

CA ARCserve® Central Virtual Standby

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.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 6

- Updated [Deploy Policies](#) (see page 40). This topic now includes a note indicating that you can view the policy deployment status on the Node list screen under the Policy column.
- Updated [Update Nodes](#) (see page 50). 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 28). This topic replaces the "Unassigned" node group with "Nodes without a policy" and replaces the "Ungrouped" node group with "Nodes without a group".
- Updated [Power on Virtual Standby Virtual Machines from Recovery Point Snapshots](#) (see page 86). Updated this topic to include a new button named Standby VM on the Node Actions toolbar. This feature enables you to power on a virtual machine directly from the application.

Update 5

- Updated to include user feedback, enhancements, corrections, and other minor changes to help improve the usability and understanding of the product or the documentation itself.
- [Add Node Groups](#) (see page 28). Updated this topic to include Group and Node Name filters.
- [Assign Nodes to a Policy](#) (see page 38). Updated this topic to include Group and Node Name filters.
- [Update Nodes](#) (see page 50). Updated this topic to include various ways to update multiple nodes.
- [Unassign Nodes from Policies](#) (see page 66). Updated this topic to include Group and Node Name filters.

Update 4

- Updated [Deploy Policies](#) (see page 40) to include more information about how the deployment process affects nodes that you import from Host-Based VM Backup.
- Updated Pause and Resume Heartbeats to describe how to pause and resume heartbeats from the [Virtual Standby server](#) (see page 81) and [directly from the node](#) (see page 83).
- Updated Pause and Resume Virtual Standby jobs to describe how to pause and resume virtual standby jobs from the [Virtual Standby server](#) (see page 84) and [directly from the node](#) (see page 85).
- Updated [Restore Data from CA ARCserve D2D Recovery Points](#) (see page 102), [Restore Data from CA ARCserve D2D File Copies](#) (see page 107), [Restore Data Using Find Files/Folders to Restore](#) (see page 112), and [Restore Microsoft Exchange Email Messages](#) (see page 160). These topics describe how to restore data using the new Restore action on the toolbar.
- Added [Change Server Communication Protocol](#) (see page 167). This topic describes how to change the communication protocol used by the CA ARCserve Central Applications components from HTTP to HTTPS and from HTTPS to HTTP using a batch file.

Contents

Chapter 1: Introducing CA ARCserve Central Virtual Standby 11

Introduction	11
How CA ARCserve Central Virtual Standby Works	12
CA ARCserve Central Applications Bookshelf	14

Chapter 2: Installing CA ARCserve Central Virtual Standby 15

Prerequisite Installation Tasks	15
Installation Considerations.....	16
Install CA ARCserve Central Virtual Standby	17
Uninstall CA ARCserve Central Virtual Standby.....	19
Install CA ARCserve Central Virtual Standby Silently.....	20
Uninstall CA ARCserve Central Virtual Standby Silently	22

Chapter 3: Getting Started With CA ARCserve Central Virtual Standby 25

Verify That the CA ARCserve Central Virtual Standby Server Can Communicate With the Nodes	25
Log in to CA ARCserve Central Virtual Standby	26
Add Nodes by IP Address or Node Name	27
Add Node Groups	28
Specify the ESX Server or vCenter Server System for VMware-Based Nodes	29
Create Policies	30
Assign Nodes to a Policy	38
Deploy Policies	40

Chapter 4: Using CA ARCserve Central Virtual Standby 43

Log In to CA ARCserve D2D Nodes	43
Log in to Monitor Servers.....	44
Node Maintenance Tasks	45
Import Nodes from a File	46
Add Nodes from CA ARCserve Central Host-Based VM Backup Servers.....	48
Update Nodes	50
Delete Nodes.....	52
Release Licenses from Nodes.....	52
Stop Monitoring Nodes from the Monitor Server	54
Update Nodes and Policies After Changing the Host Name of the CA ARCserve Central Applications Server	54

Node Group Management Tasks.....	55
Modify Node Groups.....	55
Delete Node Groups.....	57
Filter Node Groups.....	57
Virtual Standby Policy Management Tasks	58
Edit or Copy Policies.....	58
Unassign Nodes from Policies	66
Delete Policies.....	67
Application Configuration Tasks.....	68
Configure Email Settings	68
Configure Automatic Updates.....	69
Configure Social Networking Preferences.....	72
Modify the Administrator Account	73
View Logs.....	74
Add Links to the Navigation Bar	75
Virtual Standby Home Page	75
How to Use the Virtual Standby Summary Screen.....	76
How to Use the Servers List	77
View Summary Information about the Latest Virtual Standby Job.....	77
Monitor the Status of Virtual Conversion Jobs	79
View Virtual Standby Settings for Source Servers.....	80
View the Recovery Point Snapshots List	80
CA ARCserve Central Virtual Standby Monitoring Tasks	81
Pause and Resume Heartbeats from the Virtual Standby Server	81
Pause and Resume Virtual Standby Jobs from the Virtual Standby Server.....	84
Power on Virtual Standby Virtual Machines from Recovery Point Snapshots	86
View Activity Log Data about Jobs	89
View Status Information About Virtual Standby Jobs from the Virtual Standby Server	92
View Information About Policies Assigned to CA ARCserve D2D Nodes.....	95
How to Protect Virtual Standby Virtual Machines	100
Restore Data from CA ARCserve D2D Recovery Points.....	102
Restore Data from CA ARCserve D2D File Copies	107
Restore Data Using Find Files/Folders to Restore	112
Recovering Source Servers Using Bare Metal Recovery.....	116
Recover Source Servers Using CA ARCserve D2D Backup Data	118
Recover Source Servers Using Data from Hyper-V Virtual Standby Virtual Machines.....	133
Recover Source Servers Using Data From VMware Virtual Standby Virtual Machines.....	146
Restore Microsoft Exchange Email Messages	160
Change Server Communication Protocol	167

Chapter 5: Troubleshooting CA ARCserve Central Virtual Standby **169**

Cannot Connect to Specified Server Messages Appear When Attempting to Add Nodes.....	170
Blank Webpages Appear or Javascript Errors Occur	172
How to Troubleshoot Page Loading Problems	174
Web Pages Do Not Load Properly When Logging in to CA ARCserve D2D Nodes and Monitoring Servers	175
Garbage Characters Appear in Browser Windows When Accessing CA ARCserve Central Applications	176
CA ARCserve D2D Web Service Fails on CA ARCserve D2D Nodes	177
The CA ARCserve D2D Web Service Runs Slowly	180
CA ARCserve Central Virtual Standby Cannot Communicate with the CA ARCserve D2D Web Service on Remote Nodes.....	182
Certificate Error Appears When You Log In to the Application	183
Invalid Credentials Message Appears When Adding Nodes	184
Invalid Credentials Messages on Windows XP	185
Access Denied Errors Occur when Adding a Node by IP/Name	185
Nodes Do Not Appear on the Node Screen After Changing the Name of the Node.....	187
Operating System Not Found Errors Occur	187
Virtual Standby Jobs to Hyper-V Systems Fail	188
Virtual Standby Jobs Fail Due to Internal Errors.....	188
Virtual Standby Jobs Fail Using the hotadd Transport Mode.....	191
Virtual Standby Jobs End with No Sessions Warning Messages.....	192
Backup and Recovery Jobs Do Not Use the SAN Transport Mode	193
Backup and Recovery Jobs Using the hotadd Transport Mode Cannot Mount Disks	194
Troubleshooting Error Numbers	195
Add New Tab Link Not Launching Properly for Internet Explorer 8, 9, and Chrome	195
Add New Tab Link, RSS Feeds, and Social Networking Feedback Not Launching Properly on Internet Explorer 8 and 9	197
Cannot Specify an Asterisk or Underscore as a Wildcard in Filter Fields Using Japanese Keyboards	198
Virtual Machines Do Not Power On Automatically	198

Chapter 6: Applying Best Practices **199**

How the Installation Process Affects Operating Systems	199
Binary Files Containing Incorrect File Version Information.....	201
Binary Files that Do Not Contain an Embedded Manifest	201
Binary Files that have a Privilege Level of Require Administrator in Manifest	202
How CA ARCserve Central Virtual Standby Licensing Works.....	204

Glossary **207**

Index **209**

Chapter 1: Introducing CA ARCserve Central Virtual Standby

This section contains the following topics:

[Introduction](#) (see page 11)

[How CA ARCserve Central Virtual Standby Works](#) (see page 12)

[CA ARCserve Central Applications Bookshelf](#) (see page 14)

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.

Among the applications offered by CA ARCserve Central Applications is CA ARCserve Central Virtual Standby. CA ARCserve Central Virtual Standby integrates with CA ARCserve D2D and lets you provision virtual machines from CA ARCserve D2D backup sessions. The application lets you do the following:

- Convert CA ARCserve D2D recovery points that are stored on the CA ARCserve D2D destination devices to VMware Virtual Disk (VMDK) or Microsoft Virtual Hard Disk (VHD) formats based on a schedule. From the recovery point snapshots you can allow the virtual machines to function as CA ARCserve D2D source servers in the event that your source servers fail.
- Push conversion policies to CA ARCserve D2D source servers.
- Store recovery point snapshots on VMware ESX Server-based or Windows Hyper-V-based virtual machines.
- Power on virtual machines manually or automatically if an emergency situation occurs.
- Recover data from recovery point snapshots to the original or alternate source servers (V2P recoveries).

How CA ARCserve Central Virtual Standby Works

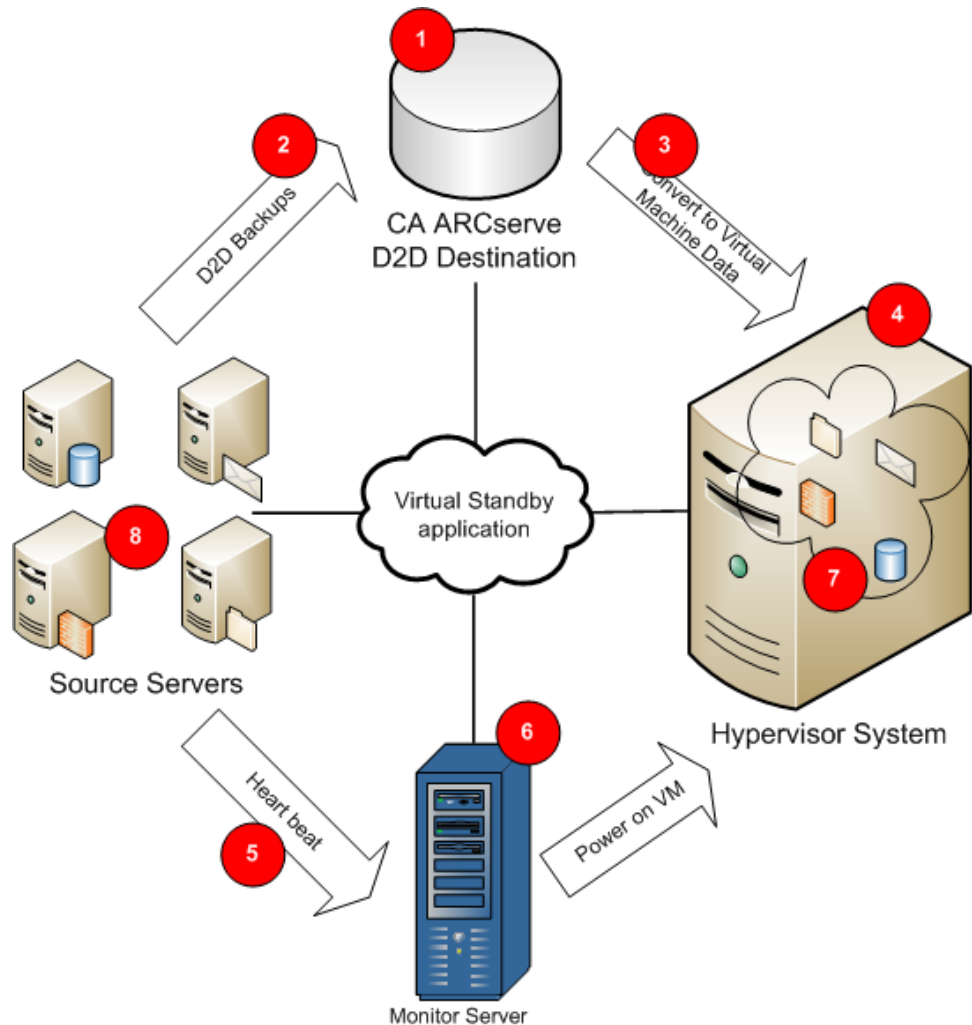
Virtual Standby lets you protect the CA ARCserve D2D source servers functioning in your environment by doing the following:

- Convert CA ARCserve D2D recovery points that are stored on the CA ARCserve D2D destination devices to VMware Virtual Disk (VMDK) or Microsoft Virtual Hard Disk (VHD) formats based on a schedule.
- Copy the converted data to a hypervisor system.
- Create recovery point snapshots from the virtual machine VMDK or VHD data.
- Monitor the health of the source server.
- Power on virtual machines automatically from the recovery point snapshots upon detection of an emergency.

Note: Virtual Standby can be configured to power on recovery point snapshots automatically or manually when a problem occurs.

- Recover the data from the virtual machine to the source server, after you correct the problems on the source server.

The following diagram illustrates this process:



CA ARCserve D2D (1) creates recovery points on the CA ARCserve D2D destination device (2) for the source servers. Virtual Standby converts the recovery points to virtual machine format (3) and stores the data as recovery point snapshots on the hypervisor system (4).

The monitor server (6) monitors the health of source servers. If the monitor server cannot detect a heartbeat (5) from a source server (8), the monitor server powers on a thin-provisioned virtual machine (7) on the hypervisor system (4) to function as the source server using data contained in the most recent Recovery Point Snapshot. CA ARCserve Central Virtual Standby creates a virtual machine partition that is the same size as the source server.

After you correct the problems on the source server, you can recover the source server (8) to its current state using the data (7) that is stored in the VM on the hypervisor system.

Note: If you want to back up the virtual machine after it is powered on, you can deploy a CA ARCserve D2D backup policy to the virtual machine using CA ARCserve Central Protection Manager.

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 CA ARCserve Central Virtual Standby

This section contains the following topics:

[Prerequisite Installation Tasks](#) (see page 15)

[Installation Considerations](#) (see page 16)

[Install CA ARCserve Central Virtual Standby](#) (see page 17)

[Uninstall CA ARCserve Central Virtual Standby](#) (see page 19)

[Install CA ARCserve Central Virtual Standby Silently](#) (see page 20)

[Uninstall CA ARCserve Central Virtual Standby Silently](#) (see page 22)

Prerequisite Installation Tasks

Before you install CA ARCserve Central Virtual Standby, complete the following prerequisite tasks:

- Verify that the latest supported release of CA ARCserve D2D is installed on the following:

- The source servers that you want to protect
- The server that you designate to store recovery point snapshots

Note: This requirement applies to only to Hyper-V servers that are configured to monitor the health of nodes (physical or virtual machine), and to store the recovery point snapshots for the nodes.

- The server that you designate to monitor the source servers

Note: If you installed CA ARCserve Central Protection Manager in your production environment, you can install CA ARCserve D2D on remote nodes using D2D Deployment. For more information, see the CA ARCserve Central Protection Manager User Guide.

- In Hyper-V environments, verify that CA ARCserve D2D is installed on the Hyper-V host system. In Hyper-V environments, Hyper-V host systems function as the storage location for recovery point snapshots and as the monitor server.
- In VMware environments, verify that CA ARCserve D2D is installed on the proxy system.

Note: In VMware environments, the target ESX Server data store functions as the storage location for recovery point snapshots. The proxy system can optionally function as the monitor server.

- Review the Release Notes file. The Release Notes file contains a description of system requirements, supported operating systems, and a list of issues that are known to exist with this release.
- Verify that your system meets the minimum software and hardware requirements that are required to install CA ARCserve Central Virtual Standby.
- 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 Virtual Standby.
- Verify that your account has VMware vCenter or ESX Server administrative privileges and Windows administrative privileges. The account requires 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 CA ARCserve Central Virtual Standby in your possession.
- Verify that you have the host names or IP address of the computers that you want to monitor the source computers in your possession.
- Verify that you have the host names or IP address of the computers where you want to store recovery point snapshots in your possession.
- Verify that you have all the licenses that are required to install CA ARCserve Central Virtual Standby available to you.
- Verify that the CA ARCserve D2D release number is the same release number as CA ARCserve Central Virtual Standby.

Installation Considerations

Before you install CA ARCserve Central Virtual Standby, 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.

- 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 Virtual Standby 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

- CA ARCserve Central Virtual Standby does not support creating virtual disk images on compressed volumes and volumes that are encrypted by the file system.

Note: This limitation applies to only Hyper-V hypervisors.

- CA ARCserve Central Virtual Standby does not support protecting VMware virtual machines that are named using JIS2004 Unicode characters.
- CA ARCserve Central Virtual Standby does not support protecting virtual machines that have a disk size that is greater than two terabytes.

Install CA ARCserve Central Virtual Standby

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 Virtual Standby

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.

The installation process executes.

After the installation process completes, the Installation Report dialog 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.

Uninstall CA ARCserve Central Virtual Standby

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

Follow these steps:

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.

Install CA ARCserve Central Virtual Standby Silently

CA ARCserve Central Applications lets you install CA ARCserve Central Virtual Standby 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 Virtual Standby 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.

Uninstall CA ARCserve Central Virtual Standby Silently

CA ARCserve Central Applications lets you uninstall CA ARCserve Central Virtual Standby silently. A silent installation eliminates the need for user interaction. The following steps describe how to uninstall the application using Windows Command Line.

Follow these steps:

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 Virtual Standby silently.

```
"%ProgramFiles%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p  
{CAED4835-964B-484B-A395-E2DF12E6F73D}
```

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.

Chapter 3: Getting Started With CA ARCserve Central Virtual Standby

The following sections describe how to configure CA ARCserve Central Virtual Standby to protect CA ARCserve D2D nodes.

Note: Before you can complete the configurations described in this section, verify that all [Prerequisite Installation Tasks](#) (see page 15) are complete.

This section contains the following topics:

[Verify That the CA ARCserve Central Virtual Standby Server Can Communicate With the Nodes](#) (see page 25)

[Log in to CA ARCserve Central Virtual Standby](#) (see page 26)

[Add Nodes by IP Address or Node Name](#) (see page 27)

[Add Node Groups](#) (see page 28)

[Specify the ESX Server or vCenter Server System for VMware-Based Nodes](#) (see page 29)

[Create Policies](#) (see page 30)

[Assign Nodes to a Policy](#) (see page 38)

[Deploy Policies](#) (see page 40)

Verify That the CA ARCserve Central Virtual Standby Server Can Communicate With the Nodes

Note: This is an optional step to configuring CA ARCserve Central Virtual Standby to protect nodes.

To help ensure that CA ARCserve Central Virtual Standby can deploy policies to nodes and protect nodes, verify that the Virtual Standby server and the nodes that you want to protect can communicate with each other using their host names.

To verify that the CA ARCserve Central Virtual Standby server can communicate with the nodes

1. From the CA ARCserve Central Virtual Standby server, ping the nodes that you want to protect using the host names of the nodes.
2. From the nodes that you want to protect, ping the CA ARCserve Central Virtual Standby server using the host name of the server.

Log in to CA ARCserve Central Virtual Standby

You can log in to CA ARCserve Central Virtual Standby directly from the computer where the application is installed or from a remote computer using a supported browser. For a complete list of the supported browsers, see the *CA ARCserve Central Virtual Standby Release Notes*.

To log in to CA ARCserve Central Virtual Standby

1. Do one of the following options:

- If you are logged in to the server where CA ARCserve Central Virtual Standby is installed; launch the application from your program files.

A browser window opens and displays the CA ARCserve Central Virtual Standby login screen.

Complete the following fields on the login screen:

- Username
- Password

Click Login.

- If you are not logged in to the server where CA ARCserve Central Virtual Standby is installed; open a browser window and specify the following url in the address bar:

`http://<CA ARCserve Central Application Server Name>:<Port Number>/virtualstandby/`

Note: You can specify the host name or the IP address of the server when CA ARCserve Central Virtual Standby is installed. The default port is 8015.

Press Enter.

A browser window opens and displays the CA ARCserve Central Virtual Standby login screen.

Complete the following fields on the login screen:

- Username
- Password

Click Login.

You are logged in to CA ARCserve Central Virtual Standby and the home page opens.

