can click "Refresh" to refresh the machine list.
You can also click "Browse" to add any backed up machines from the remote shared folder.

If you fail to browse the remote shared folder, it may be because the NIC driver is not installed or the IP address is incorrect. If necessary, you can perform the following:
Click here to launch the load driver utility
Click here to launch the network configuration utility

1 Network Adapter(s) Detected

Intel(R) PRO/1000 MT Network Connection
- IP Address: <IP address>
- Status: Connected

The following backed up machines are detected:

<Machine Name>

Backed up Information

Host Name: <Machine Name>

Operating System: Windows 7

Platform: X64

The following recovery points are detected for the specified machine. Select a recovery point and continue:

4/12/2012
- 8:20:00 PM
- 8:05:00 PM
- 7:50:00 PM
- 7:35:00 PM
- 7:20:00 PM
- 7:05:00 PM
- 6:50:00 PM
- 6:35:00 PM
- 6:20:00 PM
- 6:05:00 PM
- 5:33:34 PM

Backup Type:
- Full Backup

Backup Destination (Detected from current syste
<Detected Backup Destination>

Backup Description:
- Customized Full Backup

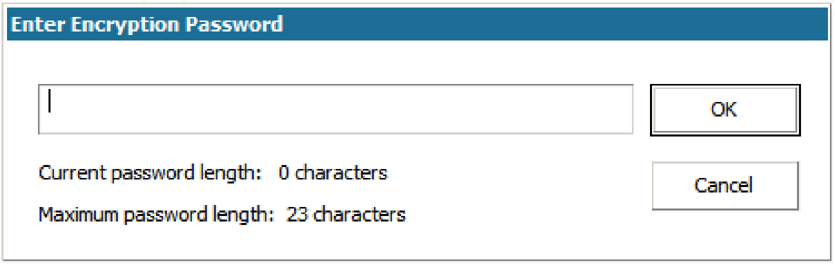
Boot Firmware:
- UEFI

CA ARCserve D2D for Windows Bare Metal Recove

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

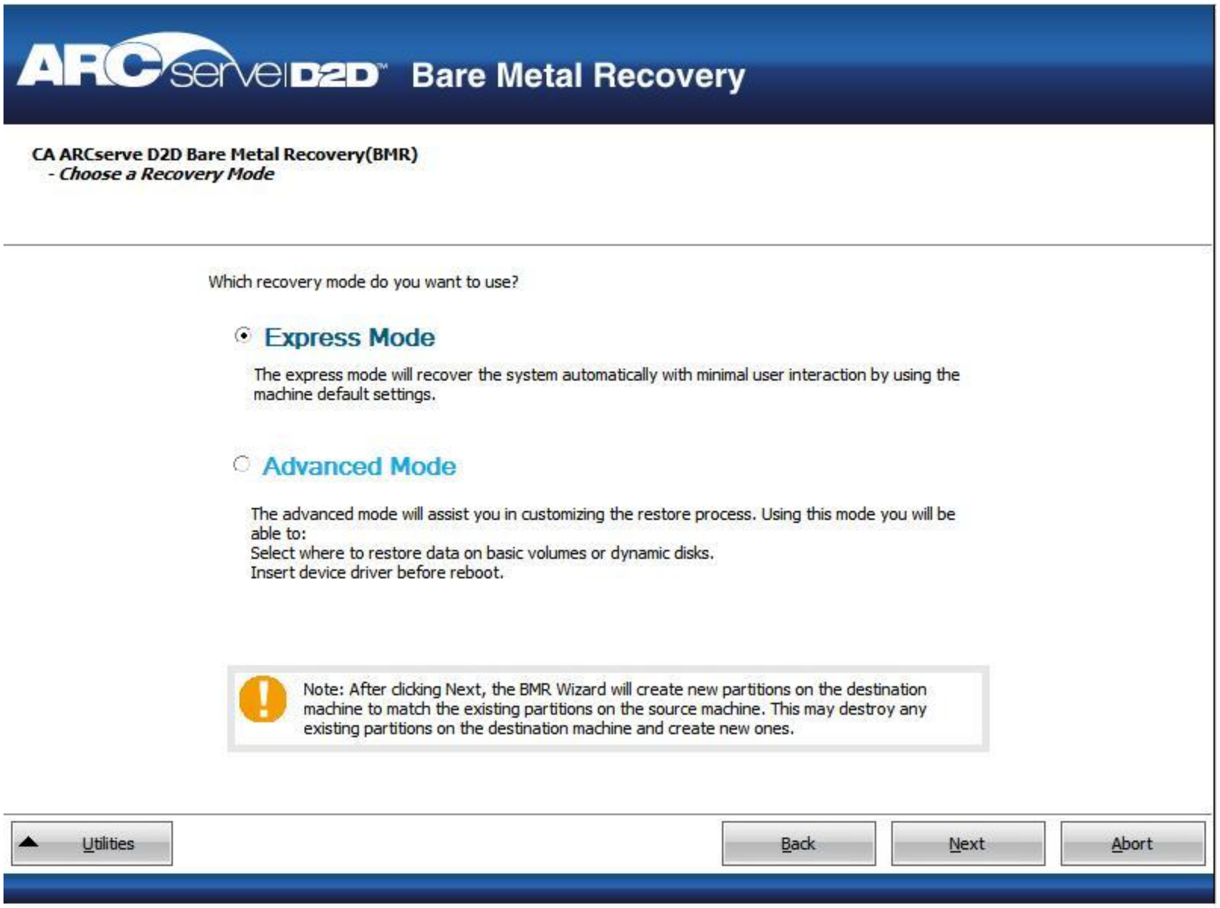
   Current password length: 0 characters

   Maximum password length: 23 characters

   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.



CA ARCserve D2D Bare Metal Recovery(BMR)
- *Choose a Recovery Mode*

Which recovery mode do you want to use?

● Express Mode

The express mode will recover the system automatically with minimal user interaction by using the machine default settings.

○ Advanced Mode

The advanced mode will assist you in customizing the restore process. Using this mode you will be able to:
Select where to restore data on basic volumes or dynamic disks.
Insert device driver before reboot.

Note: After clicking Next, the BMR Wizard will create new partitions on the destination machine to match the existing partitions on the source machine. This may destroy any existing partitions on the destination machine and create new ones.

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.

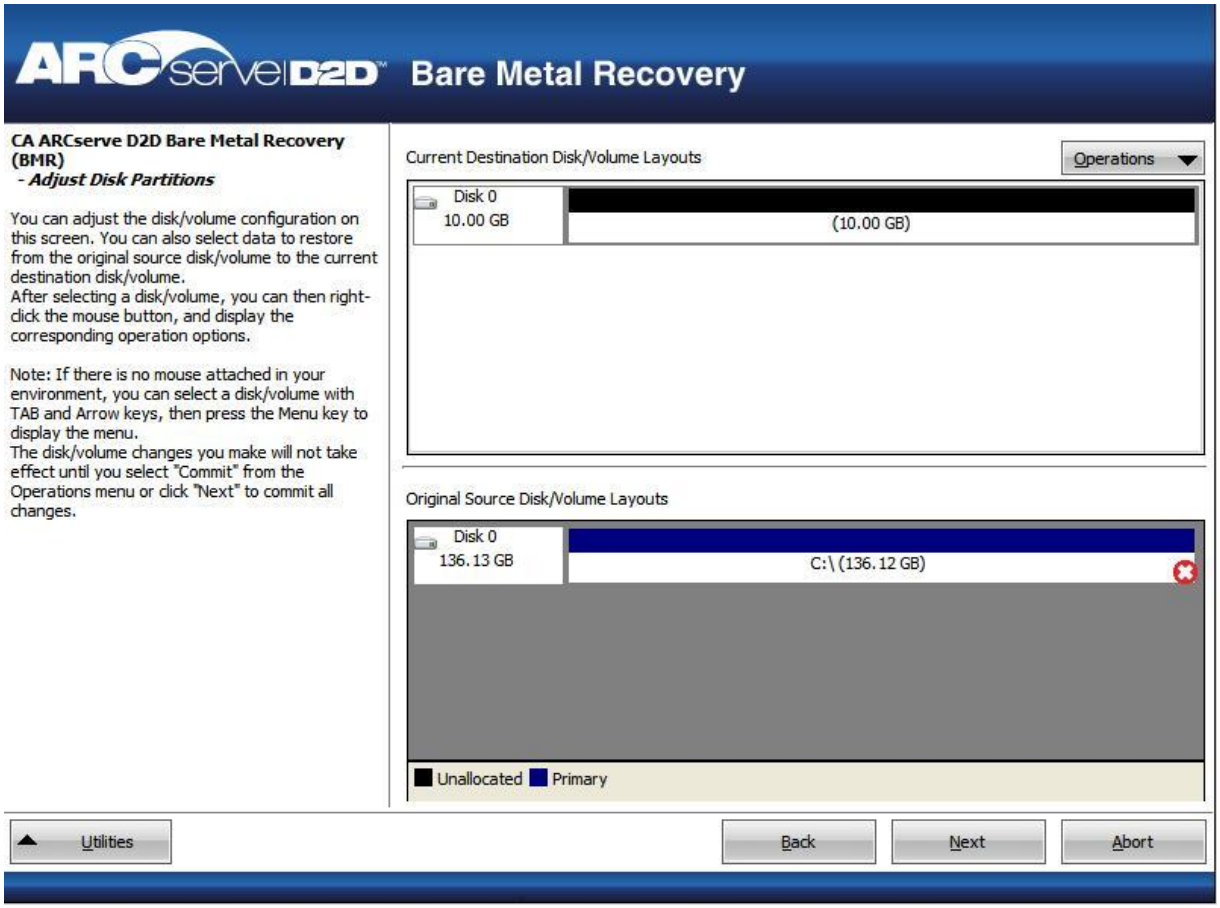
    The BMR utility starts locating the machine that is going to be recovered and displays the corresponding disk partition information.

    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.



CA ARCserve D2D Bare Metal Recovery (BMR)
- *Adjust Disk Partitions*

You can adjust the disk/volume configuration on this screen. You can also select data to restore from the original source disk/volume to the current destination disk/volume.
After selecting a disk/volume, you can then right-click the mouse button, and display the corresponding operation options.

Note: If there is no mouse attached in your environment, you can select a disk/volume with TAB and Arrow keys, then press the Menu key to display the menu.
The disk/volume changes you make will not take effect until you select "Commit" from the Operations menu or click "Next" to commit all changes.

Current Destination Disk/Volume Layouts

Disk 0 10.00 GB — (10.00 GB)

Original Source Disk/Volume Layouts

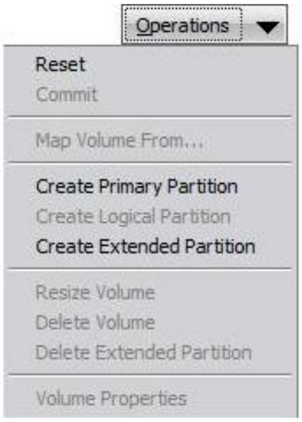
Disk 0 136.13 GB — C:\ (136.12 GB)

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.

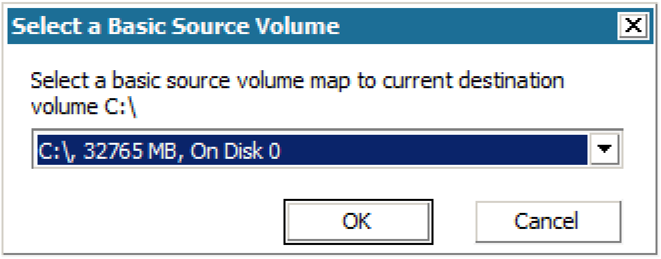
    From this menu, you can reset any existing partitions or you can create new partitions to correspond to the disk partitions on the source volume. (Reset means to reload the source and target disk layout information from the configure file and current OS, and discard any user changed disk layout information).

    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.



Select a basic source volume map to current destination volume C:\

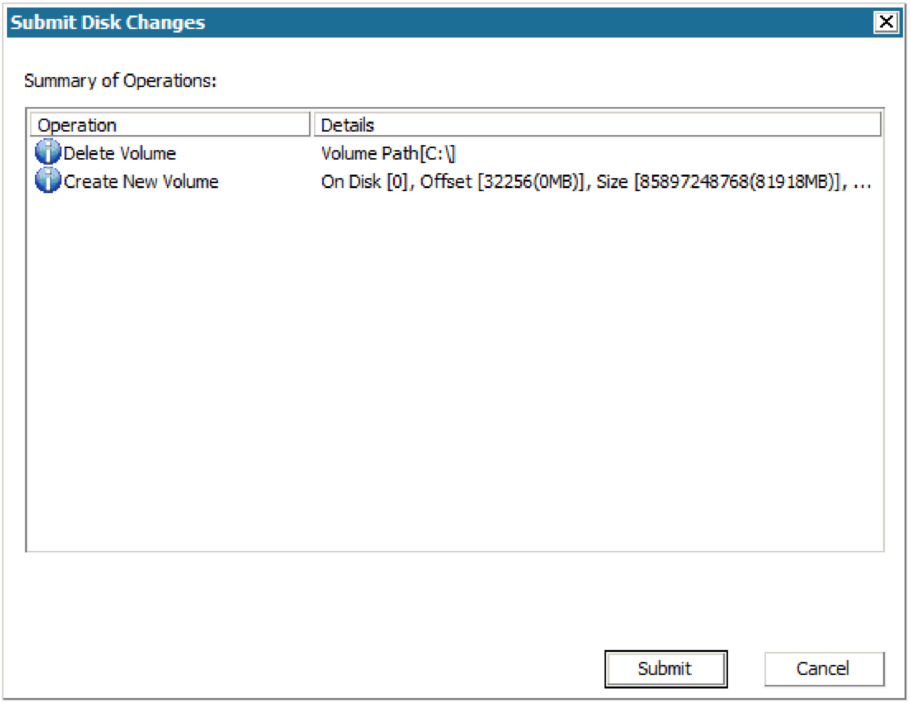
C:\, 32765 MB, On Disk 0

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.



Submit Disk Changes

Summary of Operations:

Operation	Details
Delete Volume	Volume Path[C:\]
Create New Volume	On Disk [0], Offset [32256(0MB)], Size [85897248768(81918MB)], ...

18. When you have verified the summary information is correct, click Submit. (If the information is not correct, click Cancel).

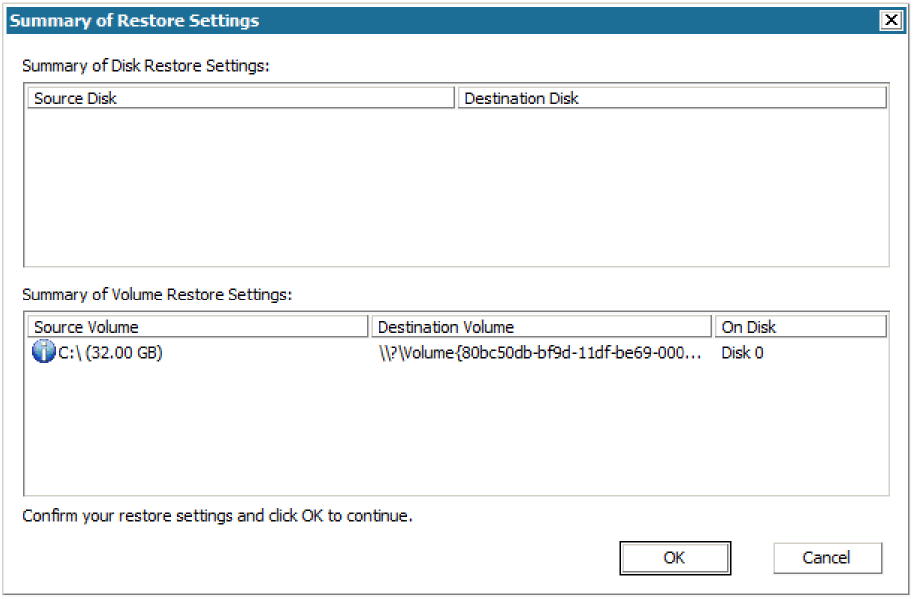
    Note: All operations to the hard drive do not take effect until you submit it.

    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:

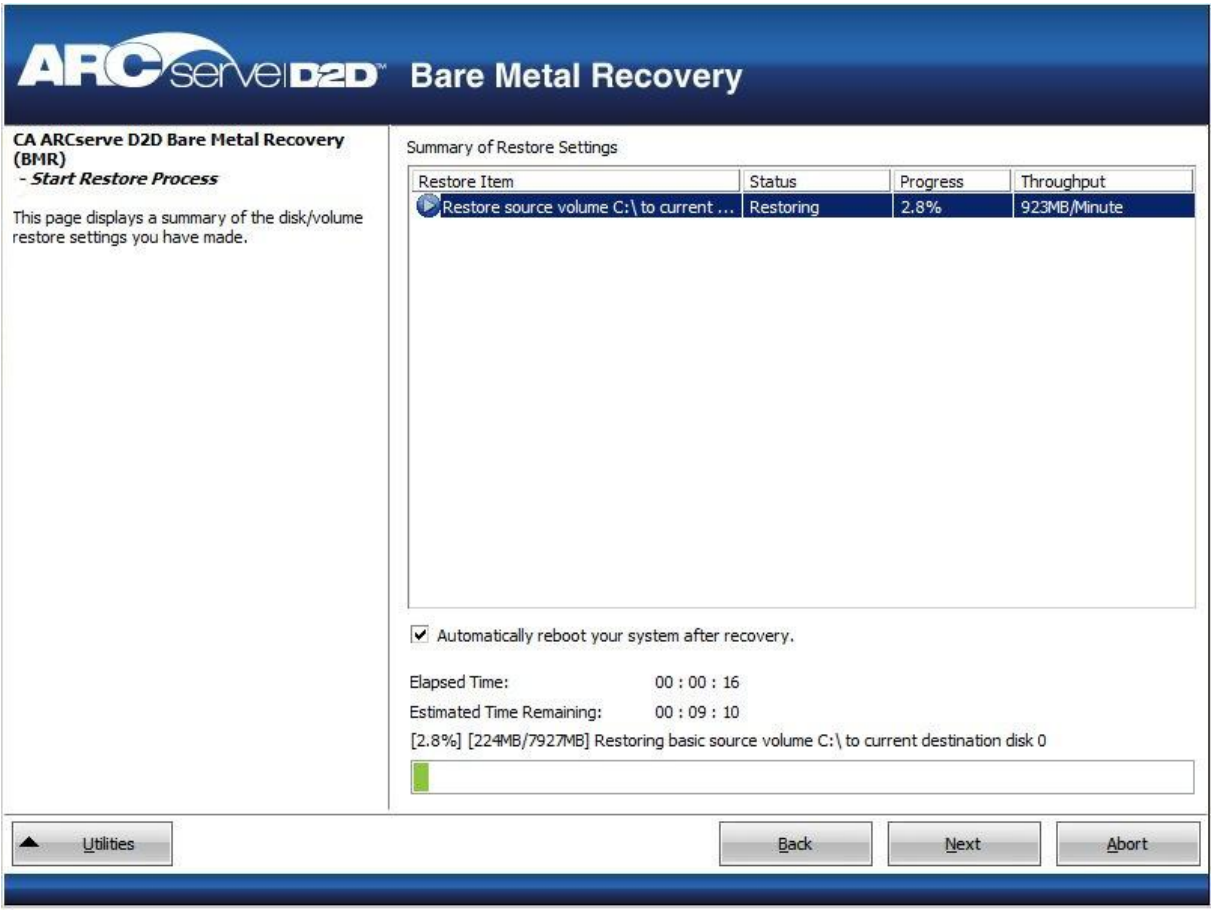
Source Volume	Destination Volume	On Disk
C:\ (32.00 GB)	\\?\Volume{80bc50db-bf9d-11df-be69-000...	Disk 0

Confirm your restore settings and click OK to continue.

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.



CA ARCserve D2D Bare Metal Recovery (BMR)
- Start Restore Process

This page displays a summary of the disk/volume restore settings you have made.

Summary of Restore Settings

Restore Item	Status	Progress	Throughput
Restore source volume C:\ to current ...	Restoring	2.8%	923MB/Minute

☑ Automatically reboot your system after recovery.

Elapsed Time: 00 : 00 : 16

Estimated Time Remaining: 00 : 09 : 10

[2.8%] [224MB/7927MB] Restoring basic source volume C:\ to current destination disk 0

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).

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.

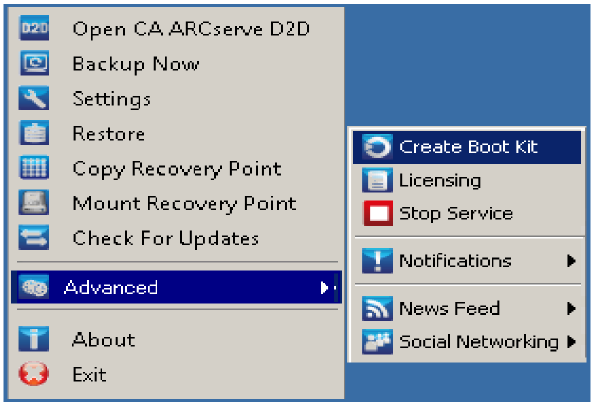
Videos

CA Support:	How to: Create a Boot Kit
YouTube:	How to: Create a Boot Kit

To create a boot kit

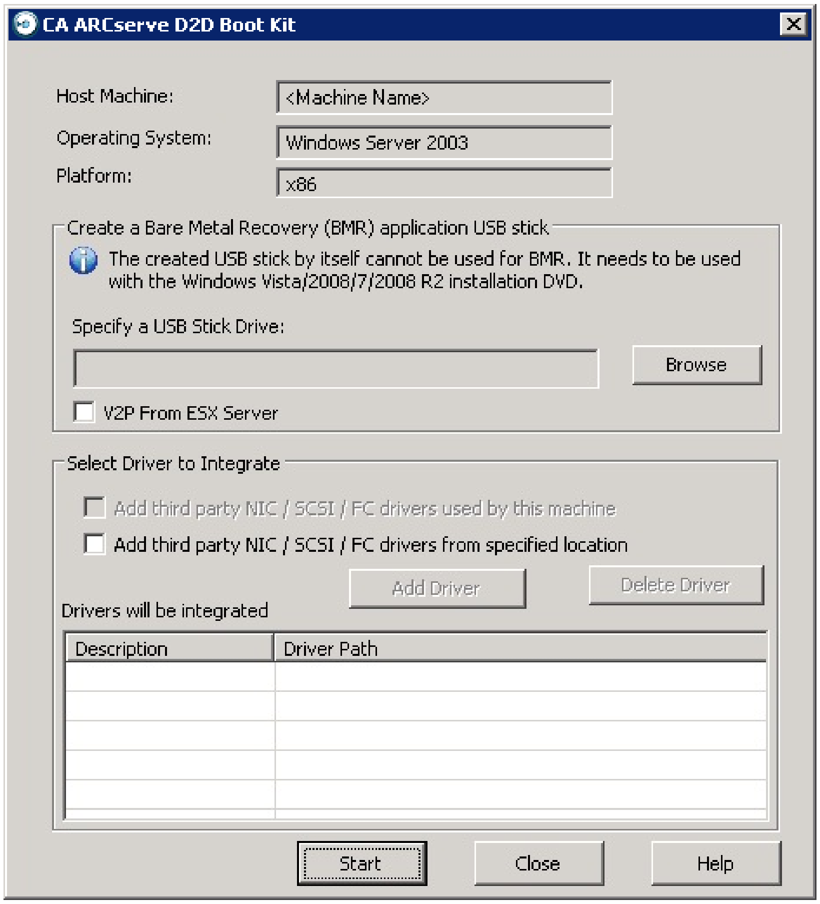
1. From the CA ARCserve D2D Monitor, click the Advanced option and then select Create Boot Kit.

   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.



CA ARCserve D2D Boot Kit

Host Machine: <Machine Name>

Operating System: Windows Server 2003

Platform: x86

Create a Bare Metal Recovery (BMR) application USB stick

The created USB stick by itself cannot be used for BMR. It needs to be used with the Windows Vista/2008/7/2008 R2 installation DVD.

Specify a USB Stick Drive:
Browse
□ V2P From ESX Server
Select Driver to Integrate
□ Add third party NIC / SCSI / FC drivers used by this machine
□ Add third party NIC / SCSI / FC drivers from specified location
Add Driver
Delete Driver
Drivers will be integrated
Description
Driver Path
Start
Close
Help

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.