Add Nodes by IP Address or Node Name

Virtual Standby lets you add nodes based on the IP address or the node name. Add the CA ARCserve D2D source nodes that you want to protect.

To add nodes by IP address or node name

1. From the home page, select Node on the Navigation bar.
The Node screen displays.
2. From the Node toolbar, click Add, and then click Add Node by IP/Name on the pop-up menu.
The Add Node by IP/Name dialog opens.
3. Complete the following fields on the Add Node by IP/Name dialog:
 - **IP/Node Name**--Lets you specify the IP address or the name of the node.
 - **Description**--Lets you specify a description for the node.
 - **Username**--Lets you specify the user name that is required to log in to the node.
 - **Password**--Lets you specify the password that is required to log in to the node.Click OK.
4. (Optional) If the newly added node does not appear in the nodes list, click Refresh on the Node toolbar.

The Add Node by IP/Name dialog closes and the node is added.

Add Node Groups

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.

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.

Specify the ESX Server or vCenter Server System for VMware-Based Nodes

Note: The following procedure applies to only VMware-based virtual machine source nodes.

In various VMware-based implementations, Virtual Standby may not be able to detect source nodes that are configured as virtual machines that reside on ESX Server and vCenter Server systems. This behavior prevents Virtual Standby from applying the correct license to the nodes, deploying policies to the nodes, and executing conversion jobs.

The procedure that follows lets you specify the host name or IP address of the ESX Server or vCenter Server system where the nodes reside. After you complete the procedure, Virtual Standby can detect, apply licenses, deploy policies, and execute conversion jobs for nodes that you want to protect. If there are multiple virtual machines that reside on one ESX Server or vCenter Server system that act as one source node, the procedure lets you consume one license for all of the nodes, which helps to reduce the overall cost of protecting the source nodes.

To specify the ESX Server or vCenter Server system for VMware-based nodes

1. Log in to the application.

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

The Node screen displays.

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

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

3. Click the node that you want to update and then click Specify ESX Server from the pop-up menu.

The Specify ESX Server dialog opens.

Note: If the application detects that VMware Tools is not installed on the virtual machine that is managed by either an ESX Server or vCenter Server system, the virtual machine resides on a Hyper-V system, or the node detected is not a virtual machine, an error message appears.

4. Complete the following fields on the Specify ESX Server dialog:

- ESX/vCenter Host

Note: Specify the host name or the IP address of the ESX Server or vCenter Server system.

- User Name

- Password

- Port

Note: The default communication port is 443. If the node communicates with the ESX Server or the vCenter Server system using a different port number, specify the port number that is used.

- Protocol

Note: The default communication protocol is HTTPS. If the node communicates with the ESX Server or the vCenter Server system using HTTP, click HTTP.

Click OK.

The ESX Server or vCenter Server system is assigned to the node.

Create Policies

Virtual Standby lets you define custom conversion policies that you assign to CA ARCserve D2D nodes.

Note: To create policies, CA ARCserve D2D must be installed on the monitor server.

To create policies

1. Log in to the Virtual Standby server and open Virtual Standby.

From the Navigation bar on the home page, click Policies.

The Policy window opens.

2. Click New on the Policies toolbar.

The New Policies dialog opens.

3. In Policy Name field, specify a name for the policy.

Click the Virtual Standby tab.

The Virtualization Server, Virtual Machine, and Stand-in Settings options display.

4. Click Virtualization Server.

The Virtualization Server options appear.

5. Complete the following Virtualization Server options:

VMware Systems:

- **Virtualization type**--Click VMware.
- **ESX Host/vCenter**--Specify the host name of the ESX or vCenter Server system.
- **User Name**--Specify the user name that is required to log in to the VMware system.

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

- **Password**--Specify the password for the User Name that is required to log in to the VMware system.
- **Protocol**--Specify HTTP or HTTPS as the protocol that you want to use for communication between the source CA ARCserve D2D node and the monitoring server.
- **Port**--Specify the port that you want to use for data transfer between the source server and the monitoring server.
- **ESX Node**--The values in this field vary based on the value specified in the ESX Host/vCenter field:
 - **ESX Server systems**--When you specify an ESX Server system in the ESX Host/vCenter field, this field displays the host name of the ESX Server system.
 - **vCenter Server systems**--When you specify a vCenter Server system the ESX Host/vCenter field, this field lets you specify (from a drop-down list) the ESX Server system that you want to associate with this policy.
- **Monitor Server**--Specify the host name of the server that you want to monitor the status of the source server.

Note: The monitor server can be any physical computer or virtual machine provided that server is not functioning as the proxy server for a CA ARCserve Central Host-Based VM Backup implementation.

- **User Name**--Specify the user name that is required to log in to the monitoring system.
- **Password**--Specify the password for the User Name that is required to log in to the monitoring system.
- **Protocol**--Specify HTTP or HTTPS as the protocol that you want to use for communication between the CA ARCserve Central Virtual Standby server and the ESX Server system (monitoring server).

- **Port**--Specify the port that you want to use for data transfer between the CA ARCserve Central Virtual Standby server and the ESX Server system (monitoring server).
- **Use monitor server as proxy for data transfer**--Specify this option to let the monitor server copy the conversion data from the CA ARCserve D2D source node to the ESX Server datastore. With this option enabled, Virtual Standby transfers the conversion data from the source node to the ESX Server datastore using fibre channel communication, which is faster than using LAN communication to transfer data.

Note: The Use monitor server as proxy for data transfer option is enabled by default. You can disable this option to allow the CA ARCserve D2D source server to copy the conversion data directly to the datastore on the ESX Server system.

Hyper-V Systems:

- **Virtualization type**--Click Hyper-V.

Note: When you click Hyper-V, the Monitoring options are not accessible. The Monitoring options behave in this manner because the Hyper-V server assumes the role of the Monitor server.

- **Hyper-V Host Name**--Specify the host name of the Hyper-V system.

- **User Name**--Specify the user name that is required to log in to the Hyper-V system.

Note: The account that you specify must be an administrative account or an account with administrative privileges on the Hyper-V system.

- **Password**--Specify the password for the User Name that is required to log in to the Hyper-V system.

- **Port**--Specify the port that you want to use for data transfer between the source server and the monitoring server.

- **Monitor Server**--Specify the host name of the server that you want to monitor the status of the source server.

- **User Name**--Specify the user name that is required to log in to the monitoring system.

- **Password**--Specify the password for the User Name that is required to log in to the monitoring system.

- **Protocol**--Specify HTTP or HTTPS as the protocol that you want to use for communication between the CA ARCserve Central Virtual Standby server and the Hyper-V Server system (monitoring server).

- **Port**--Specify the port that you want to use for data transfer between the CA ARCserve Central Virtual Standby server and the Hyper-V Server system (monitoring server).

Click Virtual Machine.

The Virtual Machine options appear.

6. Complete the following Virtual Machine options:

VMware Systems:

Apply the following Virtual Machine options to VMware systems:

- **VM Name Prefix**--Specify the prefix that you want to add to the display name for the virtual machine on the ESX Server system.
Default value: CAVM_
- **VM Resource Pool**--Specify the name of resource pool where standby virtual machine is to be grouped.
- **CPU Count**--Specify the minimum and maximum CPU count supported by the standby virtual machine.
- **Memory**--Specify the total amount of RAM in MB to be allocated for the standby virtual machine.
Note: The amount of RAM specified must be a multiple of two.
- **VM Datastore**--Specify the location where you want to store the conversion data.
 - **Specify one datastore for all virtual disks**--Lets the application copy all of the disks related to the virtual machine to one data store.
 - **Specify a datastore for each virtual disk**--Lets the application copy disk related information for the virtual machine to the corresponding datastore.
- **VM Network**--Lets you define the NICs, virtual networks, and paths that the ESX Server system uses to communicate with the virtual machines.
 - **Specify a network adapter type for each NIC and connect the network adapter to the following virtual network**--Lets you define how to map the virtual NIC to the virtual network. Specify this option when the virtual machine contains virtual NICs and a virtual network.
 - **Specify a network adapter type and a virtual network for each NIC**--Lets you define the name of the virtual network that you want the NIC to use to communicate.

Hyper-V Systems:

Apply the following Virtual Machine options to Hyper-V systems:

- **VM Basic Settings**--Complete the following VM Basic settings:
 - **VM Name Prefix**--Specify the prefix that you want to add to the display name for the virtual machine on the Hyper-V system.
Default value: CAVM_
 - **CPU Count**--Specify the minimum and maximum CPU count supported by the standby virtual system.
 - **Memory**--Specify the total amount of RAM in MB to be allocated to the standby virtual machine.
Note: The amount of RAM specified must be a multiple of four.
- **VM Path**--Specify one of the following VM Path options:
 - **Specify one path for all virtual disks**--Specify the location on the Hyper-v server where you want to store the conversion data.
 - **Specify a path for each virtual disk**--Specify the location on the Hyper-V server where you want to store the conversion data for each virtual disk.
Note: CA ARCserve Central Virtual Standby does not support creating virtual disk images (VHD files) on compressed volumes and volumes that are encrypted by the file system. If the path specified resides on compressed or encrypted Hyper-V volumes, Virtual Standby prevents you from creating the policy.
- **VM Network**--Lets you define the NICs, virtual networks, and paths that the Hyper-V server uses to communicate with the virtual machines. Specify one of the following options and complete the required fields.
 - **Specify a network adapter type for each NIC and connect the network adapter to the following network**--Lets you define how to map the virtual NIC to the virtual network. Specify this option when the virtual machine contains virtual NICs and a virtual network.
 - **Specify a network adapter type and a virtual network for each NIC**--Lets you define the name of the virtual network that you want the NIC to use to communicate.

Click Stand-in Settings.

The Stand-in Settings options appear.

7. Complete the following Stand-in Settings options:

Recovery:

Select one of the following methods:

- **Manually start the Virtual Machine**--Lets you power on and provision virtual machines manually when the source server fails or stops communicating. Specify this option when you prefer to analyze the cause of the failure before you provision the virtual machines and allow the servers to function as source servers.
- **Automatically start the Virtual Machine**--Lets you power on and provision virtual machines automatically when the source server fails or stops communicating. Specify this option when you want to allow the virtual machines to function as source servers immediately after the source servers fail or stop communicating.

Note: Manually start the Virtual Machine is the default recovery option.

Heartbeat Properties:

- **Timeout**--Specify the length time that the monitor server must wait for a heartbeat before it powers on a recovery point snapshot.
- **Frequency**--Specify the frequency that the source server communicates heartbeats to the monitor server.

Example: The Timeout value specified is 60. The Frequency value specified is 10. The source server will communicate heartbeats in 10-second intervals. If the monitoring server does not detect a heartbeat within 60 seconds of the last heartbeat that was detected, the monitor server powers on a virtual machine using the latest recovery point snapshot.

Click the Preferences tab.

The Email Alerts options appear.

8. Complete the following Email Alerts options:

- **Missing heartbeat for source machine**--Virtual Standby sends alert notifications when the monitor server does not detect a heartbeat from the source server.
- **VM powered on for source machine configured with auto power ON**--Virtual Standby sends alert notifications when it powers on a virtual machine that was configured to power on automatically when a heartbeat is not detected.
- **Missing heartbeat for source machine configured with manual power ON**--Virtual Standby sends alert notifications when it does not detect a heartbeat from a source server that is not configured to power on automatically.

- **VM storage free space less than**--Virtual Standby sends alert notifications when it detects insufficient free disk space on the defined hypervisor path. The detection occurs when the amount of free disk space is less than the user-defined threshold. The threshold can be defined either an absolute value (MB) or as a percentage of the capacity of the volume.
- **Virtual Standby errors/failure/crash**--Virtual Standby sends alert notifications when it detects an error that occurred during the conversion process.
- **Virtual Standby success**--Virtual Standby sends alert notifications when it detects that a virtual machine powered on successfully.
- **Hypervisor is not reachable**--Virtual Standby sends alert notifications when it detects that it cannot communicate with the ESX Server system or the Hyper-V system.
- **License failure**--Virtual Standby sends alert notifications upon detection of licensing problem on Virtual Standby servers, source servers, and monitoring servers.
- **The Virtual Standby did not start successfully from the Recovery Point Snapshot**--Virtual Standby sends alert notifications when it detects that a virtual machine was not powered automatically and the Automatically start the Virtual Machine Stand-in Recovery option is specified.

Click Save.

The policy is saved.

Assign Nodes to a Policy

To create recovery point snapshots, you assign virtual standby conversion policies to the CA ARCserve D2D nodes that you want to protect.

Note: You cannot apply more than one policy to a node.

Follow these steps:

1. Log in to the virtual standby server and open Virtual Standby.

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

2. From the Policies list, click the policy that you want to assign nodes.

Detailed information about the specified policy appears in the Policy Details tab and the Policy Assignment tab.

3. Click the Policy Details tab to view detailed information about the policy.

(Optional) Click Edit on the toolbar to edit the current settings for the policy.

Note: For more information, see [Edit Policies](#) (see page 58).

4. Click the Policy Assignment tab.

Click Assign and Unassign on the Policy Assignment tab.

The Assign/Unassign Policy dialog opens.

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

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

Note: The Filter fields support the use of wildcard characters.

Examples:

- Acc* lets you filter all nodes having a node name that begins with Acc.
- *.123 lets you filter all nodes having .123 in the IP Address.

Note: To clear the filter results, click X in the Filter field.

6. Do one of the following actions:

- **Assign a node**--From the Available Nodes list, locate the node that you want to assign to the policy.

Click the single right arrow.

The node moves from the Available Nodes list to the Selected Nodes list.

- **Assign nodes**--From the Available Nodes list, click the double right arrow.

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

Click OK.

The nodes are assigned to the policy.

Deploy Policies

After you create a policy, you [assign nodes to a policy](#) (see page 38) and then deploy the policy.

The following behavior applies to the policy deployment process:

- The policy deployment process fails under the following conditions:
 - The Windows Server 2008 Hyper-V Role is installed on the CA ARCserve D2D source server (node).
 - The CA ARCserve D2D node was imported from CA ARCserve Central Host-Based VM Backup. The Windows Hyper-v role is enabled on the Host-based VM backup proxy system and the backup proxy system is specified as the Virtual Standby destination.
- CA ARCserve Central Virtual Standby cannot automatically power on virtual machines that were added from CA ARCserve Central Host-Based VM Backup servers. As a result, when you deploy policies that contain a recovery method that is defined as [Automatically start the virtual machine to nodes protected by Host-Based VM Backup](#) (see page 30), Virtual Standby changes the value of the recovery method to [Manually start the virtual machine](#) (see page 30).

Follow these steps:

1. Log in to the Virtual Standby server and open Virtual Standby.
From the Navigation bar on the home page, click Policies to open the Policies screen.
2. From the Policies list, click the policy that you want to deploy.
Detailed information about the specified policy appears in the Policy Details tab and the Policy Assignment tab.
3. Click the Policy Details tab to view detailed information about the policy.
(Optional) Click Edit on the toolbar to edit the current policy settings.
Note: For more information, see [Edit Policies](#) (see page 58).
4. Click the Policy Assignment tab.
Detailed information about the nodes that are assigned to the policy appears.
(Optional) Click Assign and Unassign on the toolbar to assign or unassign nodes to the policy.
Note: For more information, see [Assign Nodes to a Policy](#) (see page 38) or [Unassign Nodes from Policies](#) (see page 66).

5. Click Deploy Now on the toolbar.

The Deploy Now confirmation message appears.

6. Click OK.

The policy is deployed.

Note: You can also view the policy deployment status for the particular node on the Node screen under the Policy column.

Chapter 4: Using CA ARCserve Central Virtual Standby

This section contains the following topics:

- [Log In to CA ARCserve D2D Nodes](#) (see page 43)
- [Log in to Monitor Servers](#) (see page 44)
- [Node Maintenance Tasks](#) (see page 45)
- [Node Group Management Tasks](#) (see page 55)
- [Virtual Standby Policy Management Tasks](#) (see page 58)
- [Application Configuration Tasks](#) (see page 68)
- [View Logs](#) (see page 74)
- [Add Links to the Navigation Bar](#) (see page 75)
- [Virtual Standby Home Page](#) (see page 75)
- [CA ARCserve Central Virtual Standby Monitoring Tasks](#) (see page 81)
- [How to Protect Virtual Standby Virtual Machines](#) (see page 100)
- [Restore Data from CA ARCserve D2D Recovery Points](#) (see page 102)
- [Restore Data from CA ARCserve D2D File Copies](#) (see page 107)
- [Restore Data Using Find Files/Folders to Restore](#) (see page 112)
- [Recovering Source Servers Using Bare Metal Recovery](#) (see page 116)
- [Restore Microsoft Exchange Email Messages](#) (see page 160)
- [Change Server Communication Protocol](#) (see page 167)

Log In to CA ARCserve D2D Nodes

From the Virtual Standby 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.

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.

Log in to Monitor Servers

Virtual Standby lets you log in directly to the server that is monitoring the CA ARCserve D2D source nodes. From the monitor server, you can perform maintenance tasks and view information about the health of the source servers that the monitor server is monitoring. You can distinguish CA ARCserve D2D nodes from monitor servers by the following icons:

Monitor server icon:



CA ARCserve D2D node icon:



To log in to monitor servers

1. Log in to the Virtual Standby server and open Virtual Standby.
From the Navigation bar on the home page, click Nodes.
The Nodes screen opens.
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. Do one of the following:
 - If you know the IP address or host name of the monitor server, browse to and click the monitor server that you want to log in to and then click Login D2D from the pop-up menu.
 - If you do not know the IP address or host name of the monitor server, browse to and click the CA ARCserve D2D node whose monitor server you want to log in and then click Log in to Monitor Server on the pop-up menu.

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 monitor server.

Node Maintenance Tasks

Virtual Standby lets you use several methods to add nodes:

- [Add nodes by IP address or node name](#) (see page 27).
- [Import nodes from a file](#) (see page 46).

Note: This method lets you import multiple nodes from a list of nodes in a comma-separated file.
- [Add nodes from CA ARCserve Central Host-Based VM Backup servers](#) (see page 48).

Note: This method lets you import virtual machine nodes that are protected by the CA ARCserve Central Host-Based VM Backup application.

In addition, you can perform the following node management tasks.

- [Update nodes](#) (see page 50).
- [Delete nodes](#) (see page 52).

Import Nodes from a File

CA ARCserve Central Virtual Standby lets you import multiple nodes from a file. You can import nodes from a comma-separated values text file (.txt) or a spread sheet (.CSV).

The application lets you import up to 100 nodes from a file. If the file contains more than 100 nodes, the application imports only the first 100 nodes. If you need to add more than 100 nodes, import 100 using a file and then add the remaining nodes manually.

Note: For information about how to add nodes manually, see [Add Nodes by IP Address or Node Name](#) (see page 27).

To import nodes from a file

1. Log in to the application.
From the Navigation Bar on the home page, select Node.
The Node screen displays.
2. From the Node toolbar, click Add, and then click Import Nodes from file on the pop-up menu.
The Select Nodes dialog opens.
3. Click Browse to specify the file that contains the nodes that you want to import.
Note: You can specify a comma separate values (CSV) file or a text file that contains comma-separated values.
Click Upload.
The Node Names and the corresponding User Names appear on the dialog.
4. Click Next.
The Node Credentials dialog opens.
If the User Names and Passwords provided are correct, a green checkmark appears in the Verified field. If the User Names and Passwords provided are not correct, a red exclamation point appears in the Verified field.

5. Do one of the following:

- To add the nodes, verify that all user names and passwords are correct. To change the credentials for a specific node, click the Node Name field.

The Validate Credential dialog opens.

Complete the required fields on the Validate Credential dialog and click OK.

- To apply a global user name and password to all nodes, complete User Name and Password fields and click Apply to Selected.

The global user name and password is applied to all nodes.

Click Finish.

The nodes are added.

Add Nodes from CA ARCserve Central Host-Based VM Backup Servers

CA ARCserve Central Host-Based VM Backup is an application that lets you back up virtual machines using one instance of CA ARCserve D2D that is installed on a backup proxy server. CA ARCserve Central Virtual Standby lets you add the nodes that CA ARCserve Central Host-Based VM Backup servers are protecting so that you can create recovery point snapshots for the nodes. The virtual machines must have CA ARCserve D2D policies assigned, and the policies were assigned using CA ARCserve Central Host-Based VM Backup.