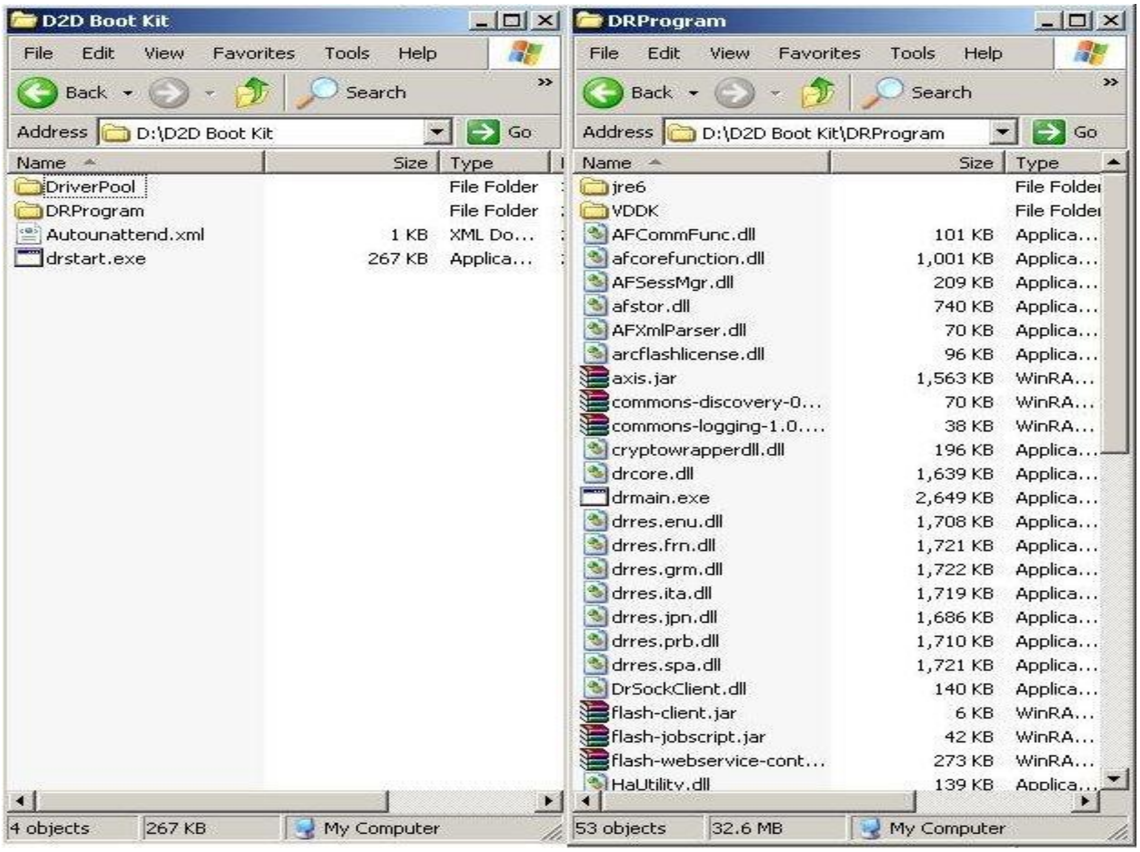
The selected drivers are then loaded during the recovery process.

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.



Address D:\D2D Boot Kit

Name	Size	Type
DriverPool		File Folder
DRProgram		File Folder
Autounattend.xml	1 KB	XML Do...
drstart.exe	267 KB	Applica...

4 objects | 267 KB | My Computer

Address D:\D2D Boot Kit\DRProgram

Name	Size	Type
jre6		File Folder
VDDK		File Folder
AFCommFunc.dll	101 KB	Applica...
afcorefunction.dll	1,001 KB	Applica...
AFSessMgr.dll	209 KB	Applica...
afstor.dll	740 KB	Applica...
AFXmlParser.dll	70 KB	Applica...
arcflashlicense.dll	96 KB	Applica...
axis.jar	1,563 KB	WinRA...
commons-discovery-0...	70 KB	WinRA...
commons-logging-1.0....	38 KB	WinRA...
cryptowrapperdll.dll	196 KB	Applica...
drcore.dll	1,639 KB	Applica...
drmain.exe	2,649 KB	Applica...
drres.enu.dll	1,708 KB	Applica...
drres.frn.dll	1,721 KB	Applica...
drres.grm.dll	1,722 KB	Applica...
drres.ita.dll	1,719 KB	Applica...
drres.jpn.dll	1,686 KB	Applica...
drres.prb.dll	1,710 KB	Applica...
drres.spa.dll	1,721 KB	Applica...
DrSockClient.dll	140 KB	Applica...
flash-client.jar	6 KB	WinRA...
flash-jobscript.jar	42 KB	WinRA...
flash-webservice-cont...	273 KB	WinRA...
HaUtility.dll	139 KB	Applica...

53 objects | 32.6 MB | My Computer

Define a Limit to the Quantity of Concurrent Backups

You can define a limit to the quantity of CA ARCserve D2D backup jobs that run concurrently. This capability lets you optimize the performance of the CA ARCserve D2D virtual machine proxy server in your backup environment. By default, Host-Based VM Backup can run up to ten D2D backup jobs concurrently. In environments that contain many virtual machines that are associated with a CA ARCserve D2D virtual machine proxy system, a high quantity of concurrent backups can have an adverse effect on network and backup performance.

Note: When the quantity of concurrent jobs exceeds the defined limit, the jobs that exceed the limit enter a job queue.

Follow these steps:

1. Log in to the CA ARCserve D2D virtual machine proxy system.
2. Open Windows Registry Editor and browse to the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D
3. Right-click CA ARCserve D2D and select New and click String Value on the pop-up menu.

   Name the key as follows:

   VsphereMaxJobNum
4. Right-click VsphereMaxJobNum and click Modify on the pop-up menu.

   The Edit String dialog opens.
5. In the Value Data field, specify the quantity of CA ARCserve D2D backup jobs that you want to allow to run concurrently.
   - **Minimum limit--**1
   - **Maximum limit--**none.
6. Click OK.

The limit is defined.

Increase the Quantity of Messages Retained in the VMVixMgr Log File

The VMVixMgr Log file retains messages that relate to VMware VIX operations. For more information about the VMware VIX API, see the VMware website.

The VMVixMgr log file (VMVixMgr.log) is stored in the following directory on the backup proxy system:

```
C:\Program Files\CA\ARCserve D2D\Logs
```

By default, the log file cannot exceed 500KB. When the log file exceeds 500KB, the messages contained in the log file will be overwritten. This behavior prevents the log file from exceeding 500KB.

When you define a schedule to back up data in 15-minute intervals, it is likely that the log file will be overwritten when the log file exceeds 500 KB. Increasing the size of the log file lets you retain more messages in the log file.

As a best practice, increase the size of the log file only when you define a schedule to back up data every 15 minutes.

Follow these steps:

1. Log in to the backup proxy system.
2. Open Windows Registry Editor and browse to the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCserve D2D
   ```

3. Right-click CA ARCserve D2D, select New, and click DWORD on the pop-up menu.

   Name the DWORD as follows:

   ```
   VixMgrLogSize
   ```

   Note: If this DWORD is not present, the default value for the log file is in effect at 500KB.

4. After you create the DWORD, right-click VixMgrLogSize and click Modify on the pop-up menu to open the Edit DWORD dialog.
5. In the Value Data field on the Edit DWORD dialog, specify a value (in KB) for the log file. For example, 750, 1000, and so on.
6. Click OK to apply the value and close the Edit DWORD dialog.

Protect the CA ARCserve D2D Backup Proxy

Backup sessions created with CA ARCserve Central Host-Based VM Backup are stored on the backup proxy. There are several ways you can protect the backup proxy itself, depending on your configuration.

- If you are running CA ARCserve Central Protection Manager, you can add the backup proxy as a node to be protected. For more information, see the CA ARCserve Central Protection Manager User Guide.
- Launch the CA ARCserve D2D instance running locally on the backup proxy and configure backup settings. Select Entire Machine as the backup source. For more information, see the CA ARCserve D2D User Guide.
- If you are running CA ARCserve Backup, you can configure a backup job to protect the proxy.

How the Installation Process Affects Operating Systems

The CA ARCserve Central Applications 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 Central Applications perform custom actions that let you install or upgrade CA ARCserve Central Applications.

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

Note: All CA ARCserve Central Applications MSI packages call the components listed in this table when you install CA ARCserve Central Applications.

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

Component	Description
CallPreUninstall	Lets the uninstallation process perform various tasks relating to uninstallation. For example, un-registering CA ARCserve Central Applications 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.)
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 Central Applications files in the following directories by default:

  C:\Program Files\CA\ARCserve Central Applications

  You can install CA ARCserve Central Applications into the default installation directory or into an alternative 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 Central Applications

  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

Binary Files Containing Incorrect File Version Information

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

Binary Name	Source
BaseLicInst.exe	CA License
UpdateData.exe	CA License
vcredist_x64.exe	Microsoft
vcredist_x86.exe	Microsoft

Binary Name	Source
WindowsInstaller-KB893803-v2-x86.exe	Microsoft
tomcat6.exe	Tomcat

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

CA ARCserve Central Applications installs binary files that are developed by third parties, other CA Technologies products, and CA ARCserve Central Applications 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 Central Applications services, components, and applications. The binaries corresponding to these services, components, and applications contain CA ARCserve Central Applications specific functionality that is not available to a basic user account. As a result, Windows will prompt you to confirm an operation by specifying your password or by using an account with administrative privileges to complete the operation.

- **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 will be 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.

Binary Name	Source
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
D2DPMConfigSettings.exe	CA ARCserve Central Applications

Binary Name	Source
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Appendix A: CA ARCserve D2D Procedures

This section has been excerpted from the CA ARCserve D2D User Guide for your convenience.

Note: Some CA ARCserve D2D settings and steps may not apply to CA ARCserve Central Host-Based VM Backup.

This section contains the following topics:

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.

Videos

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 Central Applications.

       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.

    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.

    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 Central Applications 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 162).

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 176)
- Schedule Settings (see page 190)
- Advanced Settings (see page 192)
- Pre/Post Backup Settings (see page 196)

Specify the Protection Settings

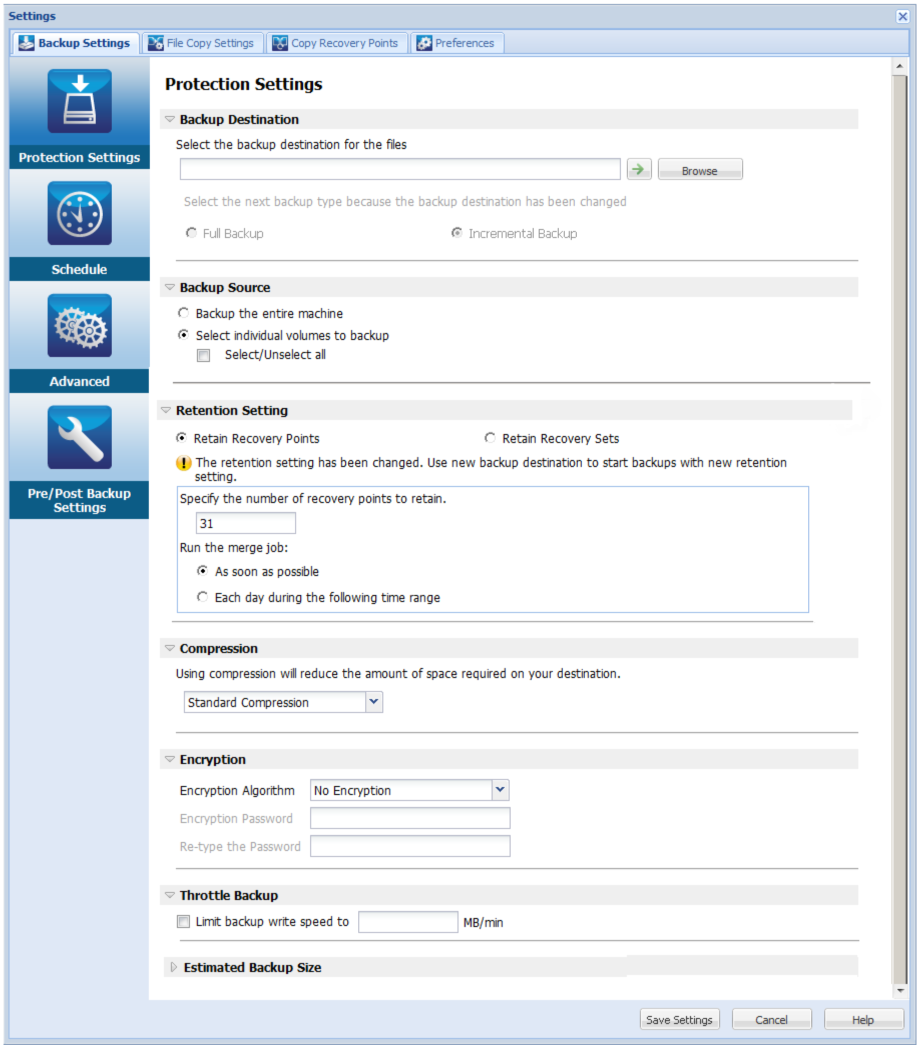
Protection settings for the information going to be backed up ensures that the backup data is reliably protected (copied and saved) against any form of data loss.

Note: To view a video that is related to these Backup Settings, see Manage Backup Settings (see page 175).

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.



Protection Settings

Backup Destination

Select the backup destination for the files

Select the next backup type because the backup destination has been changed

○ Full Backup ● Incremental Backup

Backup Source

○ Backup the entire machine

● Select individual volumes to backup

□ Select/Unselect all

Retention Setting

● Retain Recovery Points ○ Retain Recovery Sets

! The retention setting has been changed. Use new backup destination to start backups with new retention setting.

Specify the number of recovery points to retain.

31

Run the merge job:

● As soon as possible

○ Each day during the following time range

Compression

Using compression will reduce the amount of space required on your destination.

Standard Compression

Encryption

Encryption Algorithm: No Encryption

Encryption Password

Re-type the Password

Throttle Backup

□ Limit backup write speed to MB/min

Estimated Backup Size

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.

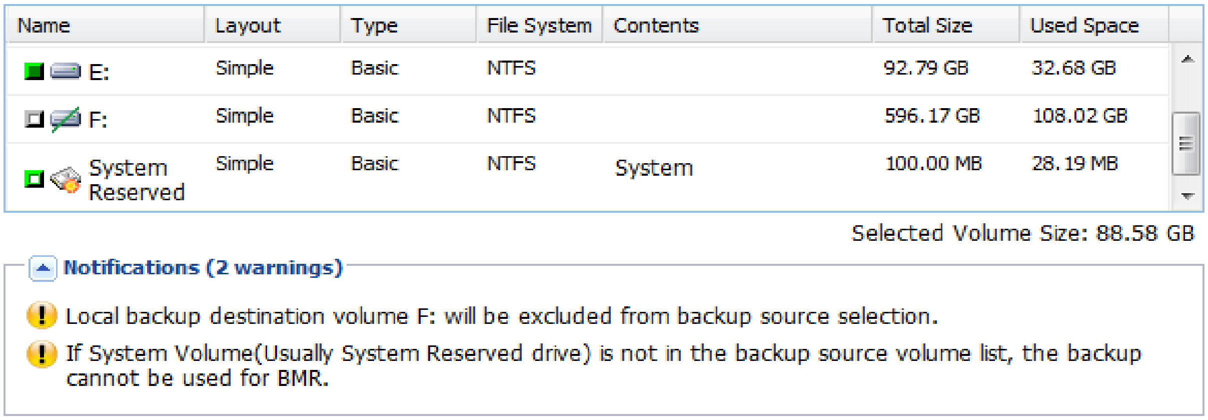
   Select individual volumes to back up

   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**.

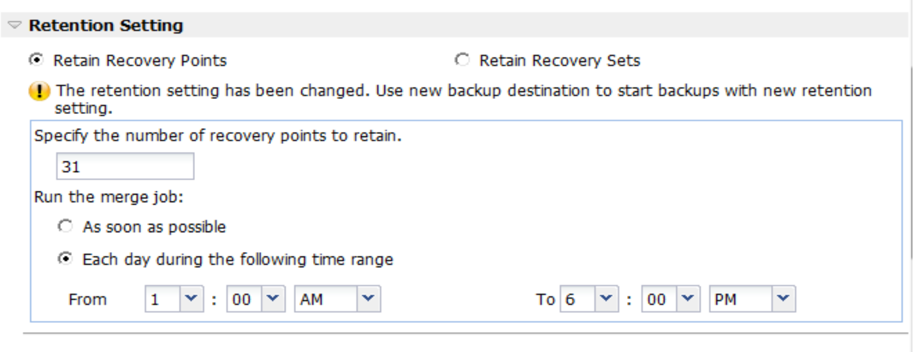
   You can set the retention setting based on the number of recovery points to retain (merges sessions) or based on the number of recovery sets to retain (deletes recovery sets and disables infinite incremental backups).

   - 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

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.



Retention Setting

● Retain Recovery Points ○ Retain Recovery Sets

The retention setting has been changed. Use new backup destination to start backups with new retention setting.

Specify the number of recovery points to retain.

31

Run the merge job:

○ As soon as possible

● Each day during the following time range

From 1 : 00 AM To 6 : 00 PM

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 Managing Merge Jobs.

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.

Run the merge job:

As soon as possible

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

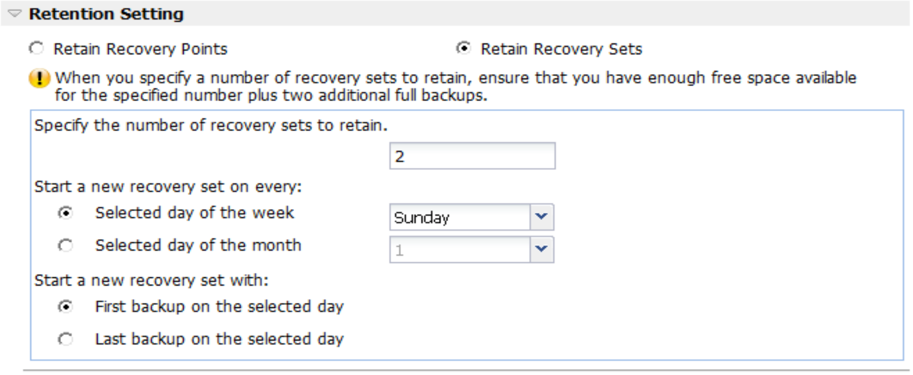
Each day during the following time range

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.



Retention Setting

○ Retain Recovery Points ● Retain Recovery Sets

When you specify a number of recovery sets to retain, ensure that you have enough free space available for the specified number plus two additional full backups.

Specify the number of recovery sets to retain.: 2

Start a new recovery set on every:

● Selected day of the week: Sunday

○ Selected day of the month: 1

Start a new recovery set with:

● First backup on the selected day

○ Last backup on the selected day

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 Status Summary Overview.

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.

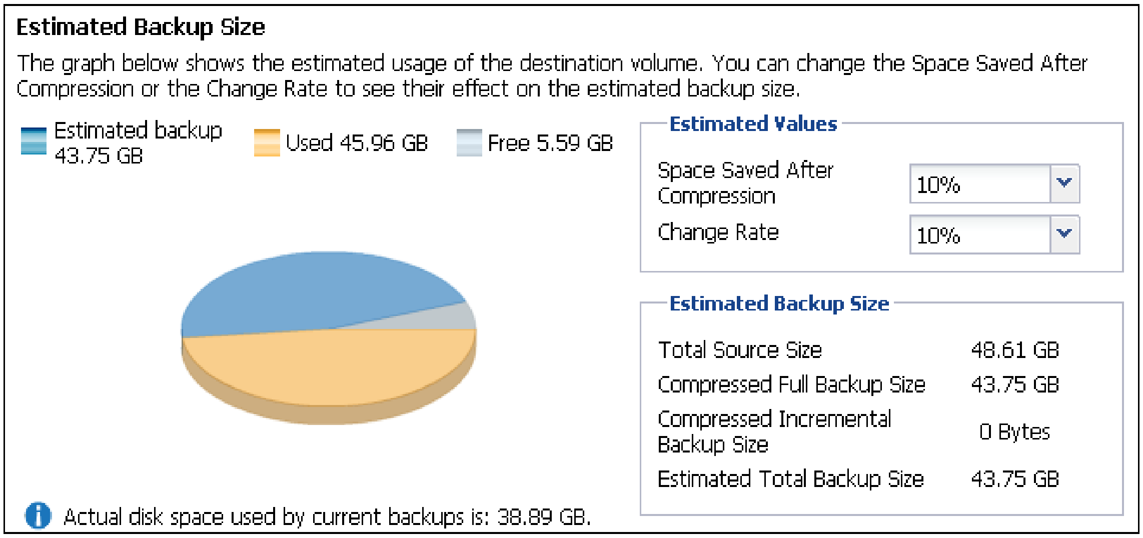
   For more information about using these estimated backup calculations, see Estimate Future Backup Space Requirements (see page 188).

9. Click Save Settings.

   Your backup protection settings are saved.

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.



Estimated Backup Size

The graph below shows the estimated usage of the destination volume. You can change the Space Saved After Compression or the Change Rate to see their effect on the estimated backup size.

Estimated Values

Space Saved After Compression: 10%

Change Rate: 10%

Estimated Backup Size

Total Source Size	48.61 GB
Compressed Full Backup Size	43.75 GB
Compressed Incremental Backup Size	0 Bytes
Estimated Total Backup Size	43.75 GB

Actual disk space used by current backups is: 38.89 GB.

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

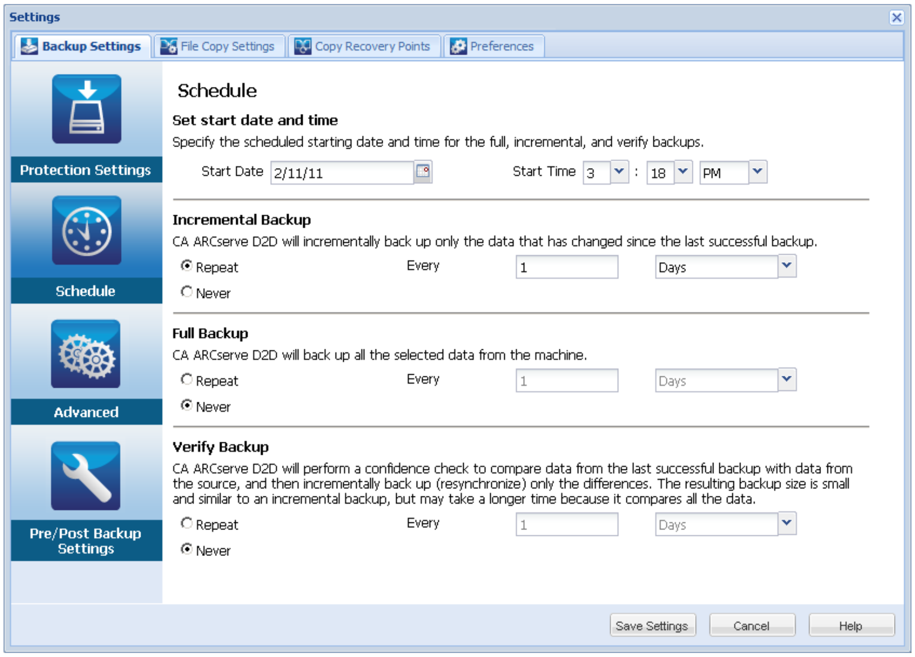
CA ARCserve D2D lets you specify the schedule for your backups.

Note: To view a video related to these Backup Settings, see Manage Backup Settings (see page 175).

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.



Schedule

Set start date and time

Specify the scheduled starting date and time for the full, incremental, and verify backups.

Start Date 2/11/11 Start Time 3 : 18 PM

Incremental Backup

CA ARCserve D2D will incrementally back up only the data that has changed since the last successful backup.

● Repeat Every 1 Days

○ Never

Full Backup

CA ARCserve D2D will back up all the selected data from the machine.

○ Repeat Every 1 Days

● Never

Verify Backup

CA ARCserve D2D will perform a confidence check to compare data from the last successful backup with data from the source, and then incrementally back up (resynchronize) only the differences. The resulting backup size is small and similar to an incremental backup, but may take a longer time because it compares all the data.

○ Repeat Every 1 Days

● Never

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

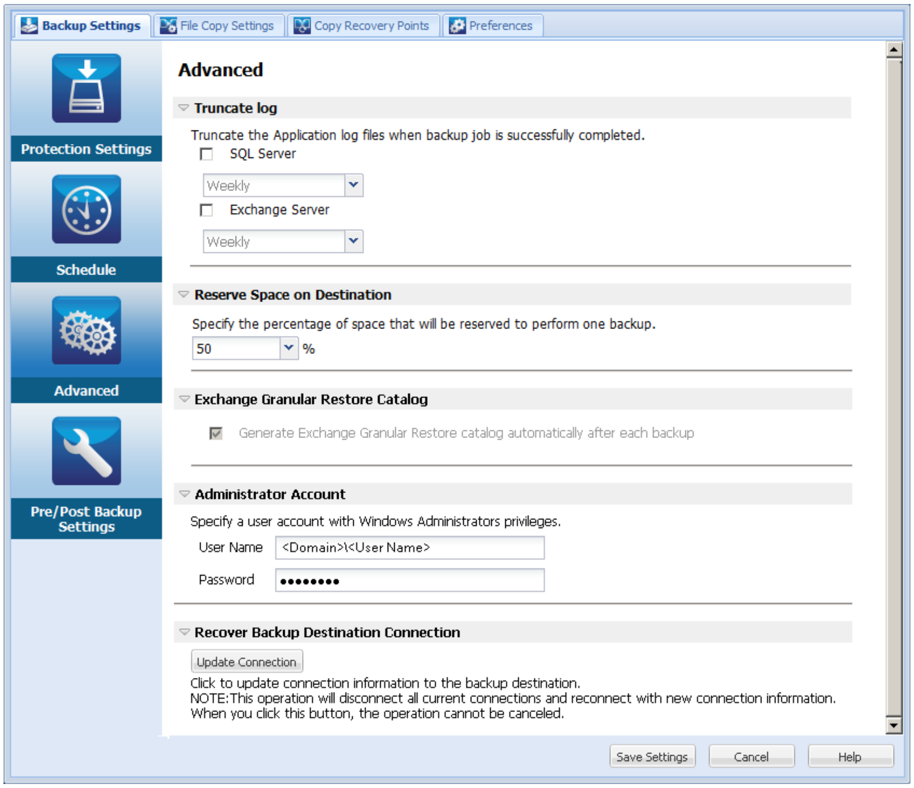
CA ARCserve D2D lets you specify the Advanced Settings for your backups.