Be aware of the following:

- CA ARCserve Central Virtual Standby lets you use several methods to add nodes:
 - Add nodes manually
 - Add nodes from a text file
 - Add nodes from CA ARCserve Central Host-Based VM Backup servers

CA ARCserve Central Virtual Standby lets you apply policies directly to nodes, whereas with CA ARCserve Central Host-Based VM Backup, you apply policies to backup proxy servers. This behavior continues after you add nodes from CA ARCserve Central Host-Based VM Backup servers.

Note: For information about assigning CA ARCserve D2D policies to virtual machine nodes, see the *CA ARCserve Central Host-Based VM Backup User Guide*.

- Virtual Standby cannot power on recovery point snapshots for nodes that were added from CA ARCserve Central Host-Based VM Backup servers automatically. However, you can power on recovery point snapshots for nodes that were added from CA ARCserve Central Host-Based VM Backup servers manually.

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 Node category, click Add, and then click Add virtual machine from the CA ARCserve Central Host-Based VM Backup server on the pop-up menu.
The Add virtual machine from CA ARCserve Central Host-Based VM Backup server dialog opens.

3. Complete the following fields on the Add VM from CA ARCserve Central Host-Based VM Backup server dialog:
 - **Machine Name**--Lets you specify the IP address or the host name of the CA ARCserve Central Host-Based VM Backup server.
 - **User Name**--Lets you specify the user name that is required to log in to the CA ARCserve Central Host-Based VM Backup server.
 - **Password**--Lets you specify the password that is required to log in to the CA ARCserve Central Host-Based VM Backup server.
 - **Port**--Lets you specify the port number that you want the application to use to communicate with the CA ARCserve Central Host-Based VM Backup server.
 - **Use HTTPS**--Lets you specify to use secure HTTPS communication.

Click OK.

One of the following events occurs:

- If this is the first time that you are importing nodes from this ESX Server system, Virtual Standby imports all of the virtual machines that contain a CA ARCserve Central Host-Based VM Backup policy assignment. After the import process is complete, you can verify the nodes on the Nodes screen.
- If this is not the first time that you are importing nodes from this ESX Server system, the Add VM from CA ARCserve Central Host-Based VM Backup server dialog provides you with a list of nodes that were imported previously. A dialog then appears that asks if you want to overwrite the information for the previously imported nodes.
- If the application does not detect new nodes, the Add VM from CA ARCserve Central Host-Based VM Backup server dialog closes. A message then appears that indicates no nodes were imported.

4. Do one of the following actions:

- **To add the newly detected nodes and overwrite the previously detected nodes:** Click the check box next to the nodes that are detected as imported previously and then click OK.

The application adds the newly detected nodes and overwrites the previously detected nodes. The application overwrites only the status and the credentials that were applied to the previously detected nodes.

- **To add only the newly detected nodes (do not import and overwrite the previously detected nodes):** Do not click the check box next to the nodes that are detected as imported previously and then click OK.

The application adds only the newly detected nodes. The application does not overwrite the previously detected nodes.

- **To exit without adding newly detected nodes and previously detected nodes:** Click Cancel.

The application does not add nodes.

5. (Optional) Click Refresh on the toolbar to verify that all of the newly added nodes appear in the nodes list.

The nodes are added.

Note: When CA ARCserve D2D information is updated on the CA ARCserve Central Host-Based VM Backup server, the server automatically informs CA ARCserve Central Virtual Standby to import the virtual machines from CA ARCserve Central Host-Based VM Backup and to redeploy the policies. If CA ARCserve Central Virtual Standby is not available, you can manually import the virtual machines from CA ARCserve Central Host-Based VM Backup.

Update Nodes

Virtual Standby lets you update information about nodes that were added previously.

Note: You cannot update nodes that were imported from a CA ARCserve Central Host-Based VM Backup server.

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.

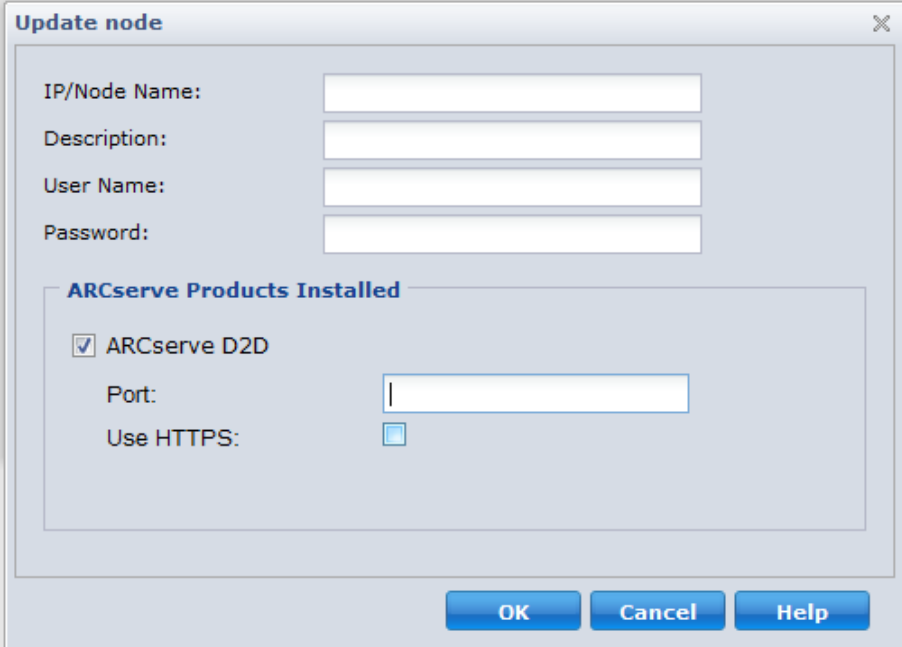
4. Update the node details as needed.

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.

Note: If changes were made to CA ARCserve D2D nodes, the Update Node dialog opens to let you specify more details.



6. (Optional) If the updated information does not display in the node list, click Refresh on the toolbar.

The node is updated.

Delete Nodes

Virtual Standby lets you delete nodes from your environment.

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.

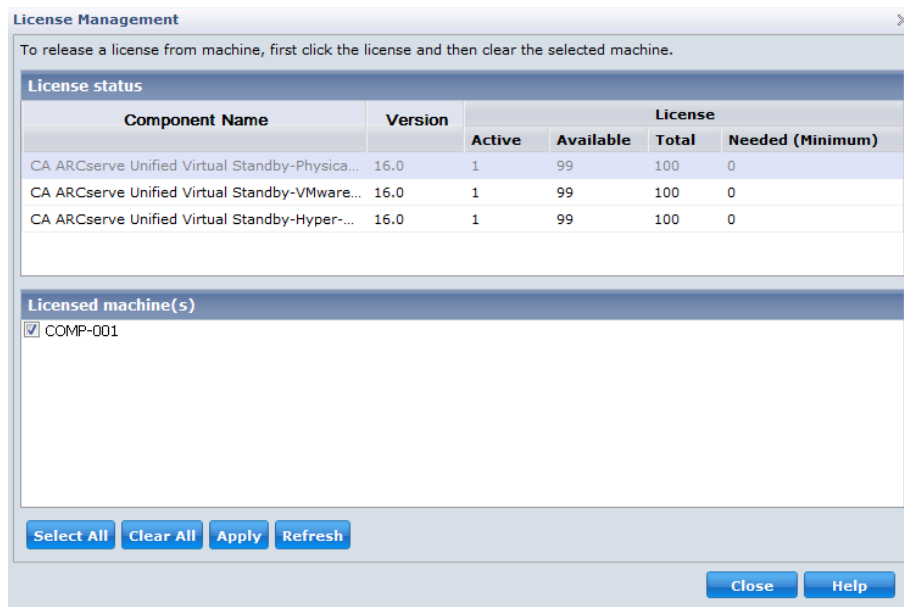
Release Licenses from Nodes

CA ARCserve Central Virtual Standby licensing functions on a count-based mechanism. Count-based licensing lets you grant a single overall license to the node with a predetermined number of active license rights included in the overall license pool. Each node that uses the license is granted an active license from the pool, on a first-come basis, until the total number of available license rights has been reached. If all the active license rights were applied and you want to add a license to a different node, release the license rights from one or more of the nodes to increase the available license count before the different node can use the license.

To release licenses from nodes

1. Log in to the application.
2. From the home screen, open the License Management dialog by clicking Help and clicking Manage Licenses.

The License Management dialog opens and displays a list of the licenses applied to physical computers, VMware-based virtual machines, and Hyper-V-based virtual machines as illustrated by the following dialog:



3. In the Licenses status section, select the license that you want to release from nodes.
The nodes using the license display in the Licensed machines section of the License Management dialog.
4. Click the check box next to the node that you want to release the license.
Note: Click Clear All to clear the check box next to all of the nodes that display in the Licensed machines section of the License Management dialog.
5. Click Apply.
The license is released from the specified node.
6. (Optional) Click Refresh to refresh the list of nodes using the specified license.

Stop Monitoring Nodes from the Monitor Server

CA ARCserve Central Virtual Standby lets you stop monitoring nodes from the Virtual Standby tab on the monitor server.

Important! When you stop monitoring nodes, the Virtual Standby virtual machines may not contain the most current recovery point snapshots that are required to power on the virtual machines. In addition, you can power on virtual machines for the nodes that you stopped monitoring (manually) only from the hypervisor system.

To stop monitoring nodes from the monitor server

1. Log in to the monitor server.

Note: For more information, see [Log in to Monitor Servers](#) (see page 44).

2. After the monitor server opens, click the Virtual Standby tab.

The Virtual Standby screen opens.

3. From the Sources tree, expand All, Source Running, Action Required, or VM Running to locate the source node that you want to stop monitoring.

4. Right-click the node that you want to stop monitoring and click Stop Monitoring on the pop-up menu.

A warning message appears.

5. If you are sure that you want to stop monitoring the specified node, click Yes.

The node is removed from the Sources tree and the monitor server stops monitoring the node.

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 Virtual Standby server, you update the nodes and the policies applied to the nodes. You perform these tasks to maintain the relationship between the CA ARCserve Central Virtual Standby server and the nodes that the CA ARCserve Central Virtual Standby 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 Virtual Standby server was changed.	No action required.

Scenario	Corrective Action
The node was added before the host name of the CA ARCserve Central Virtual Standby server was changed and a policy was not applied to the node.	Update the node. For more information, see Update Nodes (see page 50).
The node was added before the host name of the CA ARCserve Central Virtual Standby server was changed and a policy was applied to the node.	Reapply the policy. For more information, see Deploy Policies (see page 40).

Node Group Management Tasks

Virtual Standby lets you manage the CA ARCserve D2D node groups that you are protecting.

This section contains the following topics:

[Modify Node Groups](#) (see page 55)

[Delete Node Groups](#) (see page 57)

[Filter Node Groups](#) (see page 57)

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.

Delete Node Groups

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.

Filter Node Groups

Virtual Standby lets you use filters to display CA ARCserve D2D nodes in a group with a particular application installed. Virtual Standby lets you filter the nodes that have the following applications installed:

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

To filter node groups

1. Log in to the Virtual Standby server and open Virtual Standby.

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

The Node screen displays.

2. From the Groups list, click the group that you want to filter.

Note: You can filter all of the default groups (All Nodes, Unassigned, SQL Server, and Exchange) and all custom-named groups.

From the Filter toolbar, click the check box next to the application that you want to filter.

The node group is filtered.

Virtual Standby Policy Management Tasks

Virtual Standby lets you manage the conversion policies that you use to protect your CA ARCserve D2D nodes.

This section contains the following topics:

[Edit or Copy Policies](#) (see page 58)

[Unassign Nodes from Policies](#) (see page 66)

[Delete Policies](#) (see page 67)

Edit or Copy Policies

Virtual Standby lets you edit or copy policies after they are created.

To edit policies

1. Log in to the Virtual Standby server and open Virtual Standby.

From the Navigation bar on the home page, click Policies.

The Policy window opens.

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. Click the Virtual Standby tab.

The Virtualization Server, Virtual Machine, and Stand-in Settings options display.

5. Click Virtualization Server.

The Virtualization Server options appear.

6. Complete the following Virtualization Server options:

VMware Systems:

- **Virtualization type**--Click VMware.
- **ESX Host/vCenter**--Specify the host name of the ESX or vCenter Server system.
- **User Name**--Specify the user name that is required to log in to the VMware system.

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

- **Password**--Specify the password for the User Name that is required to log in to the VMware system.
- **Protocol**--Specify HTTP or HTTPS as the protocol that you want to use for communication between the source CA ARCserve D2D node and the monitoring server.
- **Port**--Specify the port that you want to use for data transfer between the source server and the monitoring server.
- **ESX Node**--The values in this field vary based on the value specified in the ESX Host/vCenter field:
 - **ESX Server systems**--When you specify an ESX Server system in the ESX Host/vCenter field, this field displays the host name of the ESX Server system.
 - **vCenter Server systems**--When you specify a vCenter Server system the ESX Host/vCenter field, this field lets you specify (from a drop-down list) the ESX Server system that you want to associate with this policy.
- **Monitor Server**--Specify the host name of the server that you want to monitor the status of the source server.

Note: The monitor server can be any physical computer or virtual machine provided that server is not functioning as the proxy server for a CA ARCserve Central Host-Based VM Backup implementation.

- **User Name**--Specify the user name that is required to log in to the monitoring system.
- **Password**--Specify the password for the User Name that is required to log in to the monitoring system.
- **Protocol**--Specify HTTP or HTTPS as the protocol that you want to use for communication between the CA ARCserve Central Virtual Standby server and the ESX Server system (monitoring server).

- **Port**--Specify the port that you want to use for data transfer between the CA ARCserve Central Virtual Standby server and the ESX Server system (monitoring server).
- **Use monitor server as proxy for data transfer**--Specify this option to let the monitor server copy the conversion data from the CA ARCserve D2D source node to the ESX Server datastore. With this option enabled, Virtual Standby transfers the conversion data from the source node to the ESX Server datastore using fibre channel communication, which is faster than using LAN communication to transfer data.

Note: The Use monitor server as proxy for data transfer option is enabled by default. You can disable this option to allow the CA ARCserve D2D source server to copy the conversion data directly to the datastore on the ESX Server system.

Hyper-V Systems:

- **Virtualization type**--Click Hyper-V.

Note: When you click Hyper-V, the Monitoring options are not accessible. The Monitoring options behave in this manner because the Hyper-V server assumes the role of the Monitor server.

- **Hyper-V Host Name**--Specify the host name of the Hyper-V system.

- **User Name**--Specify the user name that is required to log in to the Hyper-V system.

Note: The account that you specify must be an administrative account or an account with administrative privileges on the Hyper-V system.

- **Password**--Specify the password for the User Name that is required to log in to the Hyper-V system.

- **Port**--Specify the port that you want to use for data transfer between the source server and the monitoring server.

- **Monitor Server**--Specify the host name of the server that you want to monitor the status of the source server.

- **User Name**--Specify the user name that is required to log in to the monitoring system.

- **Password**--Specify the password for the User Name that is required to log in to the monitoring system.

- **Protocol**--Specify HTTP or HTTPS as the protocol that you want to use for communication between the CA ARCserve Central Virtual Standby server and the Hyper-V Server system (monitoring server).

- **Port**--Specify the port that you want to use for data transfer between the CA ARCserve Central Virtual Standby server and the Hyper-V Server system (monitoring server).

Click Virtual Machine.

The Virtual Machine options appear.

7. Complete the following Virtual Machine options:

VMware Systems:

Apply the following Virtual Machine options to VMware systems:

- **VM Name Prefix**--Specify the prefix that you want to add to the display name for the virtual machine on the ESX Server system.

Default value: CAVM_

- **VM Resource Pool**--Specify the name of resource pool where standby virtual machine is to be grouped.
- **CPU Count**--Specify the minimum and maximum CPU count supported by the standby virtual machine.
- **Memory**--Specify the total amount of RAM in MB to be allocated for the standby virtual machine.

Note: The amount of RAM specified must be a multiple of two.

- **VM Datastore**--Specify the location where you want to store the conversion data.
 - **Specify one datastore for all virtual disks**--Lets the application copy all of the disks related to the virtual machine to one data store.
 - **Specify a datastore for each virtual disk**--Lets the application copy disk related information for the virtual machine to the corresponding datastore.
- **VM Network**--Lets you define the NICs, virtual networks, and paths that the ESX Server system uses to communicate with the virtual machines.
 - **Specify a network adapter type for each NIC and connect the network adapter to the following virtual network**--Lets you define how to map the virtual NIC to the virtual network. Specify this option when the virtual machine contains virtual NICs and a virtual network.
 - **Specify a network adapter type and a virtual network for each NIC**--Lets you define the name of the virtual network that you want the NIC to use to communicate.

Hyper-V Systems:

Apply the following Virtual Machine options to Hyper-V systems:

- **VM Basic Settings**--Complete the following VM Basic settings:
 - **VM Name Prefix**--Specify the prefix that you want to add to the display name for the virtual machine on the Hyper-V system.
Default value: CAVM_
 - **CPU Count**--Specify the minimum and maximum CPU count supported by the standby virtual system.
 - **Memory**--Specify the total amount of RAM in MB to be allocated to the standby virtual machine.
Note: The amount of RAM specified must be a multiple of four.
- **VM Path**--Specify one of the following VM Path options:
 - **Specify one path for all virtual disks**--Specify the location on the Hyper-v server where you want to store the conversion data.
 - **Specify a path for each virtual disk**--Specify the location on the Hyper-V server where you want to store the conversion data for each virtual disk.
Note: CA ARCserve Central Virtual Standby does not support creating virtual disk images (VHD files) on compressed volumes and volumes that are encrypted by the file system. If the path specified resides on compressed or encrypted Hyper-V volumes, Virtual Standby prevents you from creating the policy.
- **VM Network**--Lets you define the NICs, virtual networks, and paths that the Hyper-V server uses to communicate with the virtual machines. Specify one of the following options and complete the required fields.
 - **Specify a network adapter type for each NIC and connect the network adapter to the following network**--Lets you define how to map the virtual NIC to the virtual network. Specify this option when the virtual machine contains virtual NICs and a virtual network.
 - **Specify a network adapter type and a virtual network for each NIC**--Lets you define the name of the virtual network that you want the NIC to use to communicate.

Click Stand-in Settings.

The Stand-in Settings options appear.

8. Complete the following Stand-in Settings options:

Recovery:

Select one of the following methods:

- **Manually start the Virtual Machine**--Lets you power on and provision virtual machines manually when the source server fails or stops communicating. Specify this option when you prefer to analyze the cause of the failure before you provision the virtual machines and allow the servers to function as source servers.
- **Automatically start the Virtual Machine**--Lets you power on and provision virtual machines automatically when the source server fails or stops communicating. Specify this option when you want to allow the virtual machines to function as source servers immediately after the source servers fail or stop communicating.

Note: Manually start the Virtual Machine is the default recovery option.

Heartbeat Properties:

- **Timeout**--Specify the length time that the monitor server must wait for a heartbeat before it powers on a recovery point snapshot.
- **Frequency**--Specify the frequency that the source server communicates heartbeats to the monitor server.

Example: The Timeout value specified is 60. The Frequency value specified is 10. The source server will communicate heartbeats in 10-second intervals. If the monitoring server does not detect a heartbeat within 60 seconds of the last heartbeat that was detected, the monitor server powers on a virtual machine using the latest recovery point snapshot.

Click the Preferences tab.

The Email Alerts options appear.

9. Complete the following Email Alerts options:

- **Missing heartbeat for source machine**--Virtual Standby sends alert notifications when the monitor server does not detect a heartbeat from the source server.
- **VM powered on for source machine configured with auto power ON**--Virtual Standby sends alert notifications when it powers on a virtual machine that was configured to power on automatically when a heartbeat is not detected.
- **Missing heartbeat for source machine configured with manual power ON**--Virtual Standby sends alert notifications when it does not detect a heartbeat from a source server that is not configured to power on automatically.

- **VM storage free space less than**--Virtual Standby sends alert notifications when it detects insufficient free disk space on the defined hypervisor path. The detection occurs when the amount of free disk space is less than the user-defined threshold. The threshold can be defined either an absolute value (MB) or as a percentage of the capacity of the volume.
- **Virtual Standby errors/failure/crash**--Virtual Standby sends alert notifications when it detects an error that occurred during the conversion process.
- **Virtual Standby success**--Virtual Standby sends alert notifications when it detects that a virtual machine powered on successfully.
- **Hypervisor is not reachable**--Virtual Standby sends alert notifications when it detects that it cannot communicate with the ESX Server system or the Hyper-V system.
- **License failure**--Virtual Standby sends alert notifications upon detection of licensing problem on Virtual Standby servers, source servers, and monitoring servers.
- **The Virtual Standby did not start successfully from the Recovery Point Snapshot**--Virtual Standby sends alert notifications when it detects that a virtual machine was not powered automatically and the Automatically start the Virtual Machine Stand-in Recovery option is specified.

Click Save.

The policy is edited.

Unassign Nodes from Policies

Virtual Standby lets you unassign nodes from policies. Virtual Standby does not let you assign multiple policies to nodes. When you want to assign nodes to new policies, you unassign the current policy from the nodes before you can assign the new policy to nodes.

Follow these steps:

1. Log in to the virtual standby server and open Virtual Standby.
From the Navigation bar on the home page, click Policies to open the Policy screen.
2. From the Policies list, click the policy that you want to unassign nodes.
Detailed information about the specified policy appears in the Policy Detail tab and the Policy Assignment tab.
3. Click the Policy Detail tab to view detailed information about the policy.
(Optional) Click Edit on the Policies toolbar to edit the current policy settings.

Note: For more information, see [Edit Policies](#) (see page 58).

4. Click the Policy Assignment tab.

Click Assign and Unassign on the Policy Assignment tab to open the Assign/Unassign Policy dialog.

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

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

Note: The Filter fields support the use of wildcard characters.

Examples:

- Acc* lets you filter all nodes having a node name that begins with Acc.
- *.123 lets you filter all nodes having .123 in the IP Address.

Note: To clear the filter results, click X in the Filter field.

6. Do one of the following actions:

- **Unassign a node**--From the Selected Nodes list, locate the node that you want to unassign from to the policy.

Click the single left arrow.

The node moves from the Selected Nodes list to the Available Nodes list.

- **Unassign nodes**--From the Selected Nodes list, click the double left arrow.

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

Click OK.

The nodes are unassigned from the policy.

Delete Policies

Virtual Standby lets you delete policies that were created previously.

Note: Virtual Standby does not let you delete policies that are assigned to nodes. To delete policies with assigned nodes, you must unassign the nodes from the policy and then delete the policy. For information about how to unassign nodes from a policy, see [Unassign Nodes from Policies](#) (see page 66).

To delete policies

1. Log in to the Virtual Standby server and open Virtual Standby.
From the Navigation bar on the home page, click VCM Policies.
The Policy window opens.
2. From the Policies list, click the policy that you want to delete.

3. Click Delete on the Policies toolbar.

A delete confirmation message appears.

4. Click Yes to delete the policy.

Note: If you delete a policy in error, you must recreate the policy. If you do not want to delete the policy, click No.

The policy is deleted.

Application Configuration Tasks

Virtual Standby lets you specify email alerts settings and how to update your Virtual Standby installation.

This section contains the following topics:

[Configure Email Settings](#) (see page 68)

[Configure Automatic Updates](#) (see page 69)

[Configure Social Networking Preferences](#) (see page 72)

[Modify the Administrator Account](#) (see page 73)

Configure Email Settings

You can configure email 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 Configuration to display the Email 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. Click Save.

Note: You can click Reset to revert to the previously saved values.

The email configuration is applied.

Configure Automatic Updates

CA ARCserve Central Virtual Standby lets you define when to check for product updates and how often to update your Virtual Standby installation.

To configure automatic updates

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.

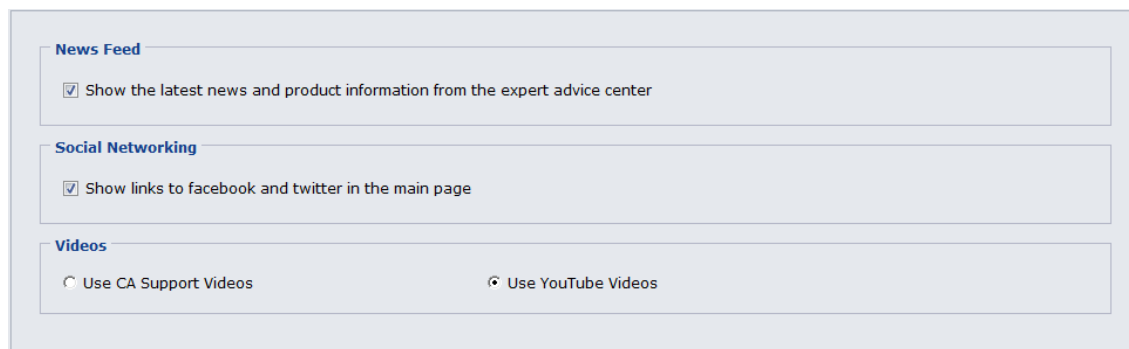
The proxy settings are configured

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.

To configure social networking preferences

1. Log in to the application.
From the Navigation bar on the home page, click Configuration.
The Configuration screen displays
2. From the Configuration panel, click Preferences Configuration.
The Preferences options appear.



The screenshot shows a configuration panel with three sections:

- News Feed**: A checkbox labeled "Show the latest news and product information from the expert advice center" is checked.
- Social Networking**: A checkbox labeled "Show links to facebook and twitter in the main page" is checked.
- Videos**: Two radio buttons are present. "Use CA Support Videos" is unselected, and "Use YouTube Videos" is selected.

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
 - PasswordClick Save

The administrator account is modified.

View 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 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 warning 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 File**--Lets you view only logs about the process of importing CA ARCserve D2D nodes into the application from a file.
- **Policy Management**--Lets you view only logs about managing policies.
- **Updates**--Lets you view only logs about updating the application.

- **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).

Click Refresh. 

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.

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.

Virtual Standby Home Page

The Virtual Standby tab on the monitor server lets you view information about all of the CA ARCserve D2D servers that you are protecting. However, the Virtual Standby tab on source servers let you view only information about the specific source server that you log in to.

This section contains the following topics:

[How to Use the Virtual Standby Summary Screen](#) (see page 76)

[How to Use the Servers List](#) (see page 77)

[View Summary Information about the Latest Virtual Standby Job](#) (see page 77)

[Monitor the Status of Virtual Conversion Jobs](#) (see page 79)

[View Virtual Standby Settings for Source Servers](#) (see page 80)

[View the Recovery Point Snapshots List](#) (see page 80)

How to Use the Virtual Standby Summary Screen

The Virtual Standby Summary screen displays icons that provide a quick visual indication of the current status, along with guidance for the urgency of any actions may need to be taken.

The following icons appear on the home page:



Successful
(No action is necessary)



Caution
(Action may be necessary soon)



Warning
(Immediate action is necessary)

The Virtual Standby Summary screen displays the following information:

- **Servers list**--Displays a list of source servers that this monitoring server is protecting. The list sorts servers by their current status. For example, All, Action Required, Server Running, and so on.

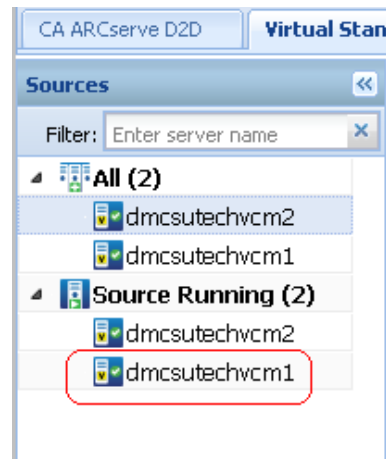
Note: The Servers list appears only when you are logged in to the monitoring server. For more information, see [How to Use the Servers List](#) (see page 77).
- **Virtual Standby Summary**--Displays summary information for the selected source server. For more information, see [Monitor the Status of Virtual Conversion Jobs](#) (see page 79).
- **Virtual Standby Settings**--Displays summary information about virtual conversion settings for the selected source server. For more information, see [View Virtual Standby Settings for Source Servers](#) (see page 80).
- **Recovery Point Snapshots**--Displays a list of recovery point snapshots that are available for the selected source server. For more information, see [View the Recovery Point Snapshots List](#) (see page 80).
- **Tasks**--Displays a list of tasks that you can perform for the selected source server. For more information, see [Virtual Standby Monitoring Tasks](#) (see page 81).
- **Support and Community Access**--Provides a mechanism that lets you initiate various support-related functions.

Note: For more information about Support and Community Access, see the CA ARCserve D2D documentation.

How to Use the Servers List

The Servers list on the Virtual Standby Summary screen displays a list of source servers that a monitoring server is protecting. The list sorts servers by their current status. For example, All, Action Required, Source Running, and so on.

To perform maintenance tasks or to view information about a CA ARCserve D2D node, click the Virtual Standby tab and then click the server as illustrated by the following screen:




View Summary Information about the Latest Virtual Standby Job

The Node screen lets you view summary information about the last Virtual Standby (conversion) job for a node. You can view information about Virtual Standby jobs that completed successfully and unsuccessfully.


Follow these steps:

1. Log in the Virtual Standby server.
Click Nodes on the Navigation bar to open the Node screen.

2. In the Status column, roll your mouse pointer over one of the following displayed icons:

 Successful

 Warning

 Error/Failed

The Node Status Summary message box appears and provides you with the following results for the most recent successful Virtual Standby job:

Most Recent Virtual Standby

The date and time the most recent Virtual Standby job that completed successfully or unsuccessfully.

Recovery Point Snapshots

Displays the number of recovery points that are converted for the node as of the Most Recent Virtual Standby.

Destination Status

Displays the amount of available free disk space on the Virtual standby destination. The destination can consist of the following:

- An ESX Server data store that is used to convert to an ESX Server system.
- Free disk space on the volume where a Hyper-V server stores the recovery point snapshots.

3. Move your mouse pointer away from the Status icon to close the Node Status Summary message box.
4. You can view more information about the latest successful or unsuccessful Virtual Standby job in the following fields:

Last Conversion Results

Results of the latest Virtual Standby job that completed successfully or unsuccessfully. For example, Finished, Canceled, Failed.

Last Conversion Time

The date and time the most recent successful or unsuccessful Virtual Standby job completed.

Monitor the Status of Virtual Conversion Jobs

Virtual Standby lets you monitor the status of in-progress virtual conversion jobs. In addition, Virtual Standby lets you view summary information about the virtual conversion data and the virtual machines that are protecting your CA ARCserve D2D source servers.

To monitor the status of virtual conversion jobs

1. Open Virtual Standby 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.

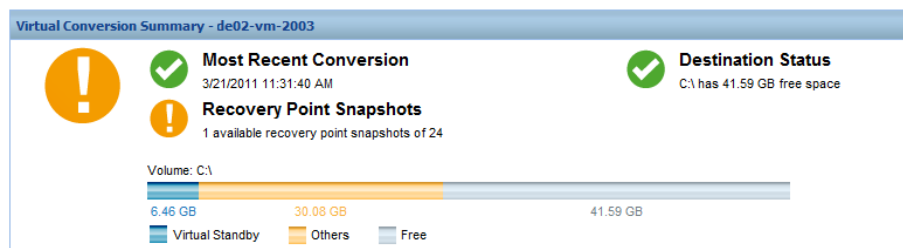
CA ARCserve D2D opens.

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.

4. Click the Virtual Standby tab.

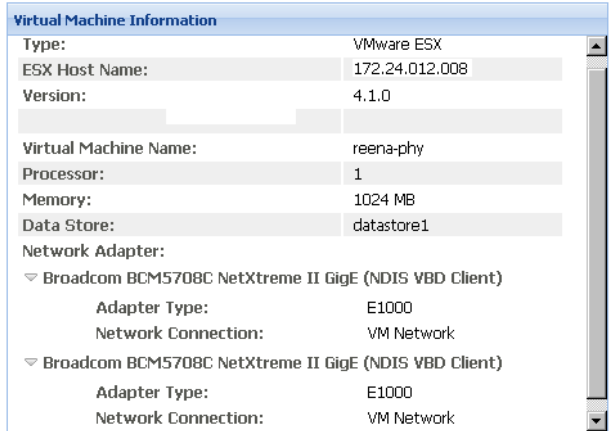
(Optional) If the CA ARCserve D2D server is a monitor server, click the Server list, expand All, Source Running, or Action Required and click the server that you want to monitor.

Virtual Standby displays information about in-progress virtual conversion jobs and summary information about virtual conversion jobs and the virtual machine that is protecting the server.



View Virtual Standby Settings for Source Servers

The Virtual Standby Summary screen displays information about the virtual machines that are protecting source servers.



View the Recovery Point Snapshots List

The Virtual Standby screen displays a list of the most recent recovery point snapshots.

The list box displays the date and time the backup of the CA ARCserve D2D server completed.

From the list of recovery point snapshots list, you can power on virtual machines. For more information, see [Power On Recovery Point Snapshots](#) (see page 86).

Recovery Point Snapshots - Ready to Power on	
Time of backup	Action
5/7/2011 11:49:04 AM	Power On VM from this Snapshot
5/7/2011 11:34:04 AM	Power On VM from this Snapshot
5/7/2011 11:19:06 AM	Power On VM from this Snapshot
5/7/2011 11:04:12 AM	Power On VM from this Snapshot
5/7/2011 11:01:22 AM	Power On VM from this Snapshot
5/7/2011 10:49:08 AM	Power On VM from this Snapshot
5/7/2011 10:30:38 AM	Power On VM from this Snapshot
5/7/2011 12:18:30 AM	Power On VM from this Snapshot

Note: If the Virtual Standby destination is a VMware ESX server, the maximum number of recovery point snapshots that are displayed is 29. If the Virtual Standby destination is a Microsoft Hyper-V server, the maximum number of recovery point snapshots that are displayed is 24.

CA ARCserve Central Virtual Standby Monitoring Tasks

Virtual Standby lets you perform the following monitoring tasks:

- [Pause and resume heartbeats](#) (see page 81).
- [Pause and resume Virtual Standby jobs](#) (see page 84).
- [View Activity Log data about virtual conversions and recovery point snapshots](#) (see page 89).
- [Power on recovery point snapshots](#) (see page 86).

Pause and Resume Heartbeats from the Virtual Standby Server

Virtual Standby lets you pause and resume the heartbeats that are detected by the monitoring server. The heartbeat is the process where the source server and monitoring server communicate about the health of the source server. If the monitoring server does not detect a heartbeat after a specified length of time, Virtual Standby provisions the virtual machine to function as the source node.

Examples: When to Pause or Resume Heartbeats

The following examples describe when to pause and resume heartbeats:

- Pause the heartbeat when you want to offline a node (source server) for maintenance.
- Resume the heartbeat after the maintenance tasks are complete and the node (source server) is online.

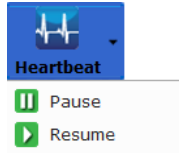
Be aware of the following behavior:

- You can pause and resume heartbeats at the group level or at the individual node level.
- You can pause and resume heartbeats for one or more nodes in one step.
- CA ARCserve Central Virtual Standby does not power on recover point snapshots while the heartbeat is in a paused state.
- When you upgrade CA ARCserve D2D installations on source nodes, CA ARCserve Central Virtual Standby pauses the heartbeat for the nodes. To help ensure that monitor servers monitor the upgraded nodes, resume the heartbeat for the nodes after you complete the upgrades on the nodes.

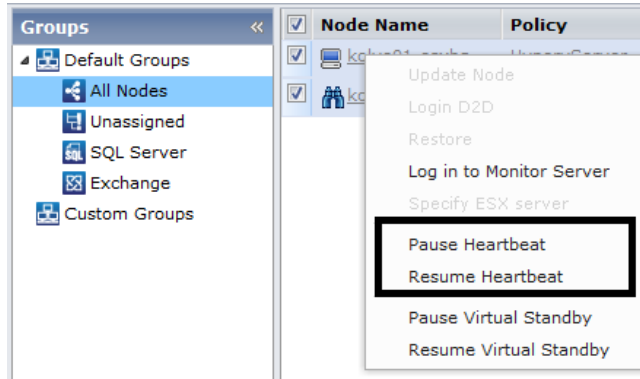
Note: Optionally, you can pause or resume heartbeats from the Virtual Standby Summary screen on the node. For more information, see [Pause and Resume Heartbeats from the Nodes](#) (see page 83).

Follow these steps:

1. Log in the Virtual Standby server.
Click Nodes on the Navigation bar to open the Node screen.
2. Do one of the following actions to specify the nodes that you want to pause or resume:
 - **Node level:** Click the group containing the nodes that you want to pause or resume and then click the check box next to the nodes that you want to pause or resume.
 - **Group level:** Click the group containing the nodes that you want to pause or resume.
3. Then do one of the following actions to pause or resume the heartbeat:
 - Click Heartbeat on the toolbar and click Pause or Resume on the pop-up menu as illustrated by the following screen:



- Right-click the selected group or right-click the nodes and click Pause Heartbeat or Resume Heartbeat on the pop-up menu as illustrated by the following screen:



Pause and Resume Heartbeats from the Nodes

Virtual Standby lets you pause and resume the heartbeats that are detected by the monitoring server. The heartbeat is the process where the source server and monitoring server communicate about the health of the source server. If the monitoring server does not detect a heartbeat after a specified length of time, Virtual Standby provisions the virtual machine to function as the source node.

Examples: When to Pause or Resume Heartbeats

The following examples describe when to pause and resume heartbeats:

- Pause the heartbeat when you want to offline a node (source server) for maintenance.
- Resume the heartbeat after the maintenance tasks are complete and the node (source server) is online.

Note: Optionally, you can pause and resume heartbeats from the Node screen on the Virtual Standby server. For more information, see [Pause and Resume Heartbeats from the Virtual Standby Server](#) (see page 81).

Follow these steps:

1. Log in the Virtual Standby server.
Click Nodes 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 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 pause or resume the heartbeat and click Login D2D from the pop-up menu.
CA ARCserve D2D opens.
4. Click the Virtual Standby tab.
Virtual Standby Summary screen opens.
5. (Optional) If you logged in to a monitoring server, expand All or Server Running from the Servers list, and click the node whose heartbeat you want to pause or resume.

Note: If the heartbeat is running, Pause Heartbeat appears in the Virtual Conversion task list. If the heartbeat is not running, Resume Heartbeat appears in the Virtual Conversion task list.

6. Do one of the following:
 - If the heartbeat is running, click Pause Heartbeat to pause the heartbeat temporarily.
Example: You want to bring the server offline to perform maintenance tasks.
 - If the heartbeat is not running (paused), click Resume Heartbeat to resume the heartbeat.
Example: The maintenance tasks are complete and you want to bring the server online.

The heartbeat pauses or resumes.

Pause and Resume Virtual Standby Jobs from the Virtual Standby Server

Virtual conversion is the process where Virtual Standby converts CA ARCserve D2D recovery points from source nodes to virtual machine data files named recovery point snapshots. In the event a source node fails, Virtual Standby uses the recovery point snapshots to power on a virtual machine for the source node.

As a best practice, allow the virtual conversion process to operate continuously. However, if you want to pause the virtual conversion process temporarily, you can do so from the Virtual Standby server. After you correct the problems on the source node, you can resume the virtual conversion process.

Note: Optionally, you can pause and resume Virtual Standby jobs directly from the nodes. For more information, see [Pause and Resume Virtual Standby Jobs from the Nodes](#) (see page 85).

Follow these steps:

1. Log in the Virtual Standby server.
Click Nodes on the Navigation bar to open the Node screen.
2. Do one of the following actions to specify the nodes that you want to pause or resume Virtual Standby jobs:
 - **Node level:** Click the group containing the nodes that you want to pause or resume and then click the check box next to the nodes that you want to pause or resume.
 - **Group level:** Click the group containing the nodes that you want to pause or resume.

3. Then do one of the following actions to pause or resume the Virtual Standby jobs:
 - Click Virtual Standby on the toolbar and click Pause or Resume on the pop-up menu.
 - Click the selected group or click the nodes and click Pause Virtual Standby or Resume Virtual Standby on the pop-up menu.

Pause and Resume Virtual Standby Jobs from the Nodes

Virtual conversion is the process where Virtual Standby converts CA ARCserve D2D recovery points from source nodes to virtual machine data files named recovery point snapshots. In the event a source node fails, Virtual Standby uses the recovery point snapshots to power on a virtual machine for the source node.

As a best practice, allow the virtual conversion process to operate continuously. However, if you want to pause the virtual conversion process temporarily, you can do so from the Virtual Standby server. After you correct the problems on the source node, you can resume the virtual conversion process.