Note: To view a video that is related to these Backup Settings, see Manage Backup Settings (see page 175).

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.



Advanced

Truncate log

Truncate the Application log files when backup job is successfully completed.

□ SQL Server

Weekly

□ Exchange Server

Weekly

Reserve Space on Destination

Specify the percentage of space that will be reserved to perform one backup.

50 %

Exchange Granular Restore Catalog

☑ Generate Exchange Granular Restore catalog automatically after each backup

Administrator Account

Specify a user account with Windows Administrators privileges.

User Name <Domain>\<User Name>

Password ••••••••

Recover Backup Destination Connection

Update Connection

Click to update connection information to the backup destination.
NOTE:This operation will disconnect all current connections and reconnect with new connection information.
When you click this button, the operation cannot be canceled.

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

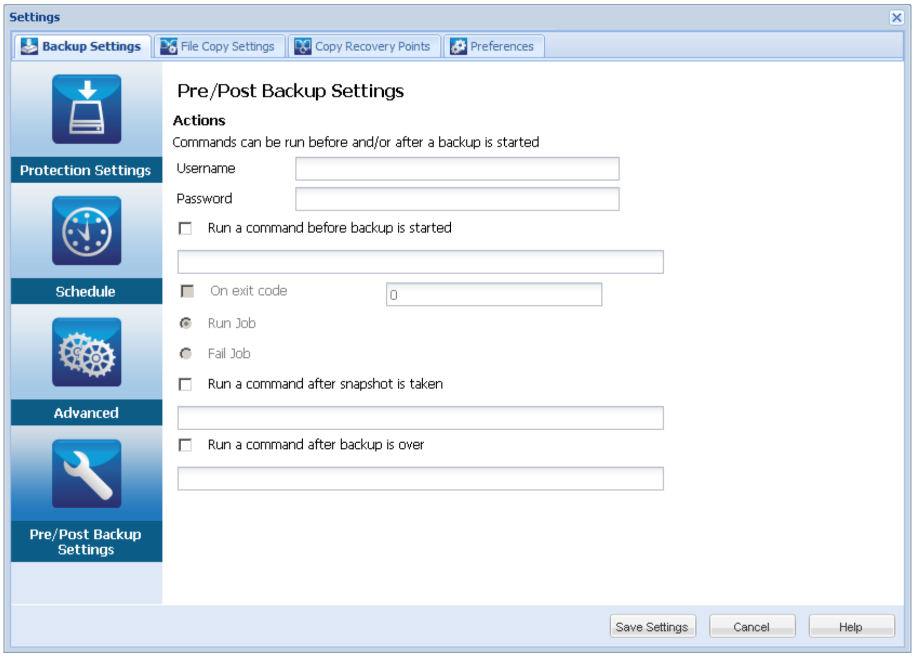
CA ARCserve D2D lets you specify the Pre/Post Backup settings.

Note: To view a video that is related to these Backup Settings, see Manage Backup Settings (see page 175).

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.



Pre/Post Backup Settings

Actions

Commands can be run before and/or after a backup is started

Username

Password

☐ Run a command before backup is started

☐ On exit code 0

○ Run Job

○ Fail Job

☐ Run a command after snapshot is taken

☐ Run a command after backup is over

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.

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 198)
- Email Alerts (see page 200)
- Updates (see page 206)

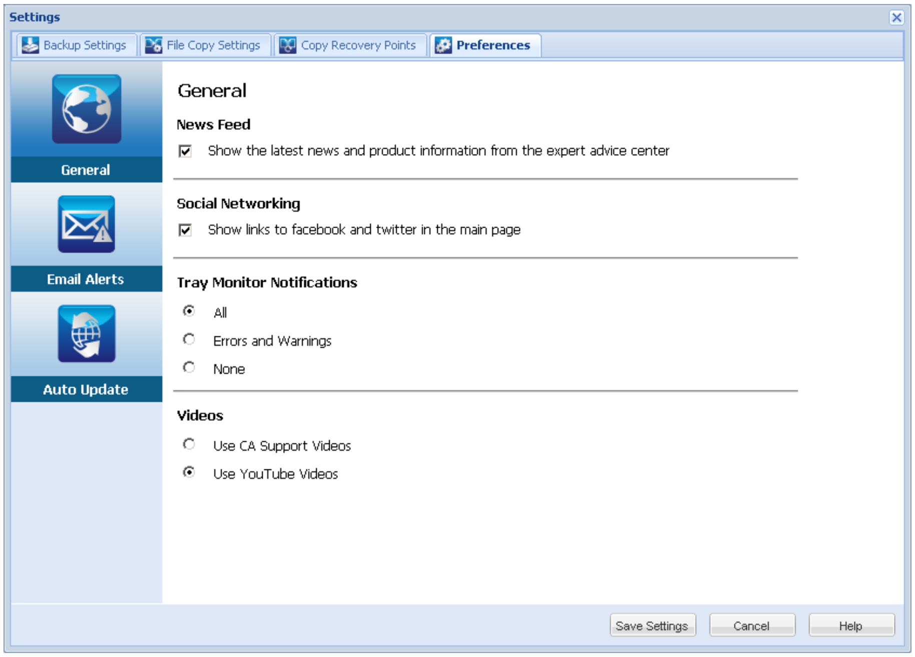
Specify General Preferences

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.



General

News Feed

☑ Show the latest news and product information from the expert advice center

Social Networking

☑ Show links to facebook and twitter in the main page

Tray Monitor Notifications

● All
○ Errors and Warnings
○ None

Videos

○ Use CA Support Videos
● Use YouTube Videos

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 screen or the Support and Community Access 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.

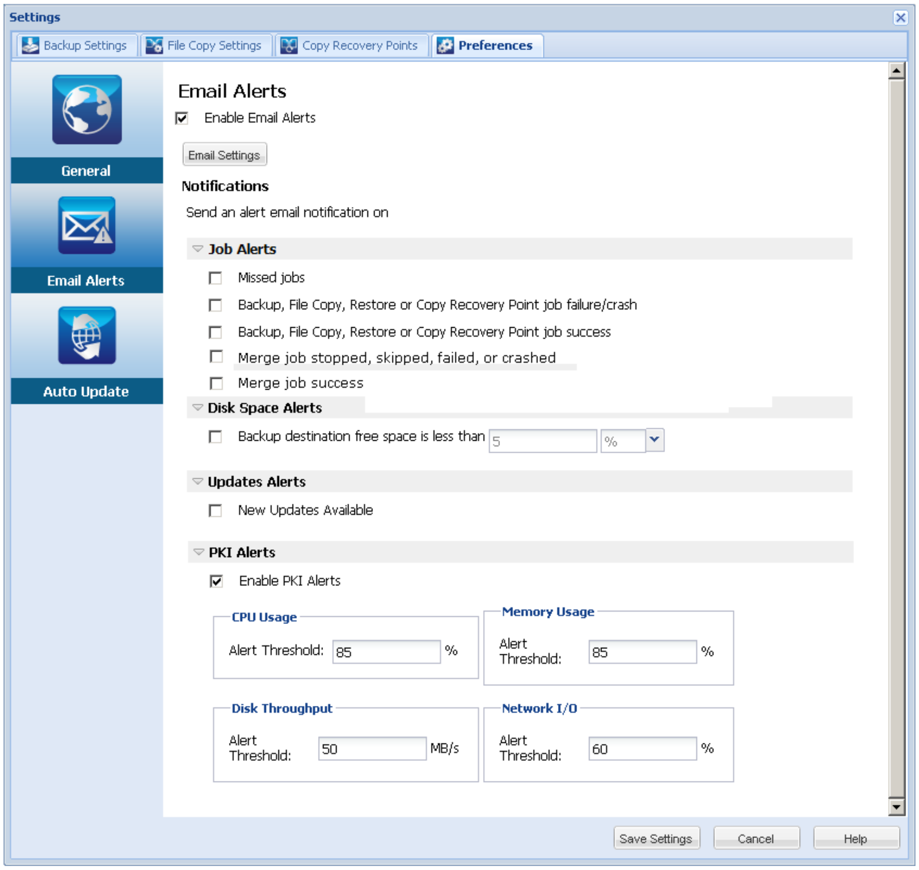
Specify Email Preferences

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.



Email Alerts

☑ Enable Email Alerts

Email Settings

Notifications

Send an alert email notification on

Job Alerts

□ Missed jobs

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

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

□ Merge job stopped, skipped, failed, or crashed

□ Merge job success

Disk Space Alerts

□ Backup destination free space is less than 5 %

Updates Alerts

□ New Updates Available

PKI Alerts

☑ Enable PKI Alerts

CPU Usage: Alert Threshold: 85 %

Memory Usage: Alert Threshold: 85 %

Disk Throughput: Alert Threshold: 50 MB/s

Network I/O: Alert Threshold: 60 %

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.

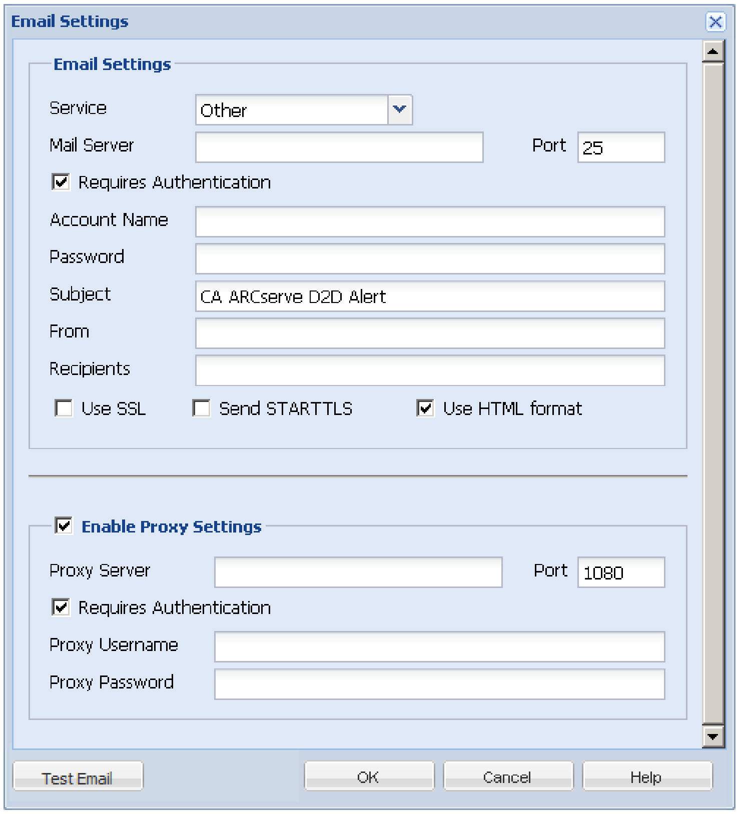
Specify Email Settings

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.



Email Settings

Email Settings

Service: Other

Mail Server: Port: 25

☑ Requires Authentication

Account Name:

Password:

Subject: CA ARCserve D2D Alert

From:

Recipients:

□ Use SSL □ Send STARTTLS ☑ Use HTML format

☑ Enable Proxy Settings

Proxy Server: Port: 1080

☑ Requires Authentication

Proxy Username:

Proxy Password:

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.

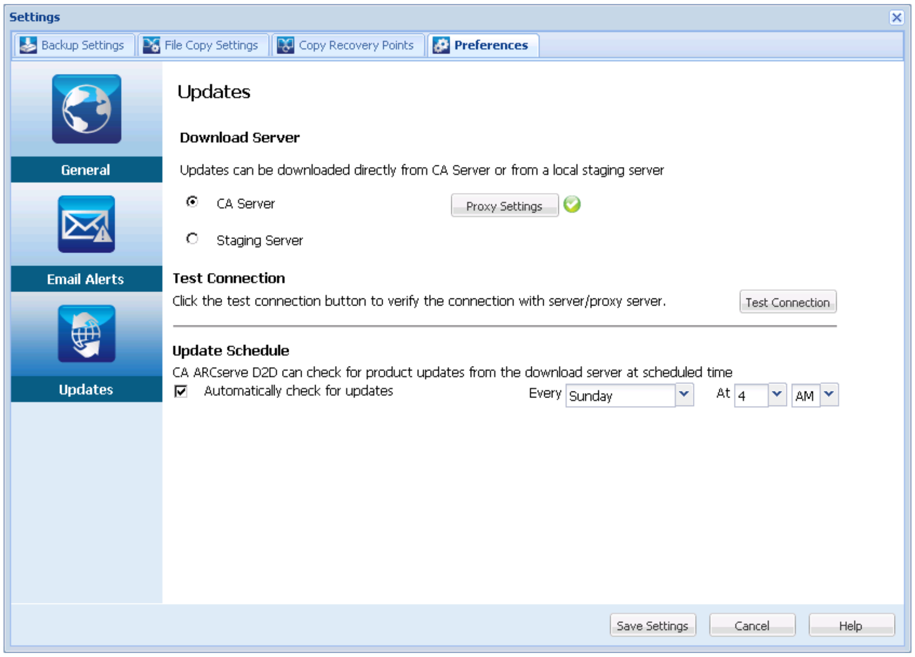
Specify Update Preferences

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.



Updates

Download Server

Updates can be downloaded directly from CA Server or from a local staging server

● CA Server

○ Staging Server

Test Connection

Click the test connection button to verify the connection with server/proxy server.

Update Schedule

CA ARCserve D2D can check for product updates from the download server at scheduled time

☑ Automatically check for updates Every Sunday At 4 AM

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**

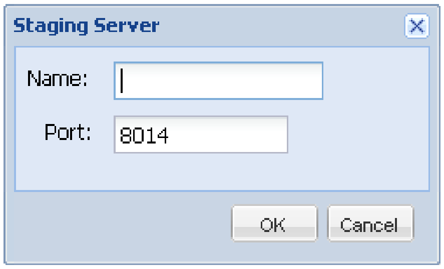
  You can use this option to specify the server that will be used as a staging server.

  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.



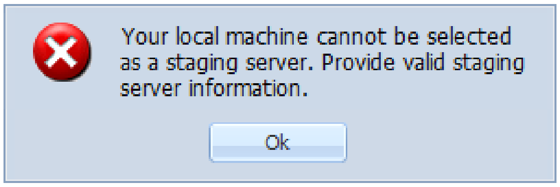
Staging Server

Name:

Port: 8014

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.

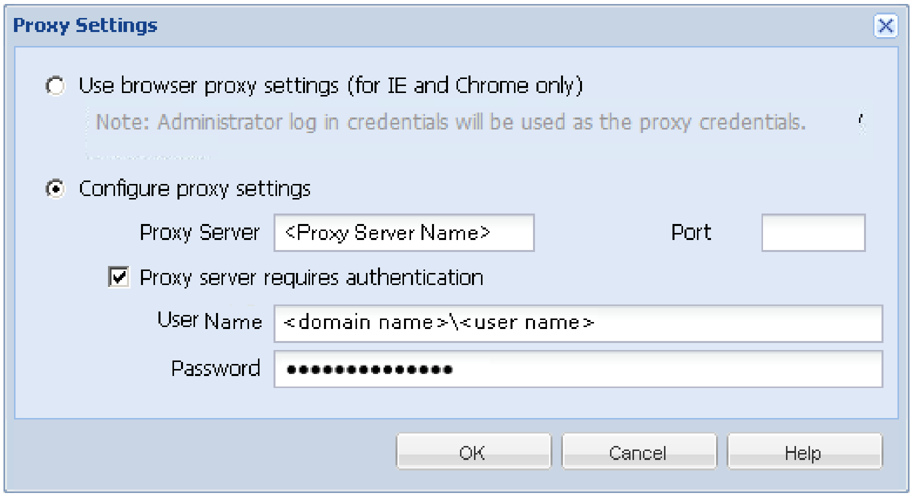
Note: You cannot download CA ARCserve D2D updates from a staging server if HTTPS is enabled on it for web communication.

- **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.



Proxy Settings

○ Use browser proxy settings (for IE and Chrome only)

Note: Administrator log in credentials will be used as the proxy credentials.

● Configure proxy settings

Proxy Server <Proxy Server Name> Port

☑ Proxy server requires authentication

User Name <domain name>\<user name>

Password ●●●●●●●●●●●●●●●

  - **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 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.