Note: Optionally, you can pause and resume virtual standby jobs from the Virtual Standby server. For more information, see [Pause and Resume Virtual Standby Jobs from the Virtual Standby Server](#) (see page 84).

Follow these steps:

1. Open Virtual Standby and click Nodes on 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 pause or resume and click Login D2D from the pop-up menu.
CA ARCserve D2D opens.
4. Click the Virtual Standby tab.
Virtual Standby Summary screen opens.
5. (Optional) If you logged in to a monitoring server, expand All or Server Running from the Servers list, and click the node whose virtual standby job you want to pause or resume.

If the virtual standby job is running, Pause Virtual Standby appears in the Virtual Standby task list. If the Virtual Standby job is not running, Resume Virtual Standby appears in the Virtual Standby task list.

6. Do one of the following:
 - If the virtual standby job is running, click Pause Virtual Standby to pause the job temporarily.
 - If the virtual standby job is not running (paused), click Resume Virtual Standby to resume the job.

The virtual standby job pauses or resumes.

Power on Virtual Standby Virtual Machines from Recovery Point Snapshots

Virtual Standby can be configured to power on Virtual Standby virtual machines from recovery point snapshots automatically when the monitoring server does not detect a heartbeat from the source server. Optionally, Virtual Standby lets you power on Virtual Standby virtual machines from recovery point snapshots manually in the event a source server fails, an emergency occurs, or you want to offline a source node for maintenance.

Note: The following steps describe how to power on Virtual Standby virtual machines from recovery point snapshots manually. For information about how to allow Virtual Standby to power on Recovery Point Snapshots automatically, see [Create Policies](#) (see page 30).

Follow these steps:

1. Open Virtual Standby and click Nodes 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 that you want to log in to.

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

3. Browse to and click the node that you want to power on from a recovery point snapshot and click Standby VM from the Actions toolbar.

The Recovery Point Snapshot dialog opens.

4. On Recovery Point Snapshot dialog, specify a date and time range to locate the recovery point snapshot that you want to use.

Click Power On VM.

The virtual machine is powered on using the data contained in the recovery point snapshot.

Note: After the virtual machine is powered on, you can be prompted to restart the computer one or more times. This behavior occurs because VMware installs VMware Tools on the virtual machine or Windows Hyper-V installs Integration Services on the virtual machine.

After you power on Virtual Standby virtual machines from recovery point snapshots, you may need to complete the following tasks:

- Activate the Windows operating system that is running on the virtual machine.
- Start CA ARCserve D2D backups on the virtual machine.

Note: For information about creating and assigning CA ARCserve D2D backup policies using CA ARCserve Central Protection Manager, see the *CA ARCserve Central Protection Manager User Guide*.

- Update CA ARCserve Central Virtual Standby with the host name, IP address, and the login credentials for the virtual machine.
- Assign the node to a policy.

Note: This task is required only when you want to create recovery point snapshots for the virtual machine that was powered on. For more information, see [Assign Nodes to a Policy](#) (see page 38).

Power on Virtual Standby Virtual Machines from Hyper-V Manager

When you want to power-on Virtual Standby virtual machines manually, the best practice is to power on the virtual machines from the Virtual Standby screen on the CA ARCserve D2D server. For more information, see [Power on Virtual Standby Virtual Machines from Recovery Point Snapshots](#) (see page 86). However, if you want to start the Virtual Standby virtual machines from the Hyper-V server, you can do so using Hyper-V Manager.

Note: The Hyper-V Manager lets you access the recovery point snapshots that CA ARCserve Central Virtual Standby created to protect the node. You should not delete the snapshots. When you delete the snapshots, the relationship between the data contained in the snapshots becomes inconsistent the next time a Virtual Standby runs. With inconsistent data, you cannot power on Virtual Standby virtual machines properly.

To power on Virtual Standby virtual machines from Hyper-V Manager

1. Log in to the Hyper-V server that is monitoring the nodes that you are protecting.
2. Start Hyper-V Manager by doing the following:

Click Start, click All Programs, click Administrative Tools, and then click Hyper-V Manager.

Hyper-V Manager opens.

3. From the Hyper-V Manager directory tree, expand Hyper-V Manager and click the Hyper-V server containing the virtual machine that you want to power on.

The virtual machines associated with the specified hyper-V server display in the Virtual Machines list in the center pane.

4. Do one of the following:
 - **To power on the virtual machine using the latest snapshot:** In the Virtual Machines list, right-click the virtual machine that you want to power on and click Start on the pop-up menu.
 - **To power on the virtual machine using an older snapshot:**
 - a. In the Virtual Machines list, click the virtual machine that you want to power on.

The snapshots associated with the virtual machine display in the Snapshots list.
 - b. Right-click the snapshot that you want to use to power on the virtual machine and click Apply on the pop-up menu.

The Apply Snapshot dialog opens.
 - c. Click Apply.
 - d. In the Virtual Machines list, right-click the virtual machine that you want to power on and click Start on the pop-up menu.

The Virtual Standby virtual machine is powered on.

If necessary, you can back up the virtual machines and create recovery point snapshots after you power on the virtual machine. For more information, see [Tasks to Perform After Powering on Virtual Standby Virtual Machines](#).

Power on Virtual Standby Virtual Machines from VMware vSphere Client

When you want to power-on Virtual Standby virtual machines manually, the best practice is to power on the virtual machines from the Virtual Standby screen on the CA ARCserve D2D server. For more information, see [Power on Virtual Standby Virtual Machines from Recovery Point Snapshots](#) (see page 86). However, if you want to start the Virtual Standby virtual machines from the ESX Server or the vCenter Server system, you can do so using VMware vSphere Client.

Note: The VMware vSphere Client lets you access the recovery point snapshots that CA ARCserve Central Virtual Standby created to protect the node. You should not delete the snapshots. When you delete the snapshots, the relationship between the data contained in the snapshots becomes inconsistent the next time a Virtual Standby runs. With inconsistent data, you cannot power on Virtual Standby virtual machines properly.

To power on Virtual Standby virtual machines from VMware vSphere Client

1. Open VMware vSphere Client and log in to the ESX Server or vCenter Server system that is monitoring the nodes that you are protecting.

From the directory tree, expand the ESX Server system or the vCenter Server system, locate, and click the virtual machine that you want to power on.

2. Do one of the following:
 - **To power on the virtual machine using the latest snapshot:** Click the Getting Started tab and then click Power on the virtual machine located on the bottom the screen.
 - **To power on the virtual machine using an older snapshot:**
 - a. Click the Snapshot Manager button on the toolbar.



The Snapshots for (virtual machine name) dialog opens to display a list of snapshots that are available for the virtual machine.

- b. From the list of snapshots, click the snapshot that you want to use to power on the virtual machine and then click Go to.

The Virtual Standby virtual machine is powered on.

If necessary, you can back up the virtual machines and create recovery point snapshots after you power on the virtual machine. For more information, see [Tasks to Perform After Powering on Virtual Standby Virtual Machines](#).

View Activity Log Data about Jobs

Virtual Standby lets view Activity Log information about Virtual Conversion jobs. The Activity Log contains Virtual Conversion job records for the CA ARCserve D2D source servers that you are protecting.

Note: The Activity Log (activity.log) is stored in the following directory on the server where CA ARCserve D2D is installed:

C:\Program Files\CA\ARCserve D2D\Logs

To view Activity Log data about jobs

1. Open Virtual Standby and click Nodes on 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.

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.

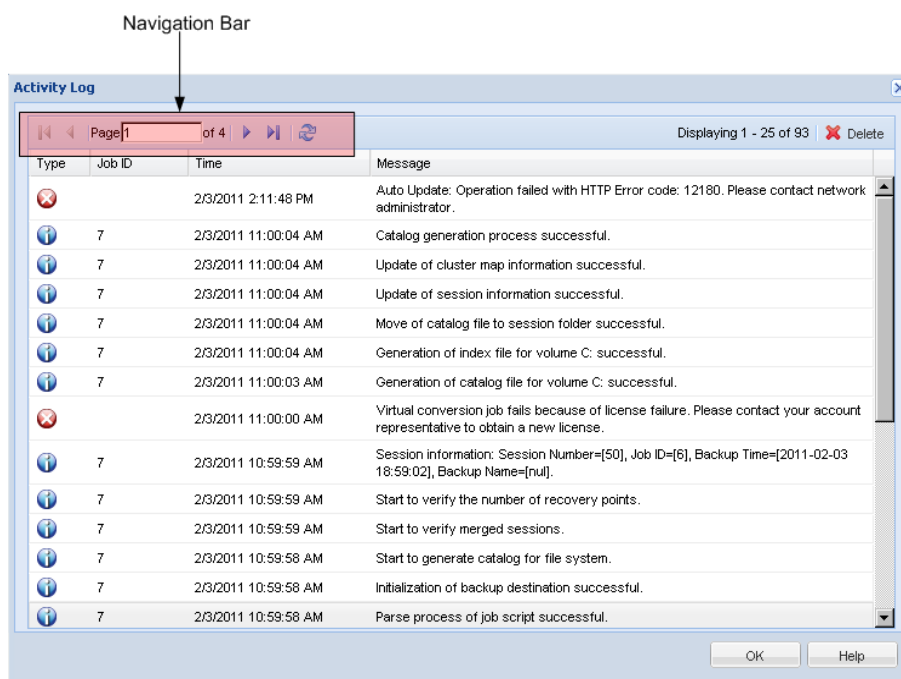
4. Click the Virtual Standby tab.

Virtual Standby Summary screen opens.

5. (Optional) If you logged in to a monitoring server, expand All or Server Running from the Servers list, and click the node whose Activity Log data you want to view.

From the Virtual Conversion Tasks list located on the right side of the Virtual Standby Summary screen, click View Logs.

The Activity Log window opens.



Use the Navigation bar to search for and view Activity Log records. The following icons appear on the Activity Log:

 Information

 Warning

 Error

Note: For information about deleting activity log records, see [Delete Activity Log Records](#) (see page 91).

Delete Activity Log Records

Virtual Standby lets you manage the overall size of Activity Log data. The Activity Log contains job records for the CA ARCserve D2D source nodes that you are protecting. If you are protecting a large quantity of source servers, you perform frequent backups, or both, the Activity Log can consume a large amount of disk space on the CA ARCserve D2D node.

You can delete Activity Log records that are older than a specified date or delete all Activity Log records.

Note: The Activity Log (activity.log) is stored in the following directory on the server where CA ARCserve D2D is installed:

C:\Program Files\CA\ARCserve D2D\Logs

To delete Activity Log records

1. Open Virtual Standby and click Nodes on 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.
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.
4. Click the Virtual Standby tab.
Virtual Standby Summary screen opens.
5. (Optional) If you logged in to a monitoring server, expand All or Server Running from the Servers list, and click the node whose Activity Log data you want to delete.
6. From the Virtual Conversion Tasks list located on the right side of the Virtual Standby Summary screen, click View Logs.
The Activity Log window opens.

7. Click Delete on the toolbar.
The Delete Activity Log dialog opens.
 8. Click one of the following options:
 - **Delete all log records**--Lets you delete all job records in the Activity Log.
Note: Use this option with care. You cannot recover deleted Activity Log records.
 - **Delete all log records older than**--Lets you delete all job records in the Activity Log that are older than the date that you specify.
- Click OK.

The records are deleted from the Activity Log.

View Status Information About Virtual Standby Jobs from the Virtual Standby Server

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

Optionally, you can access the status information from the Virtual Standby server or directly from the node. For information about how to access status information from the nodes, see [View Status Information About Virtual Standby Jobs from the Nodes](#) (see page 93).

Follow these steps:

1. Log in the Virtual Standby server.
Click Nodes on the Navigation bar to open the Node screen.
2. If there are in-progress Virtual Standby jobs, the phase of the job appears in the Job field as illustrated by the following screen:

<input type="checkbox"/>	Node Name	Policy	Virtual Machine N...	Job
<input checked="" type="checkbox"/>	 comp-001	New Policy	2k3x86d2d-1	 Connecting to 172.24.xxx.xxx

3. Click the phase to open the Virtual Standby Status Monitor dialog.
Note: For information about the fields that appear on the Virtual Standby Status Monitor, see [Virtual Standby Status Monitor](#) (see page 94).
4. Click Close to close the Virtual Standby Status Monitor dialog.

View Status Information About Virtual Standby Jobs from the Nodes

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

Optionally, you can access the status information from the Virtual Standby server or directly from the node. For information about how to access status information from the Virtual Standby server, see [View Status Information About Virtual Standby Jobs from the Virtual Standby Server](#) (see page 92).

Follow these steps:

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.

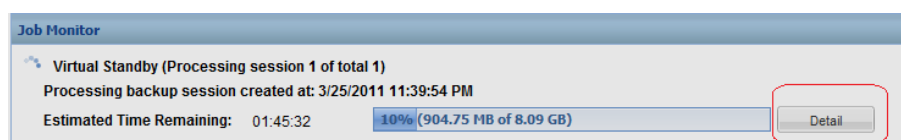
You are logged in to the CA ARCserve D2D node.

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 the Virtual Standby tab.

The Virtual Standby Summary screen opens.

If there is an in-progress Virtual Standby job, a status dialog appears in the Job Monitor field as illustrated by the following:



5. Click Detail to open the Virtual Standby Status Monitor.

Note: For information about the fields that appear on the Virtual Standby Status Monitor, see [Virtual Standby Status Monitor](#) (see page 94).

6. Click Close to close the Virtual Standby Status Monitor dialog.

Virtual Standby Status Monitor

The Virtual Standby Status Monitor displays the following real-time information about the Virtual Standby job:

Phase

Displays the current phase of the conversion process.

Cancel Job

Lets you terminate the conversion job.

Processing

Displays the overall progress of the conversion job and the session number of the recovery point that the application is converting.

Current Provision Point

Displays status information about the session that the application is converting.

Source sessions

Specifies the session number that the application is converting.

Start Time

Displays the date and time the application started to convert the session.

Elapsed Time

Displays the length of time that elapsed since the application started to convert the current session.

Throughput

Displays the rate that the application is converting the session.

Estimated Time Remaining

Displays the estimated length of time remaining to convert the current source session.

All Sessions

Displays status information about all of the sessions in the recovery point that the application is converting.

Number of Sessions Converted

Displays the total number sessions in the provision point that were converted.

Elapsed Time

Displays the length of time that elapsed since the application started to convert all sessions contained in the recovery point.

Estimated Time Remaining

Display the estimated length of time remaining to convert all sessions contained in the recovery point.

Number of Sessions Pending

Displays the number of sessions pending to be converted.

View Information About Policies Assigned to CA ARCserve D2D Nodes

The application lets you view information about the conversion policies that are assigned to CA ARCserve D2D nodes.

To view information about policies assigned 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.

You are logged in to 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 the Virtual Standby tab.

The Virtual Standby summary screen appears.

5. From the Virtual Standby Tasks list, click Virtual Standby Settings.

The Virtual Standby Settings dialog opens.

The Virtual Standby Settings dialog lets you view information about the Virtualization Server, the Virtual Machine, the Stand-in Server, and the Preferences defined in the policy that is assigned to the CA ARCserve D2D node. You cannot edit the policies assigned to the CA ARCserve D2D from the Virtual Standby Settings dialog.

Note: For information about how to edit policies, see [Edit Policies](#) (see page 58).

6. Click Cancel to close the Virtual Standby Settings dialog.

Virtual Standby Settings

The Virtual Standby Settings dialog contains information about the policy assigned to the node. You cannot edit policies from this dialog. For more information, see [Edit Policies](#) (see page 58).

The following options appear on the Virtual Standby tab:

Virtualization Server Options

■ VMware Systems:

The following options apply to VMware systems:

- **Virtualization type**--VMware.
- **ESX Host/vCenter**--Identifies the host name of the ESX or vCenter Server system.
- **User Name**--Identifies the user name that is required to log in to the VMware system.
- **Password**--Identifies that a password for User Name is required to log in to the VMware system.
- **Protocol**--Displays the communication protocol used between the source CA ARCserve D2D node and the monitoring server.
- **Port**--Identifies the port used for data transfer between the source server and the monitoring server.

■ Monitoring:

The following options apply to VMware systems.

- **Monitor Server**--Identifies the host name of the server that monitors the source server.
- **User Name**--Identifies the user name that is required to log in to the monitoring server.
- **Password**--Identifies that a password for User Name is required to log in to the monitor server.

- **Protocol**--Identifies the communication protocol used between the CA ARCserve Central Virtual Standby server and the ESX Server system (monitoring server).
- **Port**--Identifies the port used for data transfer between the CA ARCserve Central Virtual Standby server and the ESX Server system (monitoring server).
- **Use monitor server as proxy for data transfer**--Identifies that the monitor server copies the conversion data from the CA ARCserve D2D source server to the ESX Server datastore.

Note: The Use monitor server as proxy for data transfer option is enabled by default. You can disable this option to allow the CA ARCserve D2D source server to copy the conversion data directly to the ESX Server datastore.

■ **Hyper-V Systems:**

The following options apply to Hyper-V systems:

- **Virtualization type**--Hyper-V.
- **Hyper-V Host Name**--Identifies the host name of the Hyper-V system.
- **User Name**--Identifies the user name that is required to log in to the Hyper-V system.
- **Password**--Identifies that a password for User Name is required to log in to the Hyper-V system.
- **Port**--Identifies the port used for data transfer between the source server and the monitoring server.

Virtual Machine Options

■ **VMware Systems:**

- **VM Name Prefix**--Identifies the prefix added to the display name for the virtual machine on the ESX Server system.
Default value: CAVM_
- **VM Resource Pool**--Identifies the name of resource pool where the standby virtual machine is grouped.

- **Datastore**--Identifies the location where you want to store the conversion data.
 - **Use one datastore for all virtual machine source disks**--Indicates that the application copies all of the disks related to the virtual machine to one data store.
 - **Choose a datastore for each VM source disk**--Indicates that the application copies disk-related information for the virtual machine to the corresponding datastore.
- **Networks**--Identifies the NICs, virtual networks, and paths that the ESX Server system uses to communicate with the virtual machines.
 - **Connect all virtual NICs to the following virtual network**--Identifies the virtual NICs that are mapped to the virtual network. This option is specified when the virtual machine contains virtual NICs and a virtual network.
 - **Choose a virtual network for each virtual NIC**--Identifies the name of the virtual network that you want the NIC to use to communicate.
- **CPU Count**--Identifies the minimum and maximum CPU count supported by the standby virtual machine.
- **Memory**--Identifies the total amount of RAM in MB allocated for the standby virtual machine.
- **Hyper-V Systems:**
 - **VM Name Prefix**--Identifies the prefix added to the display name for the virtual machine on the Hyper-V system.
Default value: CAVM_
 - **Path**--Identifies the location on the Hyper-v Server where the conversion data is stored.
 - **Networks**--Identifies the NICs, virtual networks, and paths that the Hyper-V server uses to communicate with the virtual machines.
 - **CPU Count**--Identifies the minimum and maximum CPU count supported by the standby virtual machine.
 - **Memory**--Identifies the total amount of RAM in MB allocated to the standby virtual machine.

Stand-in Settings**■ Recovery:**

- **Manually start the Virtual Machine**--Indicates that the virtual machines are powered on and provisioned manually when the source server fails or stops communicating.
- **Automatically start the Virtual Machine**--Indicates that the virtual machines are powered on and provisioned automatically when the source server fails or stops communicating.

■ Heartbeat Properties:

- **Timeout**--Identifies the length time that the monitor server must wait for a heartbeat before it powers on a recovery point snapshot.
- **Frequency**--Identifies the frequency that the source server communicates heartbeats to the monitor server.

The following options appear on the Preferences tab:

■ Email Alerts:

- **Missing heartbeat for source machine**--Indicates that Virtual Standby sends alert notifications when the monitor server does not detect a heartbeat from the source server.
- **VM powered on for source machine configured with auto power ON**--Indicates that Virtual Standby sends alert notifications when it powers on a virtual machine that was configured to power on automatically when a heartbeat is not detected.
- **Missing heartbeat for source machine configured with manual power ON**--Indicates that Virtual Standby sends alert notifications when it does not detect a heartbeat from a source server that is not configured to power on automatically.
- **VM storage free space less than**--Indicates that Virtual Standby sends alert notifications when it detects insufficient free disk space on the defined hypervisor path. The detection occurs when the amount of free disk space is less than the user-defined threshold. The threshold can be defined either an absolute value (MB) or as a percentage of the capacity of the volume.
- **Virtual Standby errors/failure/crash**--Indicates that Virtual Standby sends alert notifications when it detects an error that occurred during the conversion process.
- **Virtual Standby success**--Indicates that the process of creating a virtual standby virtual machine completed successfully.

- **Hypervisor is not reachable**--Indicates that Virtual Standby sends alert notifications when it detects that it cannot communicate with the ESX Server system or the Hyper-V system.
- **License failure**--Indicates that Virtual Standby sends alert notifications upon detection of licensing problem on Virtual Standby servers, source servers, and monitoring servers.
- **The Virtual Standby did not start successfully from the Recovery Point Snapshot**--Indicates that the process of creating a virtual standby virtual machine from a recovery point snapshot did not complete successfully.

How to Protect Virtual Standby Virtual Machines

After a Virtual Standby virtual machine is powered on (either manually or automatically), the CA ARCserve D2D backup job and the Virtual Standby job do not run as they were scheduled. If you want to resume the jobs after the Virtual Standby virtual machine is powered on, do the following:

1. Modify the VM Name Prefix in the Virtual Standby policy.

When CA ARCserve Central Virtual Standby powers on Virtual Standby virtual machines, the application defines the virtual machine names of the powered on virtual machines as the concatenation of the VM Name Prefix option specified in the Virtual Standby policy and the host name of the source node.

Example:

- VM Name Prefix: AA_
- Host name of the source node: Server1
- Virtual machine name of the Virtual Standby virtual machine: AA_Server1

After the Virtual Standby virtual machines are powered on, virtual machine name conflicts can occur when you do not modify the VM Name Prefix in the Virtual Standby policy. Problems of this type occur when the source nodes and the Virtual Standby virtual machines reside on the same hypervisor.

For information about modifying the VM Name Prefix in the Virtual Standby policy, see [Edit Policies](#) (see page 58). If necessary, you can update other Virtual Standby policy settings. Optionally, you can create a new Virtual Standby Policy to protect the Virtual Standby virtual machine. For information about creating new policies, see [Create Policies](#) (see page 30).

2. After you update the policy or create a new policy, deploy the policy to the Virtual Standby virtual machine. For more information, see [Deploy Policies](#) (see page 40).
3. After you deploy the policy to the Virtual Standby virtual machine, resume the Virtual Standby job. For more information, see [Pause and Resume Virtual Standby Jobs](#) (see page 84).

4. After you deploy the policy, log in to CA ARCserve D2D on the Virtual Standby virtual machine and schedule a repeat method for the CA ARCserve D2D backup job. For more information, see the *CA ARCserve D2D User Guide*.

Note: CA ARCserve Central Protection Manager and CA ARCserve Central Virtual Standby have a mechanism that lets you automatically resynchronize the policies to the managed CA ARCserve D2D nodes on a weekly basis. This mechanism lets CA ARCserve Central Protection Manager restart the backup jobs on the Virtual Standby virtual machines by redeploying the policy that was in effect on the CA ARCserve D2D node to the Virtual Standby virtual machine. The policy deployment process behaves in this manner because the source node and the Virtual Standby virtual machine have the same host name, which lets CA ARCserve Central Protection Manager resynchronize the policy. The only limitation to this behavior is the CA ARCserve Central Protection Manager server and the Virtual Standby virtual machine must be able to communicate with each other through the network. After CA ARCserve Central Protection Manager resynchronizes and deploys the policy to the Virtual Standby virtual machine, you then resume the Virtual Standby job on the Virtual Standby virtual machine. For more information, see [Pause and Resume Virtual Standby Jobs](#) (see page 84).

Restore Data from CA ARCserve D2D Recovery Points

Virtual Standby lets you recover data from the available recovery points. The recovery points are point-in-time snapshots of data that resides on CA ARCserve D2D source nodes. From the recovery points you can specify the data that you want to recover.

To restore data from CA ARCserve D2D recovery points

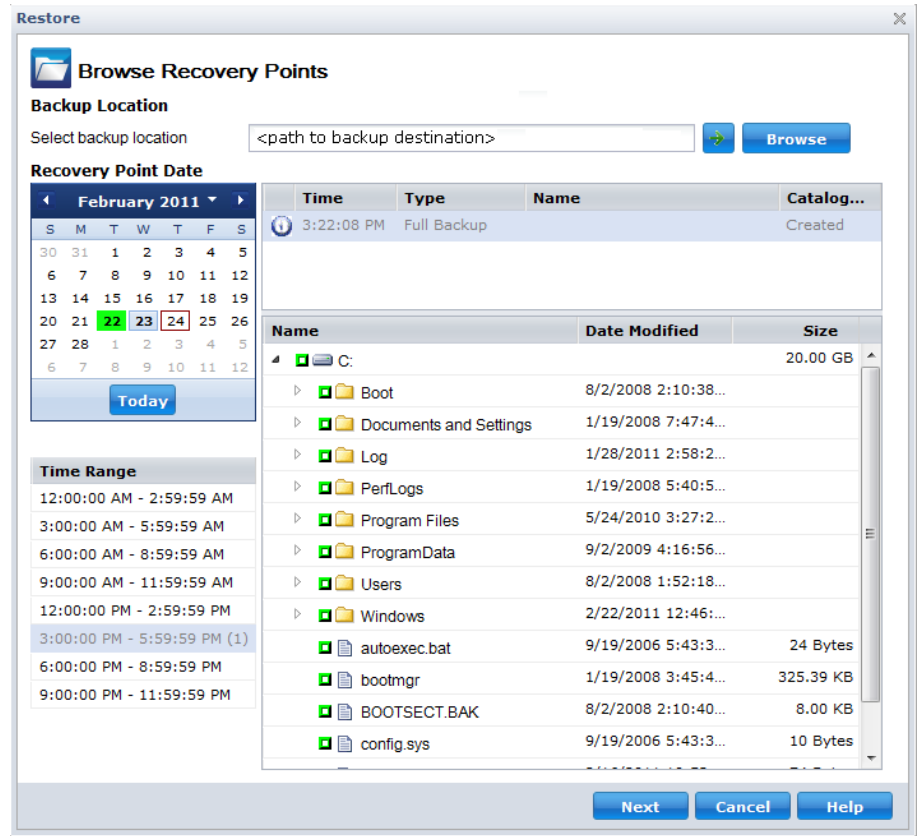
1. Log in to the application and click Node on the Navigation bar.

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 Browse Recovery Points dialog opens.



3. Specify the backup source. You can either specify a location or browse to the location where your backup images are stored. If necessary, enter the User name and Password credentials to gain access to that location. You can click green arrow validate icon to verify proper access to the source location.

The calendar view will highlight (in green) all dates during the displayed time period that contain recovery points for that backup source.

4. Specify the data that you want to restore.
 - a. Select the calendar date for the backup image you want to restore.

The corresponding recovery points for that date are displayed, along with the time of the backup, the type of backup that was performed, and the name of the backup.
 - b. Select a recovery point that you want to restore.

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

Note: A clock icon with a lock symbol indicates the recovery point contains encrypted information and may require a password for restore.
 - c. Select the content to be restored.
 - For a volume-level restore, you can specify to restore the entire volume or selected files/folders within the volume.
 - For an application-level restore, you can specify to restore the entire application or selected components, databases, instances, and so on within the application.

5. After you specify the data that you want to restore, click Next.

The Restore Options dialog opens.

6. Complete the following options on the Restore Options dialog:
 - **Destination**--Select the destination for the restore.
 - Restore to Original Location--Lets you restore data to the original location from where the backup image was captured.
 - Restore to--Lets you specify or browse to the location where your backup images will be restored. Click the arrow next to the Restore to field to verify the connection to the specified location.

If necessary, you will need to enter the User Name and Password credentials to gain access to that location.

- **Resolving Conflicts**--Lets you specify how you want CA ARCserve D2D to resolve conflicts that are encountered during the restore process.
 - Overwrite existing files--Lets you overwrite (replace) existing files that are located at the restore destination. All objects will be restored from the backup files regardless of their current presence on your machine.
 - Replace active files--Lets you replace active files upon reboot. If the restore attempt CA ARCserve D2D detects that the existing file is currently in use, it will not immediately replace that file, but instead to avoid any problems will delay the replacement of the active files until the next time the machine is rebooted. (The restore will occur immediately, but the replacement of any active files is done during the next reboot).

Note: If this option is not selected any active file will be skipped from the restore.
 - Rename files--Lets you create new files if the file name already exists. Selecting this option will copy the source file to the destination with the same filename but a different extension. Data will then be restored to the new file.
 - Skip existing files--Lets you skip over and not overwrite (replace) any existing files that are located at the restore destination. Only objects that do not currently exist on your computer will be restored from the backup files.

By default, this option is selected.

- **Directory Structure**--Lets you specify what CA ARCserve D2D will or will not do with the directory structure during the restore process.
 - Create root directory--Lets you specify that if a root directory structure exists in the captured backup image, CA ARCserve D2D will recreate that same root directory structure on the restore destination path.

When the Create Root Directory option is not selected (unchecked), the file/folder to be restored will be restored directly to the destination folder.

Example:

If during the backup you captured the files "C:\Folder1\SubFolder2\A.txt" and "C:\Folder1\SubFolder2\B.txt" and during the restore you specified to the restore destination as "D:\Restore".

If you select to restore the "A.txt" and "B.txt" files individually, the destination for the restored files will be "D:\Restore\A.txt" and "D:\Restore\B.txt" (the root directory above the specified file level will not be recreated).

If you select to restore from the "SubFolder2" level, the destination for the restored files will be "D:\Restore\SubFolder2\A.txt" and "D:\Restore\SubFolder2\B.txt" (the root directory above the specified folder level will not be recreated).

When the Create Root Directory option is selected (checked), the entire root directory path for the files/folders (including the volume name) will be recreated to the destination folder. If the files/folders to be restored are from the same volume name, then the destination root directory path will not include that volume name. However, if the files/folders to be restored are from different volume names, then the destination root directory path will include the volume name.

Example:

If during the backup you captured the files "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", and also E:\Folder3\SubFolder4\C.txt" and during the restore you specified to the restore destination as "D:\Restore".

If you select to restore just the "A.txt" file, the destination for the restored file will be "D:\Restore\Folder1\SubFolder2\A.txt" (the entire root directory without the volume name will be recreated).

If you select to restore both the "A.txt" and "C.txt" files, the destination for the restored files will be "D:\Restore\C\Folder1\SubFolder2\A.txt" and "D:\Restore\E\Folder3\SubFolder4\C.txt" (the entire root directory with the volume name will be recreated).

- **Encryption Password**--If the recovery point data you are trying to restore is encrypted, you may need to provide the encryption password.

A password is not required if you are attempting to restore to the same machine from where the encrypted backup was performed. However, if you are attempting to restore to a different machine, a password is required.

Note: The following icons indicate whether the recovery point contains encrypted information and may require a password for restore.

Non-encrypted recovery point:



Encrypted recovery point:



Click Next.

The Restore Summary dialog opens.

7. Verify that the information on the Restore Summary dialog is correct.

Note: If you want to change the restore options that you specified, click Previous and go back to the applicable dialog to change the values.

Click Finish.

The restore options are applied and the data is recovered.

Restore Data from CA ARCserve D2D File Copies

Virtual Standby lets you recover data from CA ARCserve D2D file copies. Files copies are copies of CA ARCserve D2D recovery points that you copy to offline storage, such as a disk or the cloud. From the file copies, you can specify the data that you want to recover.

To restore data from CA ARCserve D2D file copies

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

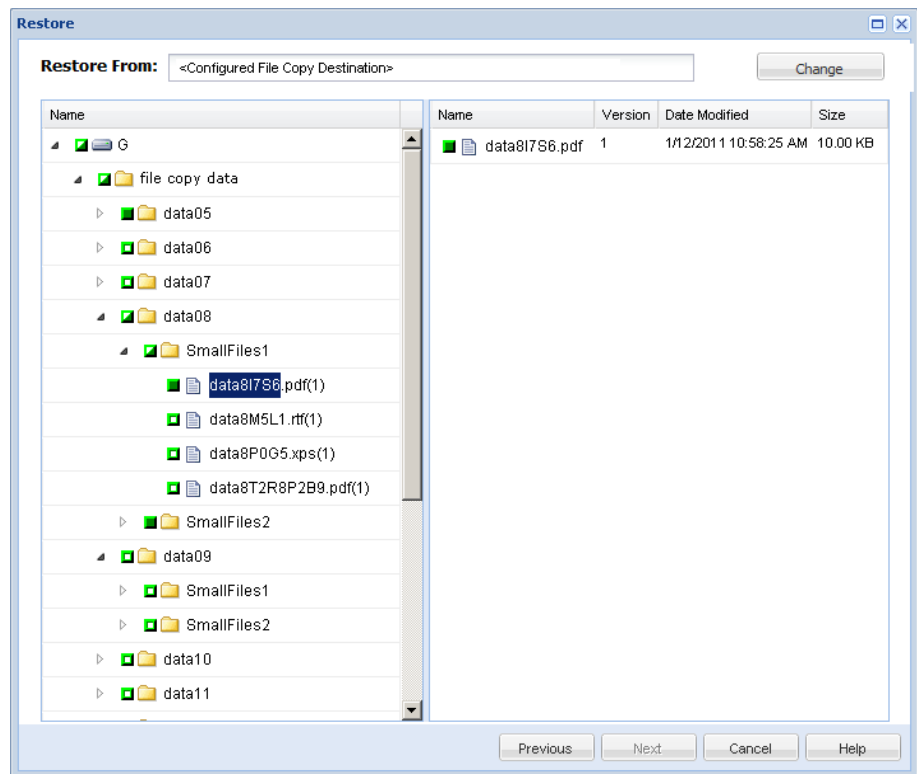
From the Node screen, expand the group containing the node that you want to restore.

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 File Copies.

The Browse File Copies dialog opens as illustrated by the following dialog.

Note: The destination that is currently showing in the right pane is the default destination.

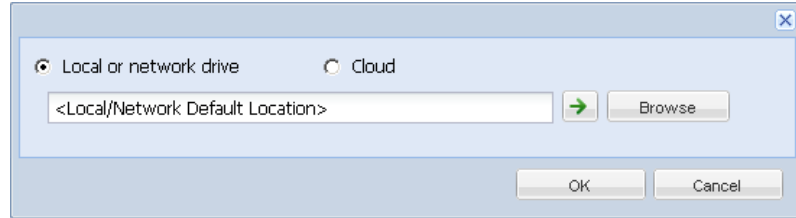


3. From the Name pane, specify the file copy data that you want to recover. You can specify any combination of files and folders, or the volume.

When you select an individual file to be restored, all file copied versions of that file will be displayed in the right pane. If multiple versions are available, select the version of file copy that you want to recover.

- **Change Destination**--Lets you browse to an alternative location where your file copy images are stored.

A dialog opens that displays the available alternative destination options.



- **Local or network drive**--The Select a Backup Location dialog opens, allowing you to browse to and select an alternate local or network drive location.
 - **Cloud**--The Cloud Configuration dialog opens, allowing you to access and select an alternate cloud location.
4. Click Next.

The Restore Options dialog opens.

5. Complete the following options on the Restore Options dialog:

- **Destination**--Select the destination for the restore.
 - Restore to Original Location--Lets you restore data to the original location from where the backup image was captured.
 - Restore to--Lets you specify or browse to the location where your backup images will be restored. Click the arrow next to the Restore to field to verify the connection to the specified location.

If necessary, you will need to enter the User Name and Password credentials to gain access to that location.

- **Resolving Conflicts**--Lets you specify how you want CA ARCserve D2D to resolve conflicts that are encountered during the restore process.
 - Overwrite existing files--Lets you overwrite (replace) existing files that are located at the restore destination. All objects will be restored from the backup files regardless of their current presence on your machine.
 - Replace active files--Lets you replace active files upon reboot. If the restore attempt CA ARCserve D2D detects that the existing file is currently in use, it will not immediately replace that file, but instead to avoid any problems will delay the replacement of the active files until the next time the machine is rebooted. (The restore will occur immediately, but the replacement of any active files is done during the next reboot).

Note: If this option is not selected any active file will be skipped from the restore.
 - Rename files--Lets you create new files if the file name already exists. Selecting this option will copy the source file to the destination with the same filename but a different extension. Data will then be restored to the new file.
 - Skip existing files--Lets you skip over and not overwrite (replace) any existing files that are located at the restore destination. Only objects that do not currently exist on your computer will be restored from the backup files.

By default, this option is selected.

- **Directory Structure**--Lets you specify what CA ARCserve D2D will or will not do with the directory structure during the restore process.

- Create root directory--Lets you specify that if a root directory structure exists in the captured backup image, CA ARCserve D2D will recreate that same root directory structure on the restore destination path.

When the Create Root Directory option is not selected (unchecked), the file/folder to be restored will be restored directly to the destination folder.

Example:

If during the backup you captured the files "C:\Folder1\SubFolder2\A.txt" and "C:\Folder1\SubFolder2\B.txt" and during the restore you specified to the restore destination as "D:\Restore".

If you select to restore the "A.txt" and "B.txt" files individually, the destination for the restored files will be "D:\Restore\A.txt" and "D:\Restore\B.txt" (the root directory above the specified file level will not be recreated).

If you select to restore from the "SubFolder2" level, the destination for the restored files will be "D:\Restore\SubFolder2\A.txt" and "D:\Restore\SubFolder2\B.txt" (the root directory above the specified folder level will not be recreated).

When the Create Root Directory option is selected (checked), the entire root directory path for the files/folders (including the volume name) will be recreated to the destination folder. If the files/folders to be restored are from the same volume name, then the destination root directory path will not include that volume name. However, if the files/folders to be restored are from different volume names, then the destination root directory path will include the volume name.

Example:

If during the backup you captured the files "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", and also E:\Folder3\SubFolder4\C.txt" and during the restore you specified to the restore destination as "D:\Restore".

If you select to restore just the "A.txt" file, the destination for the restored file will be "D:\Restore\Folder1\SubFolder2\A.txt" (the entire root directory without the volume name will be recreated).

If you select to restore both the "A.txt" and "C.txt" files, the destination for the restored files will be "D:\Restore\C\Folder1\SubFolder2\A.txt" and "D:\Restore\E\Folder3\SubFolder4\C.txt" (the entire root directory with the volume name will be recreated).

- **Encryption Password**--If the recovery point data you are trying to restore is encrypted, you may need to provide the encryption password.

A password is not required if you are attempting to restore to the same machine from where the encrypted backup was performed. However, if you are attempting to restore to a different machine, a password is required.

Note: The following icons indicate whether the recovery point contains encrypted information and may require a password for restore.

Non-encrypted recovery point:



Encrypted recovery point:



Click Next.

The Restore Summary dialog opens.

6. Verify that the information on the Restore Summary dialog is correct.

Note: If you want to change the restore options that you specified, click Previous and go back to the applicable dialog to change the values.

Click Finish.

The restore options are applied and the data is recovered.

Restore Data Using Find Files/Folders to Restore

Virtual Standby lets you search CA ARCserve D2D recovery points and file copies for specific files or folders to restore.

To restore data using Find Files/Folders to Restore

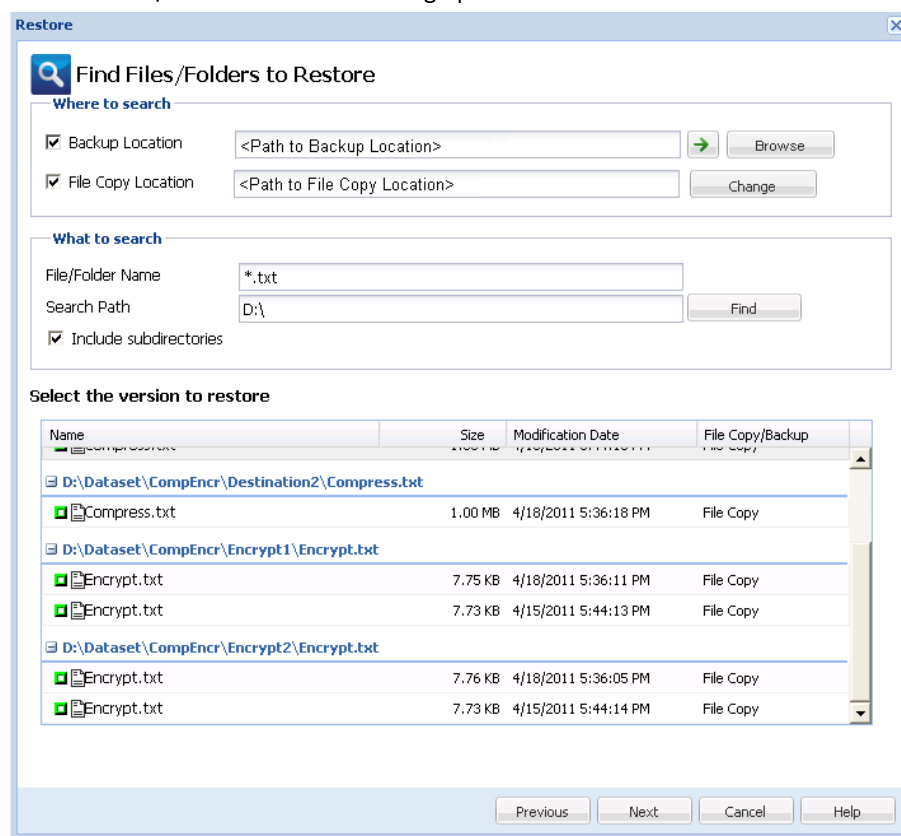
1. Log in to the application and click Node on the Navigation bar.