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 210)
- Microsoft SQL Server (see page 217)

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.

Videos

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.

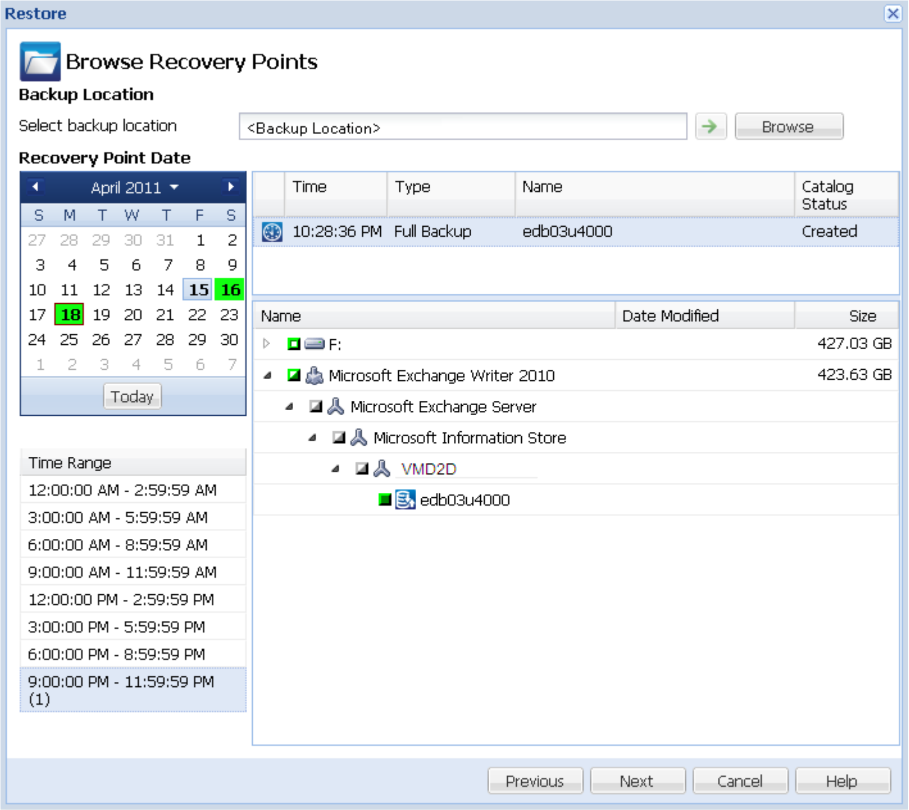
2. Click the Browse Recovery Points option.

   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.



Restore

Browse Recovery Points

Backup Location

Select backup location <Backup Location>

Recovery Point Date

April 2011

S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

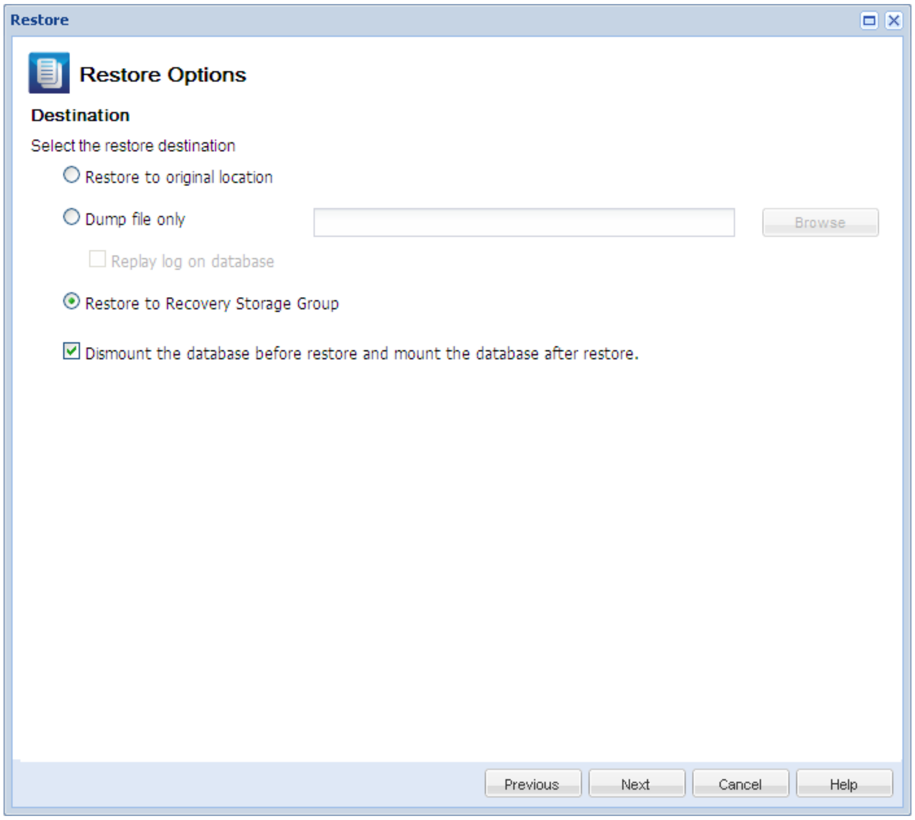
Time Range
12:00:00 AM - 2:59:59 AM
3:00:00 AM - 5:59:59 AM
6:00:00 AM - 8:59:59 AM
9:00:00 AM - 11:59:59 AM
12:00:00 PM - 2:59:59 PM
3:00:00 PM - 5:59:59 PM
6:00:00 PM - 8:59:59 PM
9:00:00 PM - 11:59:59 PM (1)

Time	Type	Name	Catalog Status
10:28:36 PM	Full Backup	edb03u4000	Created

Name	Date Modified	Size
F:		427.03 GB
Microsoft Exchange Writer 2010		423.63 GB
Microsoft Exchange Server		
Microsoft Information Store		
VMD2D		
edb03u4000		

4. Click Next.

   The Restore Options dialog opens.



Restore

Restore Options

Destination

Select the restore destination

○ Restore to original location

○ Dump file only

□ Replay log on database

● Restore to Recovery Storage Group

☑ Dismount the database before restore and mount the database after restore.

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)

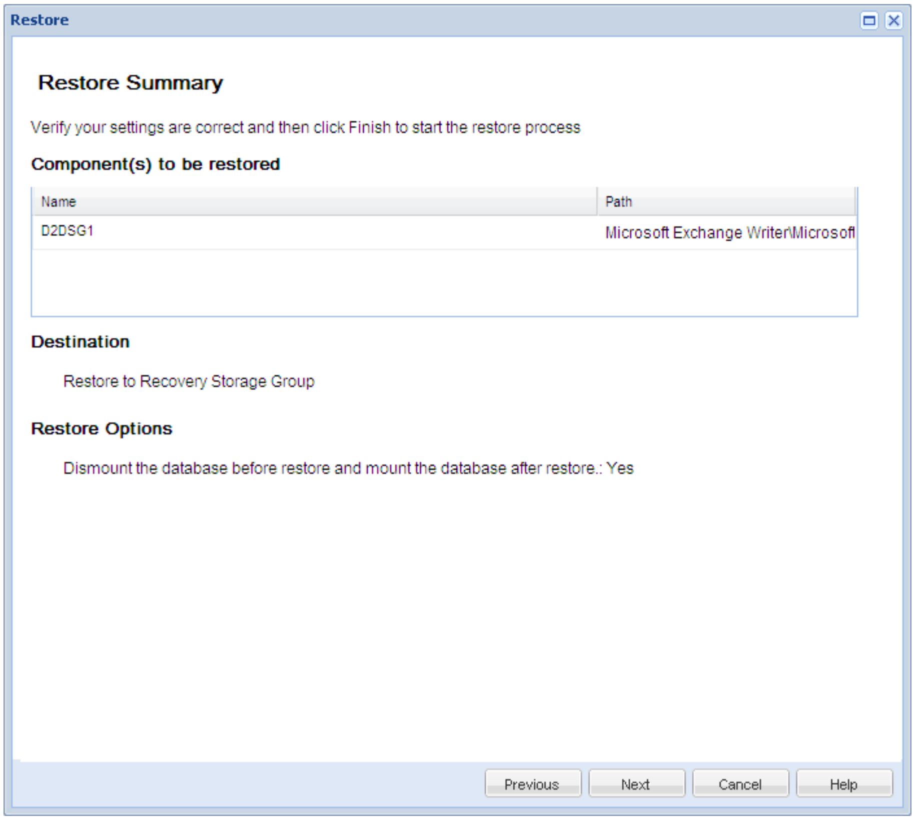
Restores the database to a Recovery Database. A Recovery Database is a database that can be used for recovery purposes. You can restore a Microsoft Exchange Mailbox Database from a backup to a Recovery Database and then recover and extract data from it, without affecting the production database that 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.



Restore

Restore Summary

Verify your settings are correct and then click Finish to start the restore process

Component(s) to be restored

Name	Path
D2DSG1	Microsoft Exchange Writer\Microsoft

Destination

Restore to Recovery Storage Group

Restore Options

Dismount the database before restore and mount the database after restore.: Yes

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.

Videos

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.

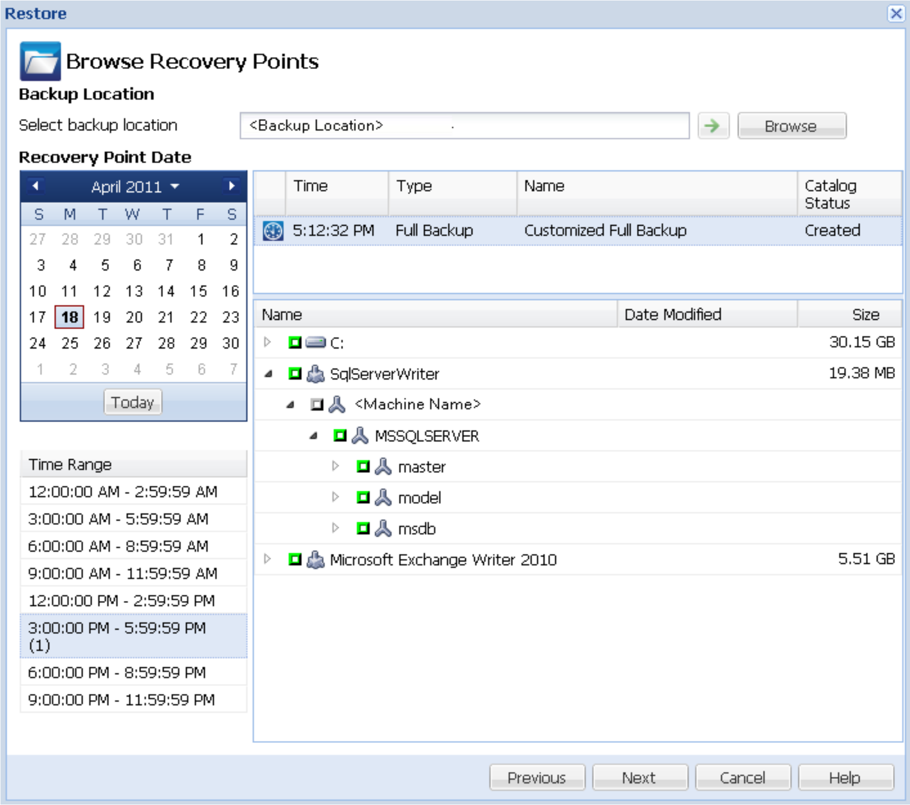
   The restore methods selection dialog opens.

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.



Backup Location

Select backup location <Backup Location>

Recovery Point Date

April 2011

S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

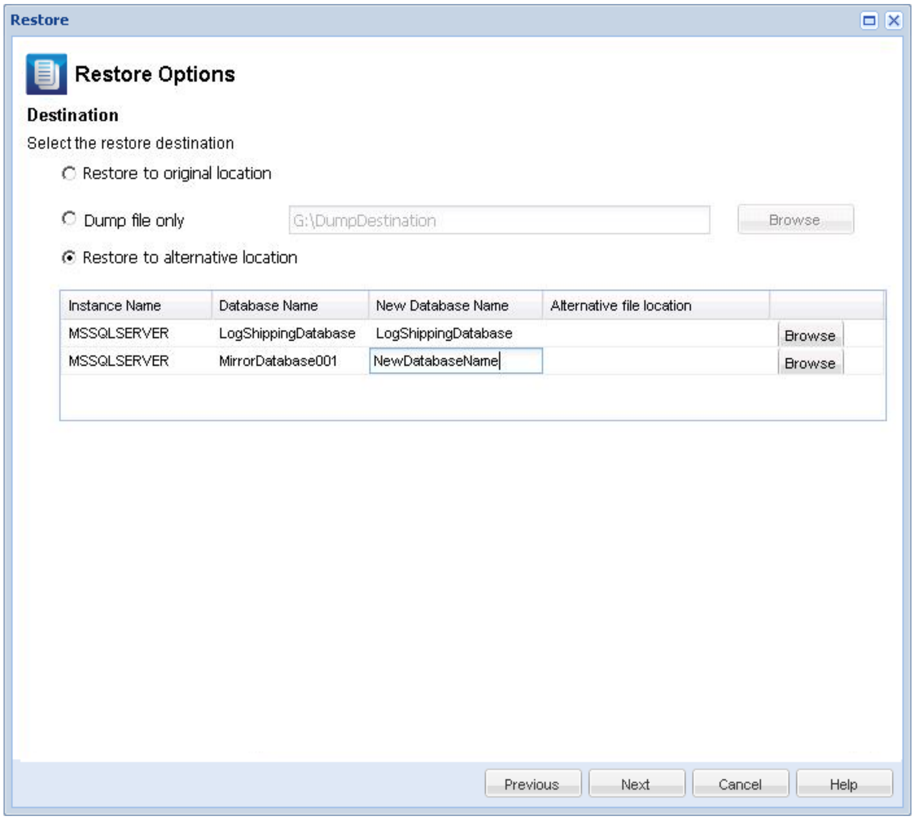
Time Range
12:00:00 AM - 2:59:59 AM
3:00:00 AM - 5:59:59 AM
6:00:00 AM - 8:59:59 AM
9:00:00 AM - 11:59:59 AM
12:00:00 PM - 2:59:59 PM
3:00:00 PM - 5:59:59 PM (1)
6:00:00 PM - 8:59:59 PM
9:00:00 PM - 11:59:59 PM

Time	Type	Name	Catalog Status
5:12:32 PM	Full Backup	Customized Full Backup	Created

Name	Date Modified	Size
C:		30.15 GB
SqlServerWriter		19.38 MB
<Machine Name>		
MSSQLSERVER		
master		
model		
msdb		
Microsoft Exchange Writer 2010		5.51 GB

4. Click Next.

   The Restore Options dialog opens.



Restore

Restore Options

Destination

Select the restore destination

○ Restore to original location

○ Dump file only G:\DumpDestination

● Restore to alternative location

Instance Name	Database Name	New Database Name	Alternative file location	
MSSQLSERVER	LogShippingDatabase	LogShippingDatabase		Browse
MSSQLSERVER	MirrorDatabase001	NewDatabaseName		Browse

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.

   Restore to original location

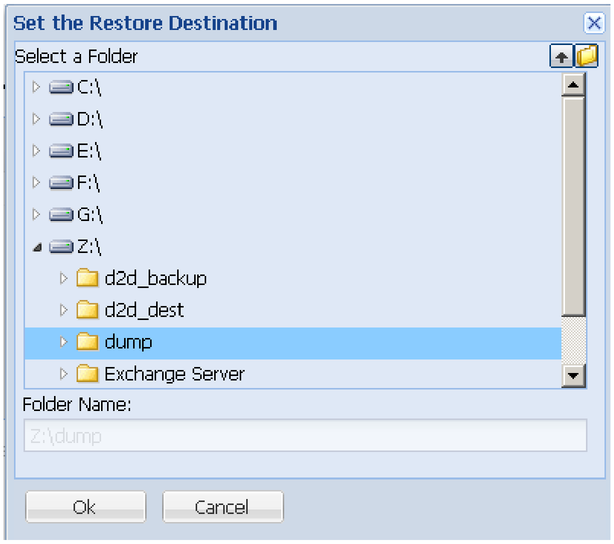
   Restores to the original location from where the backup image was captured.

   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.

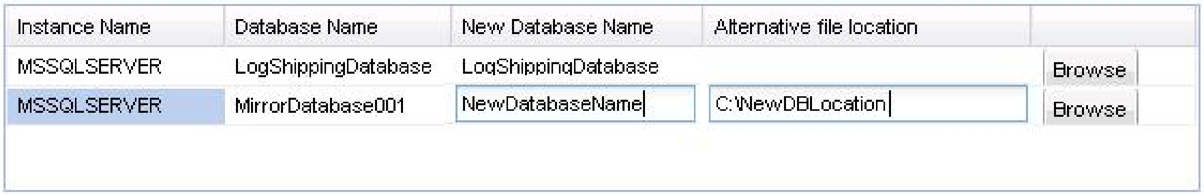


Set the Restore Destination

Folder Name: Z:\dump

Restore to alternate location

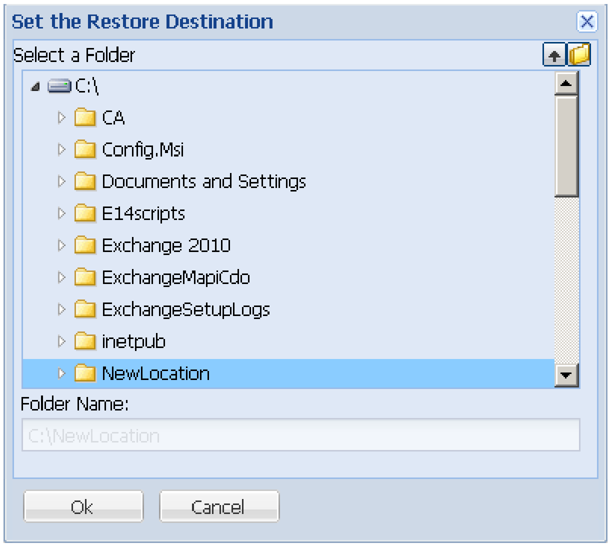
Restores to an alternate location (not the original location).



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 221).



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.

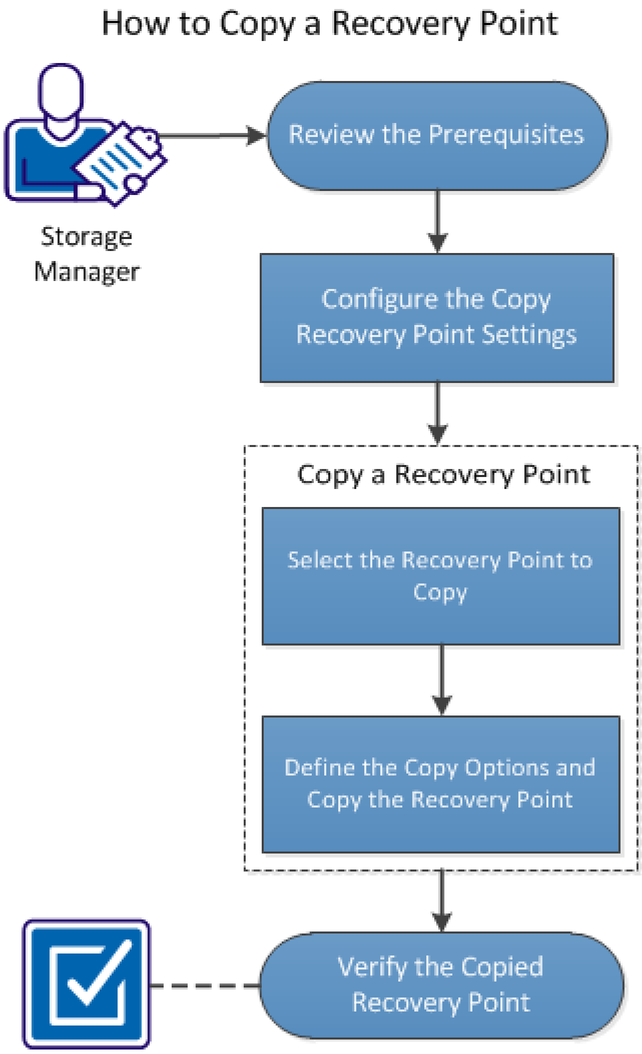
  For example, you can restore a SQL Server 2005 machine to a SQL Server 2008 machine; however, you cannot restore a SQL Server 2008 machine to a SQL Server 2005 machine.

- Restoring a database of 64-bit instance to 32-bit instance is not supported.

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:


How to Copy a Recovery Point
Storage Manager
Review the Prerequisites
Configure the Copy Recovery Point Settings
Copy a Recovery Point
Select the Recovery Point to Copy
Define the Copy Options and Copy the Recovery Point
Verify the Copied Recovery Point

Perform the following tasks to copy a recovery point:

1. Review the Prerequisites (see page 225)
2. Configure the Copy Recovery Point Settings (see page 225)
3. Copy a Recovery Point (see page 230)
   a. Select the Recovery Point to Copy (see page 230)
   b. Define the Copy Options and Copy the Recovery Point (see page 232)
4. Verify the Copied Recovery Point (see page 234)