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.

The Find Files/Folders to Restore dialog opens.



3. Specify where to search (backup and/or archive source).

You can either specify a location or browse to the location where your backup/archive images are stored. If necessary, enter the User name and Password credentials to gain access to that location. You can click green arrow validate icon to verify proper access to the source location.

- Specify what to search for (file or folder name to restore).

Note: The File Name field supports full name searching and wildcard searching. If you do not know the complete file name, you can simplify the results of the search by specifying the wildcard characters "*" and "?" in the File Name field.

The wildcard characters supported for the file or folder name are as follows:

- "*" - Use the asterisk to substitute zero or more characters in a file or folder name.
- "?" - Use the question mark to substitute a single character in a file or folder name.

For example, if you specify *.txt, all files with a .txt file extension appear in the search results.

Note: If necessary, you can also specify a path to further filter your search and select whether to include or not include any subdirectories.

- Click Find to launch the search.

The results of the search display. If the search discovers multiple occurrences (recovery points) of the same searched file, it will list all occurrences sorted by date (with the most recent listed first). It will also indicate if the searched file has been backed up or archived.

- Select the version (occurrence) of the file/folder that you want to restore and click Next.

The Restore Options dialog opens.

- Complete the following options on the Restore Options dialog:

- **Destination**--Select the destination for the restore.
 - Restore to Original Location--Lets you restore data to the original location from where the backup image was captured.
 - Restore to--Lets you specify or browse to the location where your backup images will be restored. Click the arrow next to the Restore to field to verify the connection to the specified location.

If necessary, you will need to enter the User Name and Password credentials to gain access to that location.

- **Resolving Conflicts**--Lets you specify how you want CA ARCserve D2D to resolve conflicts that are encountered during the restore process.
 - Overwrite existing files--Lets you overwrite (replace) existing files that are located at the restore destination. All objects will be restored from the backup files regardless of their current presence on your machine.
 - Replace active files--Lets you replace active files upon reboot. If the restore attempt CA ARCserve D2D detects that the existing file is currently in use, it will not immediately replace that file, but instead to avoid any problems will delay the replacement of the active files until the next time the machine is rebooted. (The restore will occur immediately, but the replacement of any active files is done during the next reboot).

Note: If this option is not selected any active file will be skipped from the restore.
 - Rename files--Lets you create new files if the file name already exists. Selecting this option will copy the source file to the destination with the same filename but a different extension. Data will then be restored to the new file.
 - Skip existing files--Lets you skip over and not overwrite (replace) any existing files that are located at the restore destination. Only objects that do not currently exist on your computer will be restored from the backup files.

By default, this option is selected.

- **Directory Structure**--Lets you specify what CA ARCserve D2D will or will not do with the directory structure during the restore process.
 - Create root directory--Lets you specify that if a root directory structure exists in the captured backup image, CA ARCserve D2D will recreate that same root directory structure on the restore destination path.

When the Create Root Directory option is not selected (unchecked), the file/folder to be restored will be restored directly to the destination folder.

Example:

If during the backup you captured the files "C:\Folder1\SubFolder2\A.txt" and "C:\Folder1\SubFolder2\B.txt" and during the restore you specified to the restore destination as "D:\Restore".

If you select to restore the "A.txt" and "B.txt" files individually, the destination for the restored files will be "D:\Restore\A.txt" and "D:\Restore\B.txt" (the root directory above the specified file level will not be recreated).

If you select to restore from the "SubFolder2" level, the destination for the restored files will be "D:\Restore\SubFolder2\A.txt" and "D:\Restore\SubFolder2\B.txt" (the root directory above the specified folder level will not be recreated).

When the Create Root Directory option is selected (checked), the entire root directory path for the files/folders (including the volume name) will be recreated to the destination folder. If the files/folders to be restored are from the same volume name, then the destination root directory path will not include that volume name. However, if the files/folders to be restored are from different volume names, then the destination root directory path will include the volume name.

Example:

If during the backup you captured the files "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", and also E:\Folder3\SubFolder4\C.txt" and during the restore you specified to the restore destination as "D:\Restore".

If you select to restore just the "A.txt" file, the destination for the restored file will be "D:\Restore\Folder1\SubFolder2\A.txt" (the entire root directory without the volume name will be recreated).

If you select to restore both the "A.txt" and "C.txt" files, the destination for the restored files will be "D:\Restore\C\Folder1\SubFolder2\A.txt" and "D:\Restore\E\Folder3\SubFolder4\C.txt" (the entire root directory with the volume name will be recreated).

- **Encryption Password**--If the recovery point data you are trying to restore is encrypted, you may need to provide the encryption password.

A password is not required if you are attempting to restore to the same machine from where the encrypted backup was performed. However, if you are attempting to restore to a different machine, a password is required.

Note: The following icons indicate whether the recovery point contains encrypted information and may require a password for restore.

Non-encrypted recovery point:



Encrypted recovery point:



Click Next.

The Restore Summary dialog opens.

8. Verify that the information on the Restore Summary dialog is correct.

Note: If you want to change the restore options that you specified, click Previous and go back to the applicable dialog to change the values.

Click Finish.

The restore options are applied and the data is recovered.

Recovering Source Servers Using Bare Metal Recovery

After you correct the problems or perform maintenance on your source servers, Virtual Standby lets you recover the source servers to their last healthy state, and include the incremental changes that occurred while the Recovery Point Snapshot was powered on.

This recovery process is called a V2P (virtual to physical) recovery.

The V2P recovery process leverages the CA ARCserve D2D Bare Metal Recovery (BMR) process to restore data from virtual machines to physical machines. 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.

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.

The application lets you recover data using the methods described in the following table:

Recovery Method	More Information
Recover source servers from data that was backed up using CA ARCserve D2D.	Recover Source Servers Using CA ARCserve D2D Backup Data (see page 118).

Recovery Method	More Information
Recover source servers from data that was converted to Hyper-V-based Virtual Standby virtual machines.	Recover Source Servers Using Data from Hyper-V Virtual Standby Virtual Machines (see page 133).
Recover source servers from data that was converted to VMware-based Virtual Standby virtual machines.	Recover Source Servers Using Data From VMware Virtual Standby Virtual Machines (see page 146).

Recover Source Servers Using CA ARCserve D2D Backup Data

The application lets you recover source servers from data that was backed up using CA ARCserve D2D.

Note: The application uses the bare metal recovery process to recover source servers from CA ARCserve D2D backup data. For more information, see [Recovering Source Servers Using Bare Metal Recovery](#) (see page 116).

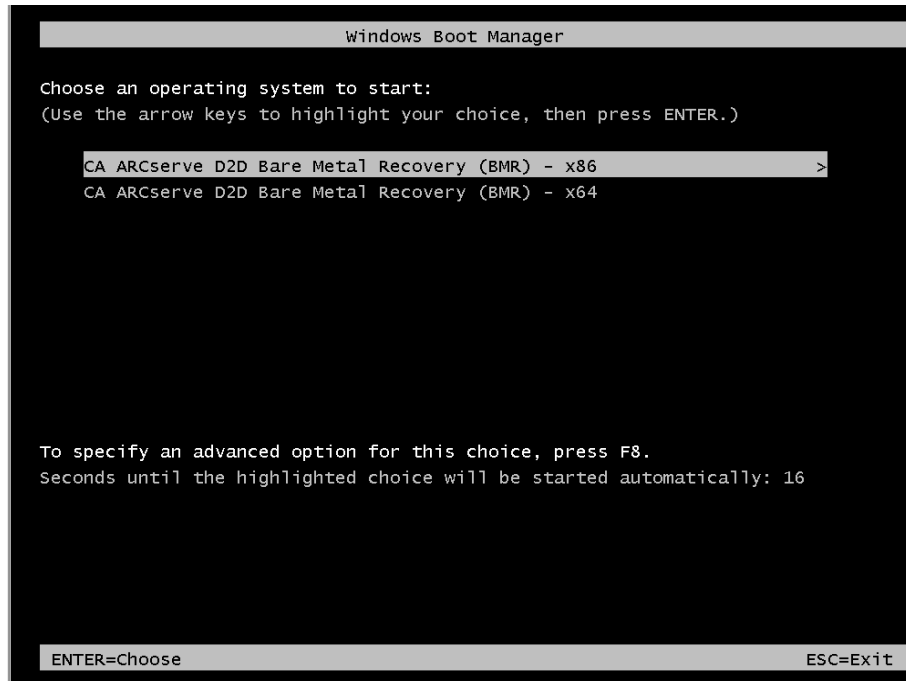
To recover source servers using CA ARCserve D2D backup data

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.

- 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.



3. The CA ARCserve D2D language select screen is displayed. Select a language and press "Next" to continue.

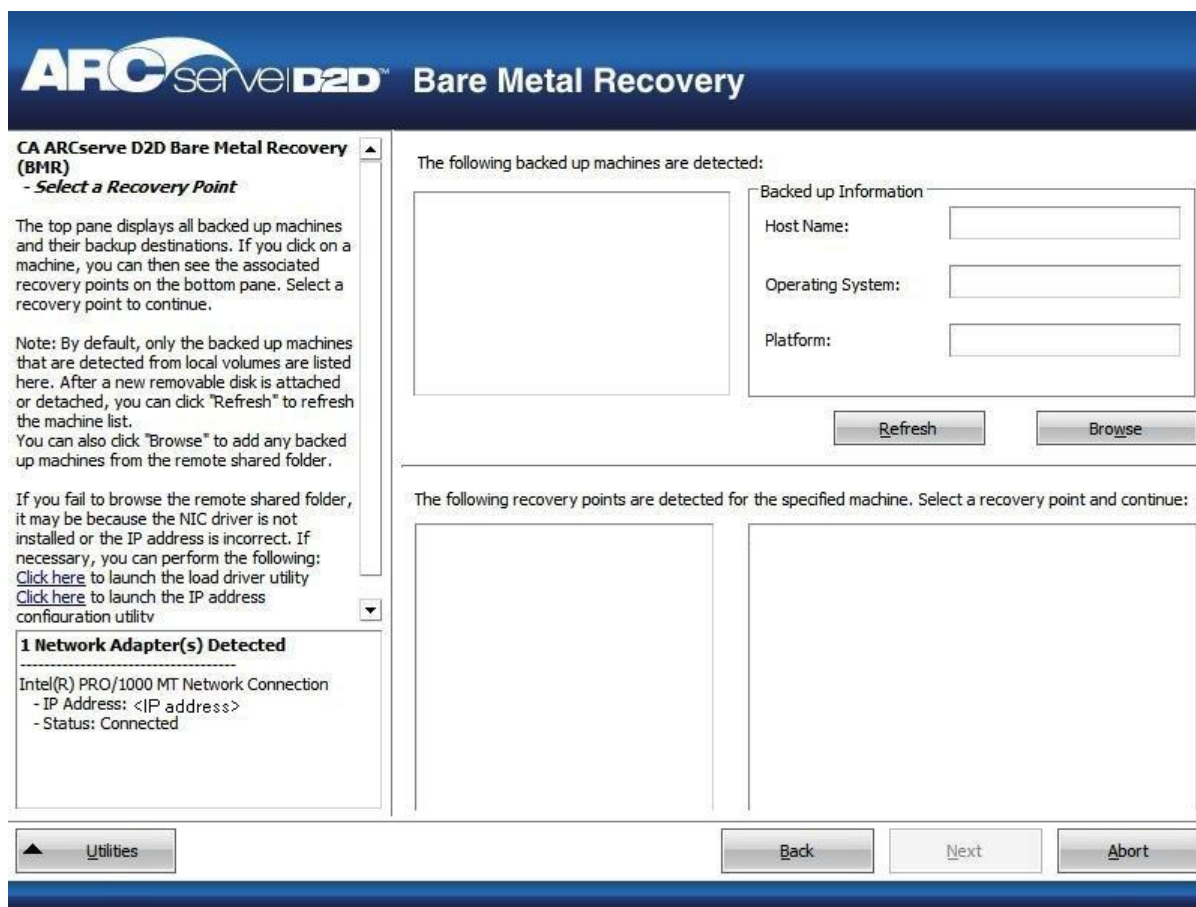
Note: If you perform BMR with a BMR USB stick and a Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 installation media (CD/DVD) not supported with a Multilingual User Interface (MUI), the language select screen is suppressed.



The Bare Metal Recovery process is initiated and the initial BMR wizard screen is displayed.



4. Click Recover data backed up using CA ARCserve D2D and then click Next.
The Select a Recovery Point wizard screen is displayed.



5. From the Select a Recovery Point wizard screen, select the machine (or volume) which contains recovery points for your backup image.

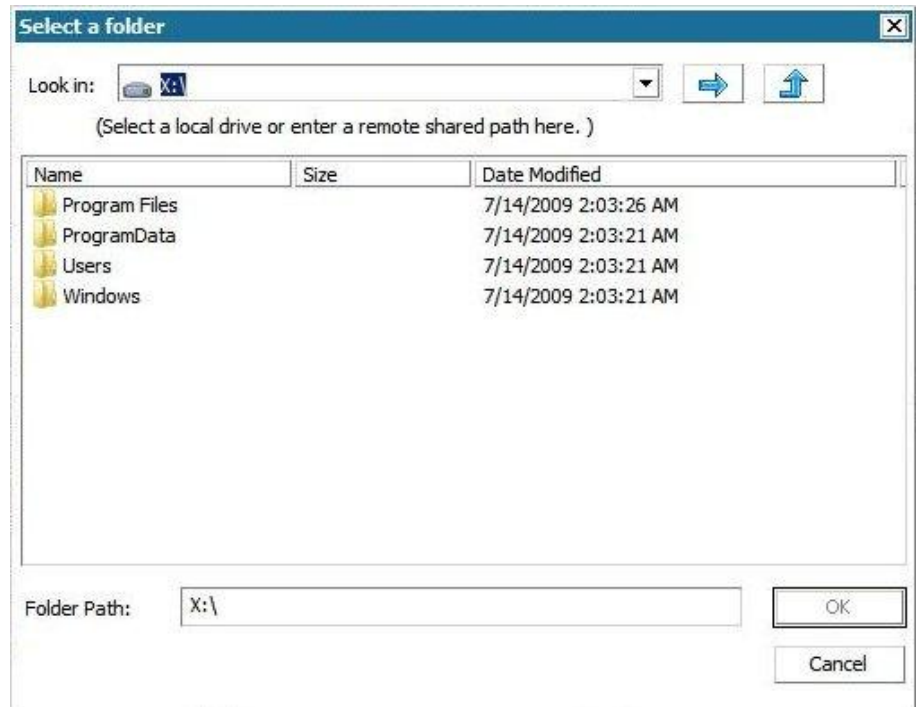
CA ARCserve D2D lets you recover from any local drive or from a network share.

- If you are recovering from a local backup, the BMR wizard automatically detects and displays all volumes that contain recovery points.
- If you are recovering from a remote share, you must browse to the remote location where the recovery points are stored. If there are multiple machines that contain recovery points, all machines are displayed.

You may also need access information (User Name and Password) for the remote machine.

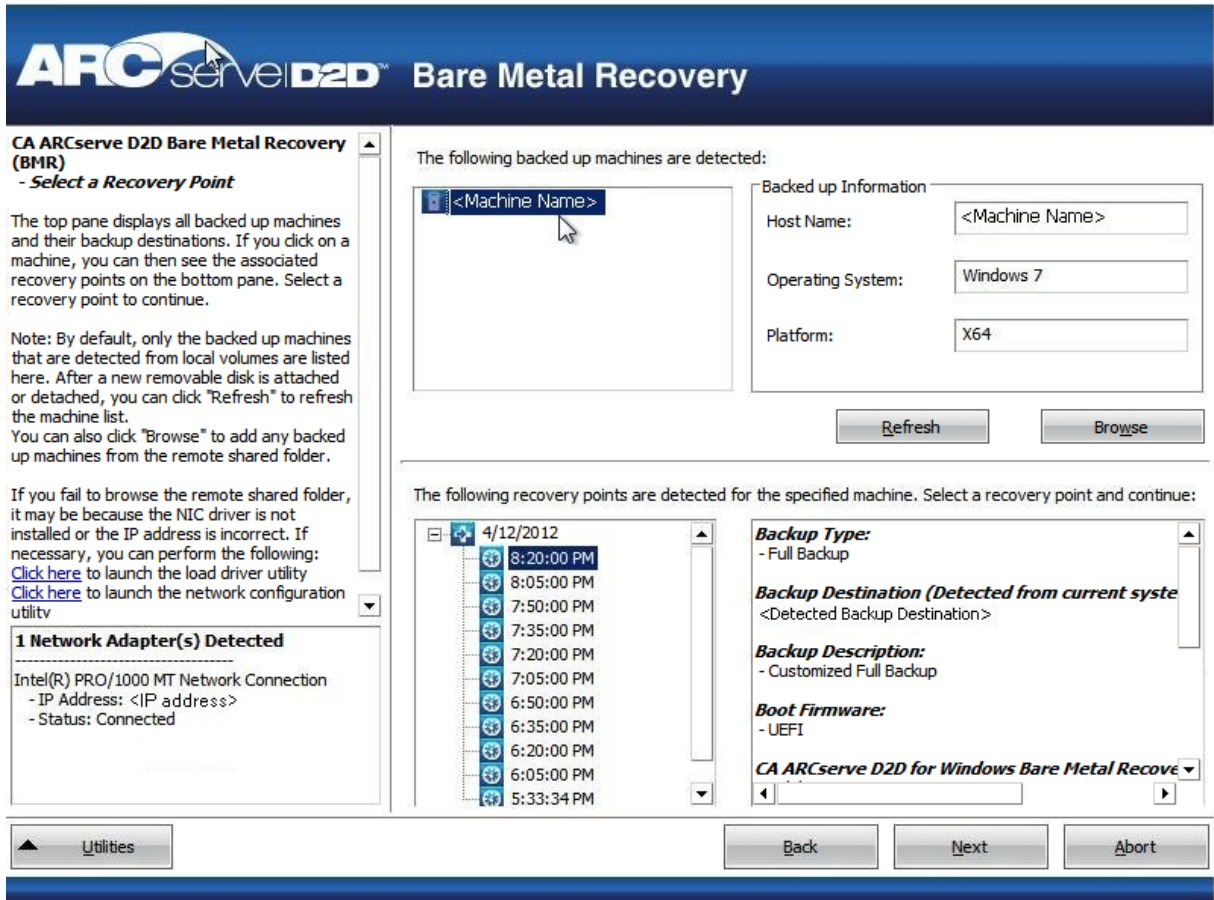
Note: The network must be up and running to browse to remote recovery points. If necessary you can check/refresh your network configuration information or load any missing drivers from the Utilities menu.

6. If the BMR module cannot detect any local destination volume, the "Select a Folder" dialog is automatically displayed and you must provide the remote share where the backups are residing.



7. 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).

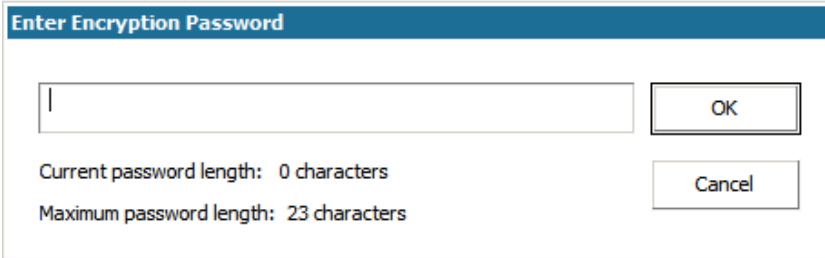
The BMR wizard screen now displays the machine name (in the upper left pane), with the related backup information (in the upper right pane) and all the corresponding recovery points (in the lower left pane).