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.

Videos

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 228).

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.

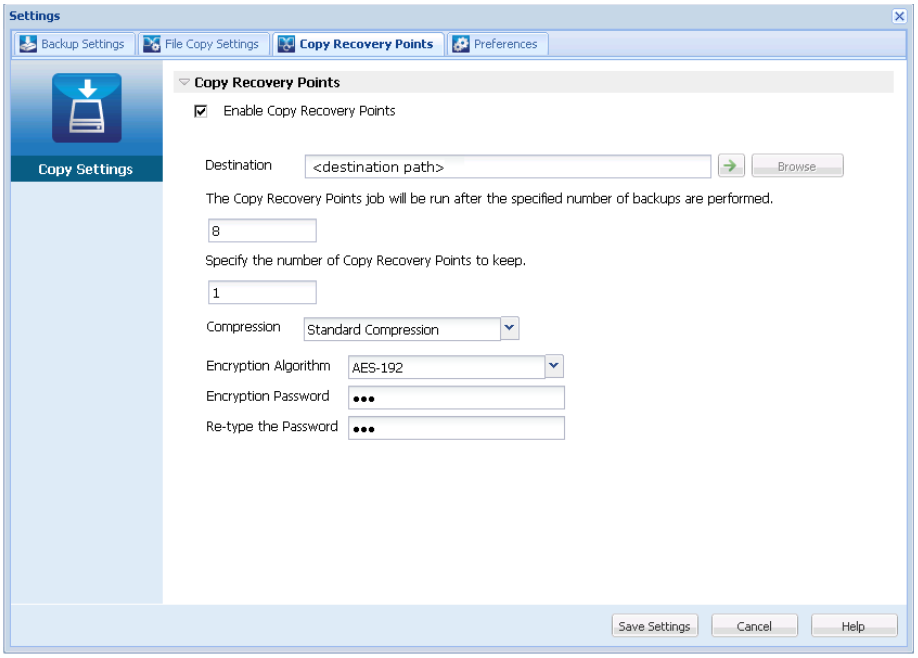
Follow these steps:

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.



Copy Recovery Points

☑ Enable Copy Recovery Points

Destination <destination path>

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

8

Specify the number of Copy Recovery Points to keep.

1

Compression Standard Compression

Encryption Algorithm AES-192

Encryption Password •••

Re-type the Password •••

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 230).
2. Define the Copy Options and Copy the Recovery Point (see page 232).

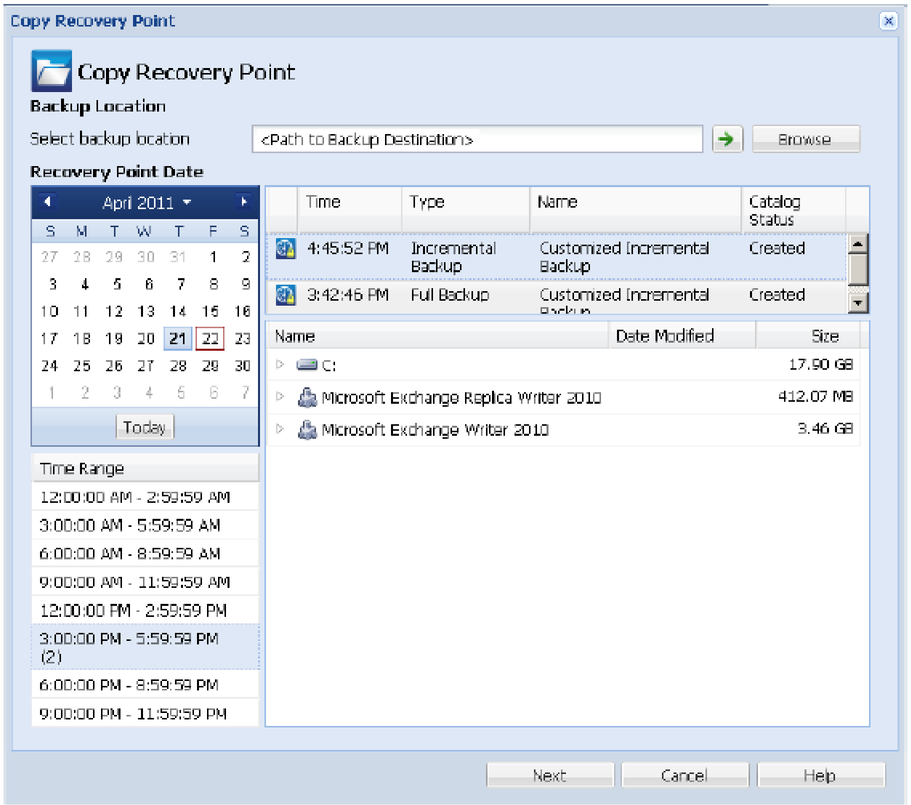
Select the Recovery Point to Copy

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.



Select backup location: <Path to Backup Destination>

April 2011

S	M	T	W	T	F	S
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Time Range
12:00:00 AM - 2:59:59 AM
3:00:00 AM - 5:59:59 AM
6:00:00 AM - 8:59:59 AM
9:00:00 AM - 11:59:59 AM
12:00:00 PM - 2:59:59 PM
3:00:00 PM - 5:59:59 PM (2)
6:00:00 PM - 8:59:59 PM
9:00:00 PM - 11:59:59 PM

Time	Type	Name	Catalog Status
4:45:52 PM	Incremental Backup	Customized Incremental Backup	Created
3:42:46 PM	Full Backup	Customized Incremental Backup	Created

Name	Date Modified	Size
C:		17.90 GB
Microsoft Exchange Replica Writer 2010		412.07 MB
Microsoft Exchange Writer 2010		3.46 GB

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.

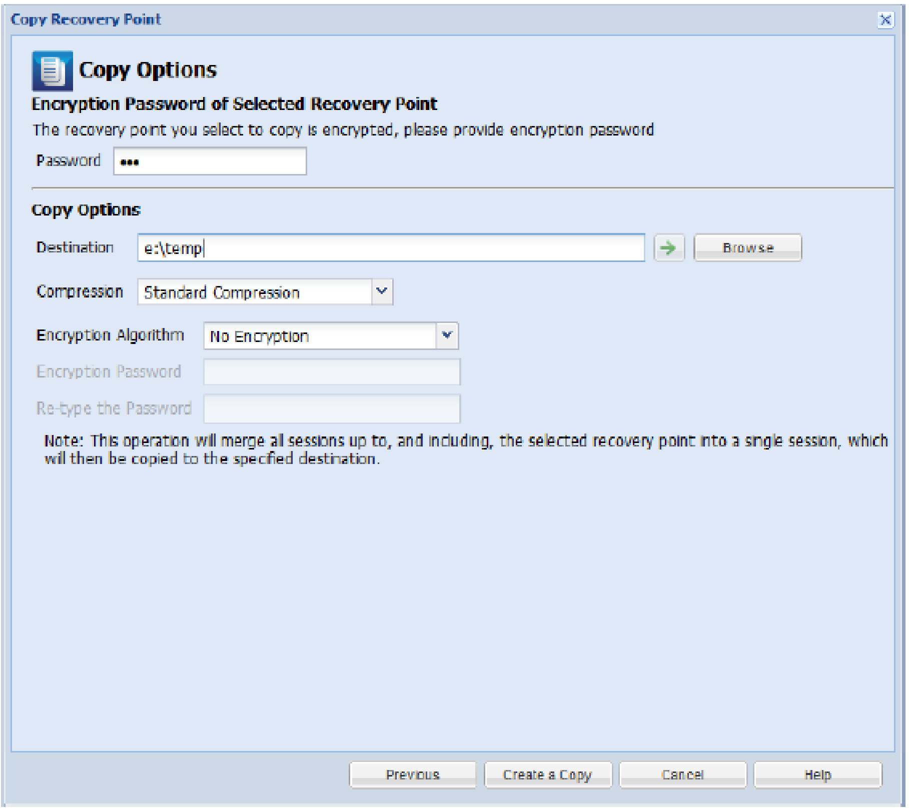
The recovery point to copy is specified.

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:



Copy Recovery Point

Copy Options

Encryption Password of Selected Recovery Point

The recovery point you select to copy is encrypted, please provide encryption password

Password: •••

Copy Options

Destination: e:\temp

Compression: Standard Compression

Encryption Algorithm: No Encryption

Encryption Password

Re-type the Password

Note: This operation will merge all sessions up to, and including, the selected recovery point into a single session, which will then be copied to the specified destination.

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.

Glossary

Auto Discovery

Auto discovery is a process by which nodes are detected and added to one or more CA ARCserve Central Applications for central management.

Backup Proxy

A backup proxy is the host computer on which CA ARCserve D2D is running. The proxy performs the back up operations configured in CA ARCserve Central Host-Based VM Backup.

Catalog File

A catalog file is a directory of information about the backup data contained within the CA ARCserve D2D database. For more information about the CA ARCserve D2D catalog file, see the *CA ARCserve D2D User Guide.*

HOTADD Transport Mode

The HOTADD transport mode is a data transport method that lets you back up virtual machines configured with SCSI disks. For more information, see the Virtual Disk API Programming Guide on the VMware website.

NBD Transport Mode

Network Block Device (NBD) transport mode, also referred to as LAN transport mode, uses the Network File Copy (NFC) protocol to communicate. Various VDDK and VCB operations use one connection for each virtual disk that it accesses on each ESX/ESXi Server host when using NBD.

NBDSSL Transport Mode

Network Block Device Secure Sockets Layer (NBDSSL) transport mode uses the Network File Copy (NFC) protocol to communicate. NBDSSL transfers encrypted data using TCP/IP communication networks.

Node

A node is a physical or virtual machine managed by one or more CA ARCserve Central Applications.

Node Group

A node group is a method by which all nodes managed by one or more CA ARCserve Central Applications can be organized, such as by purpose, by OS, or by installed applications.

Policy

A policy is a set of specifications for protecting a node in one or more CA ARCserve Central Applications.

Preflight Check

Preflight Check (PFC) is a utility that lets you run vital checks on nodes to detect conditions that can cause backup jobs to fail. You can view the results of the PFC for a node by clicking the icon in the PFC Status column on the Node screen.

Recovery Point

A recovery pointy is a backup image comprised of parent-plus-oldest-child blocks. Child backups are merged with the parent backup to create new recovery point images so that the value specified is always maintained.

SAN Transport Mode

The SAN (Storage Area Network) transport mode lets you transfer backup data from proxy systems connected to the SAN to storage devices using Fibre Channel communication.

SRM

Storage Resource Management (SRM) is a feature by which information is collected for effective management of your environment such as application data, hardware and software data, or performance key indicators.

Synchronization

Synchronization is the process by which data in different databases is kept up to date so that the central site database is consistent with registered branches, nodes, or sites.

Index