8. Select which recovery point to restore.

The related information for the selected recovery point is displayed (in the lower right pane). This display includes such information as the type of backup that was performed (and saved), the backup destination, and the volumes that were backed up.

If the recovery point contains encrypted sessions (the recovery point clock icon includes a lock), a password required screen appears. Enter the session password and click OK.



Enter Encryption Password

OK

Cancel

Current password length: 0 characters

Maximum password length: 23 characters

Note: If your machine is a Domain Controller, CA ARCserve D2D supports a non-authoritative restore of the active directory (AD) database file during BMR. (Restore of MSCS clusters are not supported).

9. Verify this is the recovery point that you want to restore and click Next.

A BMR wizard screen is displayed with the available recovery mode options.



10. 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.

11. Click Next.

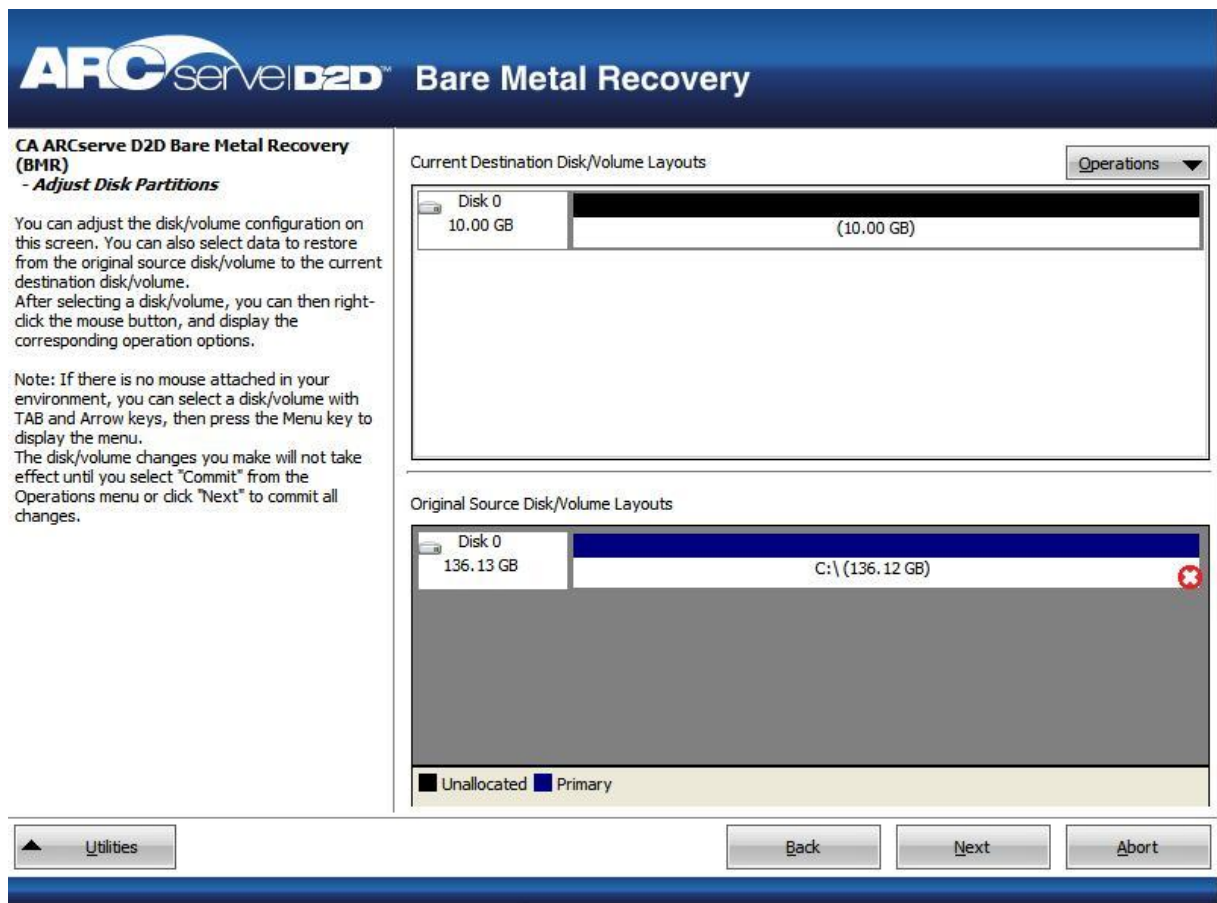
The BMR utility starts locating the machine that is going to be recovered and displays the corresponding disk partition information.

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.



- 12. If the current disk information you are seeing does not appear correct, you can access the Utilities menu and check for missing drivers.
- 13. If necessary, on the target volume pane you can click the Operations drop-down menu to display the available options.

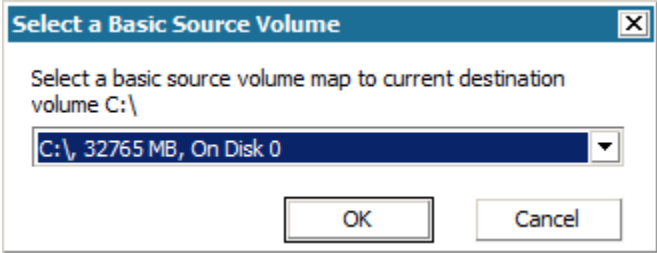
From this menu, you can reset any existing partitions or you can create new partitions to correspond to the disk partitions on the source volume. (Reset means to reload the source and target disk layout information from the configure file and current OS, and discard any user changed disk layout information).

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.



- 14. 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.

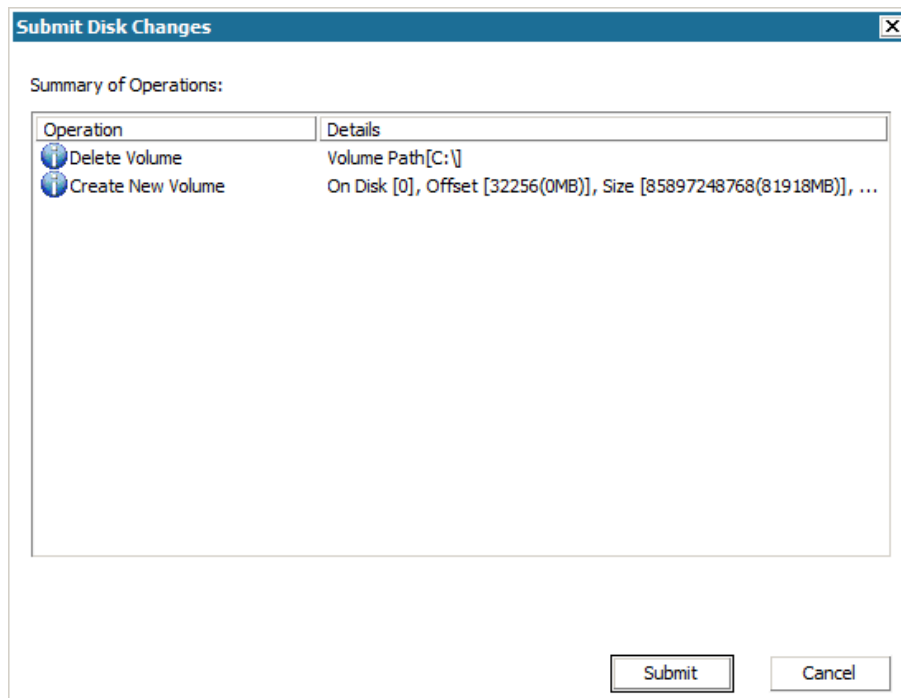
The Select a Basic Source Volume dialog opens.



- 15. 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.

16. 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.



17. When you have verified the summary information is correct, click Submit. (If the information is not correct, click Cancel).

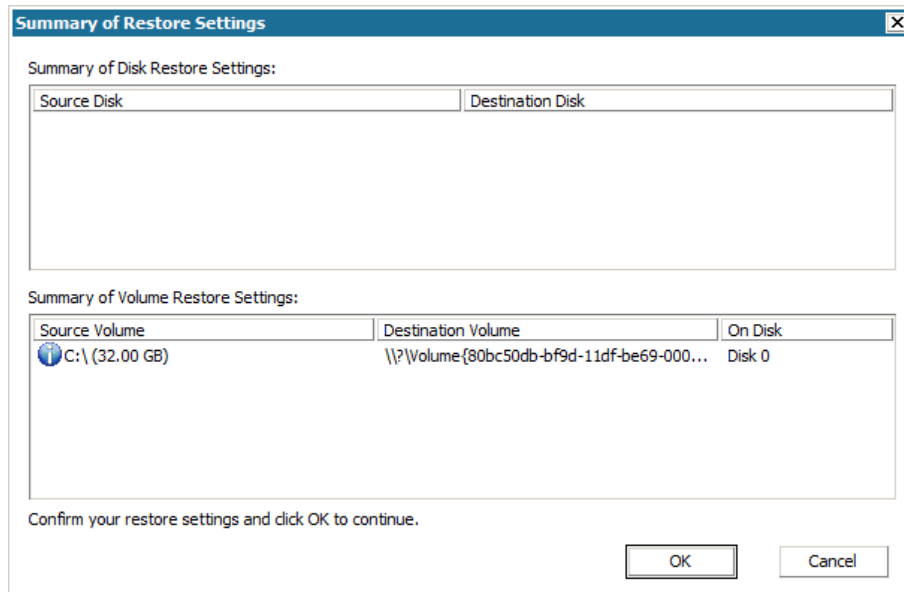
Note: All operations to the hard drive do not take effect until you submit it.

On the target machine, the new volumes are created and mapped to the corresponding source machine.

18. 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.

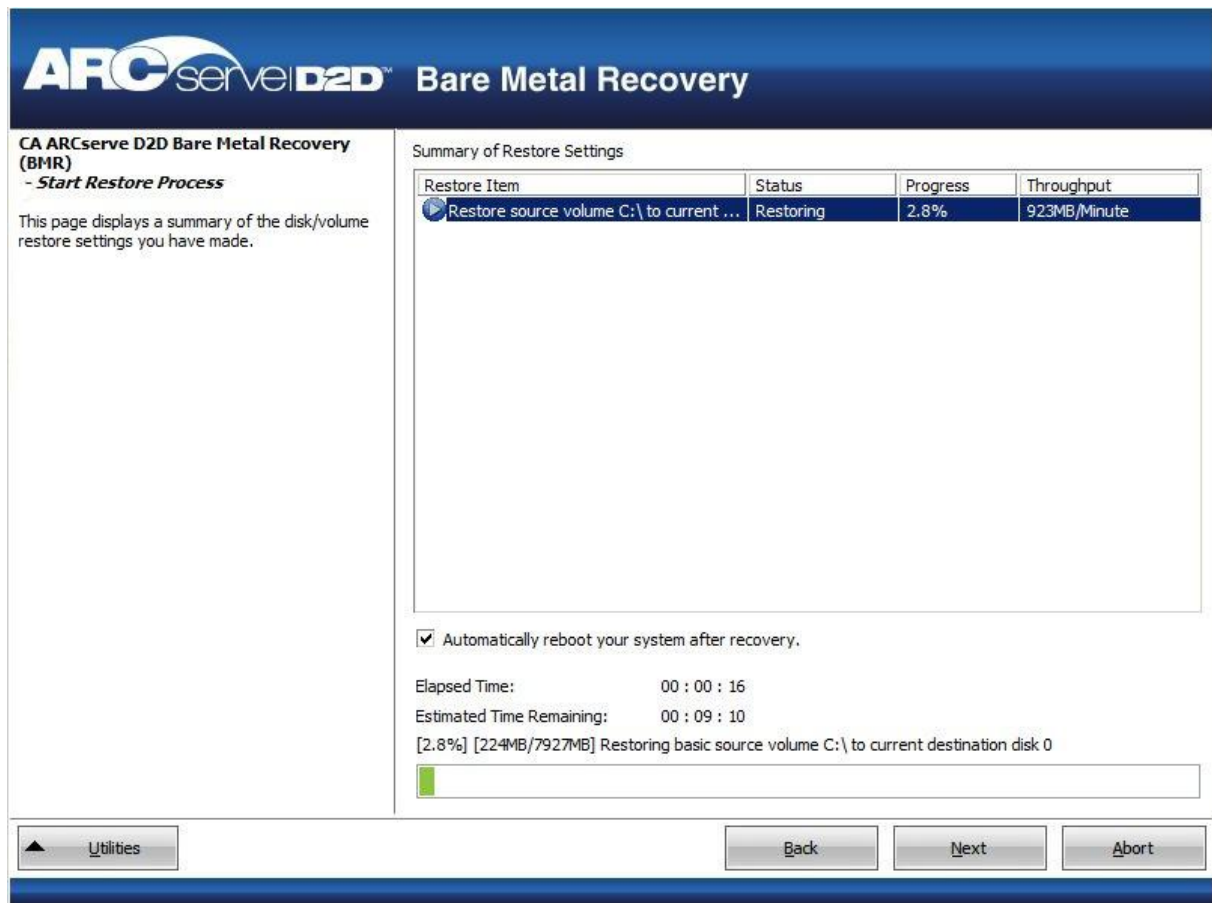
Note: On the bottom of restore summary window, the drive letters listed in "Destination Volume" column are automatically generated from the Windows Preinstallation Environment (WinPE). They can be different from the drive letters listed in "Source Volume" column. However, the data is still restored to proper volume even if drive letters are different.



19. 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.



20. 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.

21. 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.

22. When the BMR process is completed, a confirmation notification is displayed.

Notes: After completion of BMR:

- The first backup that is performed is a Verify Backup.
- Verify that the BIOS is configured to boot from the disk on which the boot volume was restored to.
- When the machine has been rebooted, you may need to configure the network adapters manually if you restored to dissimilar hardware.
- For dynamic disks, if the status of the disk is offline, you can manually change it to online from the disk management UI (accessed by running the Diskmgmt.msc control utility).
- For dynamic disks, if the dynamic volumes are in a failed redundancy status, you can manually resynchronize the volumes from the disk management UI (accessed by running the Diskmgmt.msc control utility).

Recover Source Servers Using Data from Hyper-V Virtual Standby Virtual Machines

The application lets you recover source servers using CA ARCserve D2D data that was converted to Hyper-V Virtual Standby virtual machines.

Note: The application uses the bare metal recovery process to recover source servers from Hyper-V virtual machines. For more information, see [Recovering Source Servers Using Bare Metal Recovery](#) (see page 116).

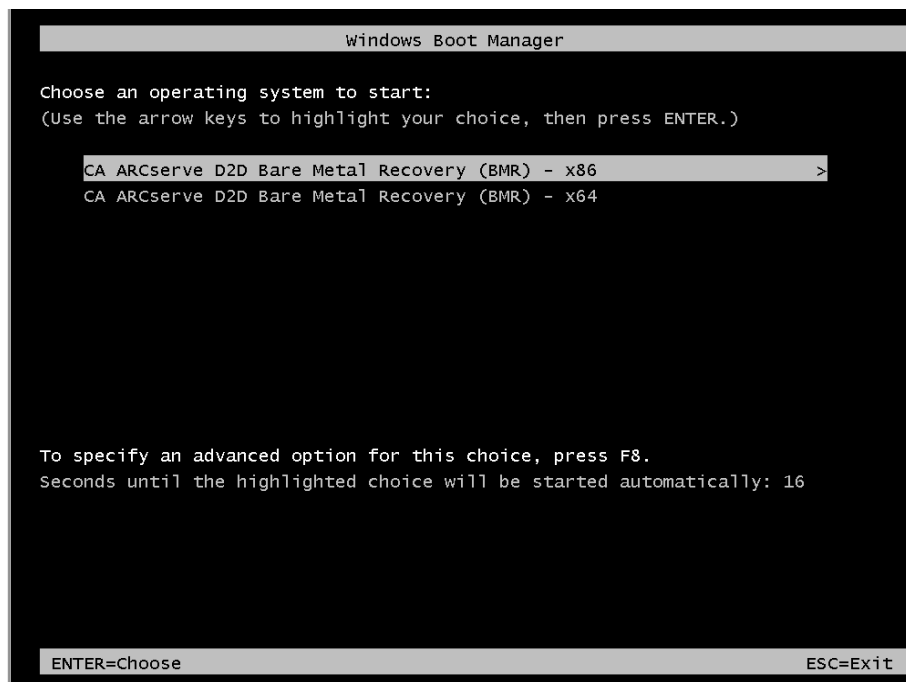
To recover source servers using data from Hyper-V Virtual Standby virtual machines

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.



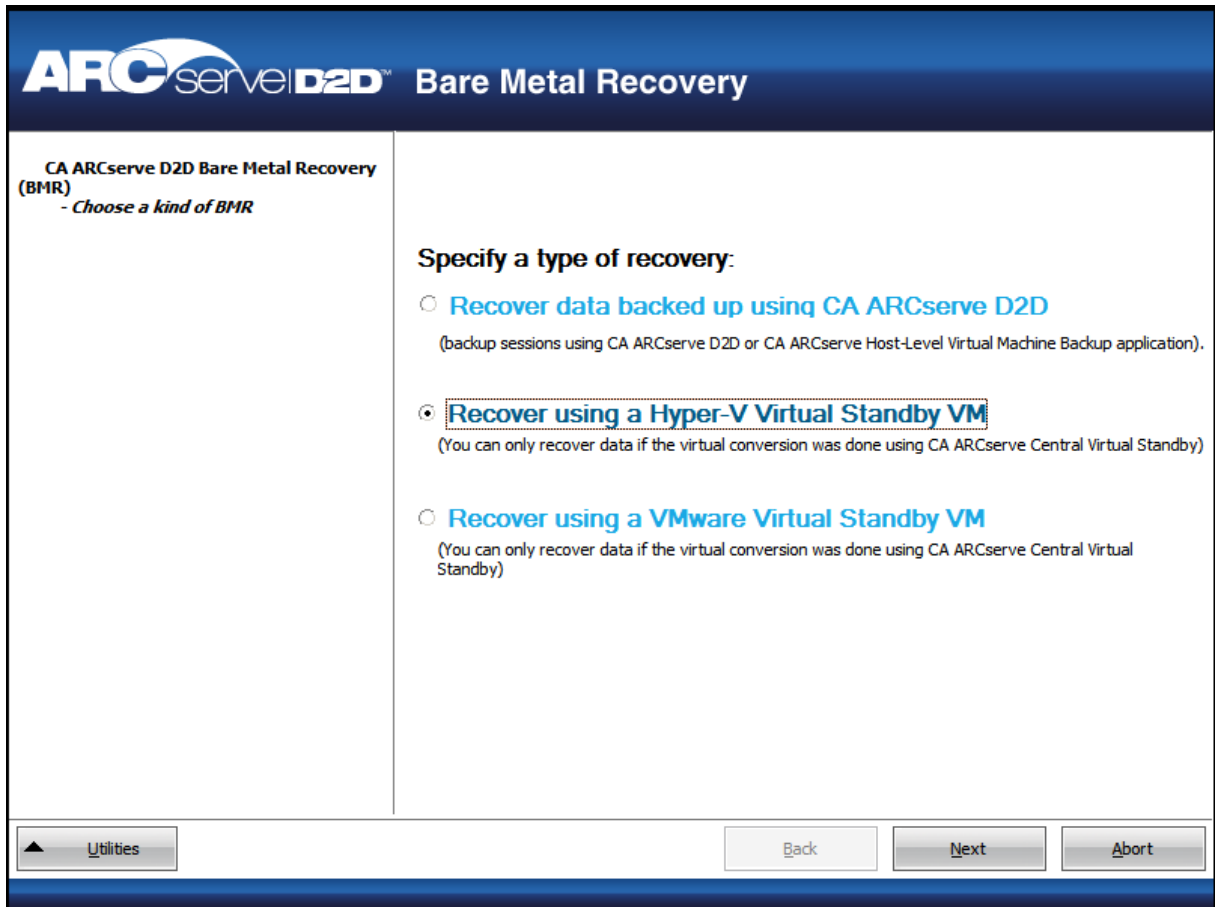
3. The CA ARCserve D2D language select screen is displayed. Select a language and press "Next" to continue.

Note: If you perform BMR with a BMR USB stick and a Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 installation media (CD/DVD) not supported with a Multilingual User Interface (MUI), the language select screen is suppressed.



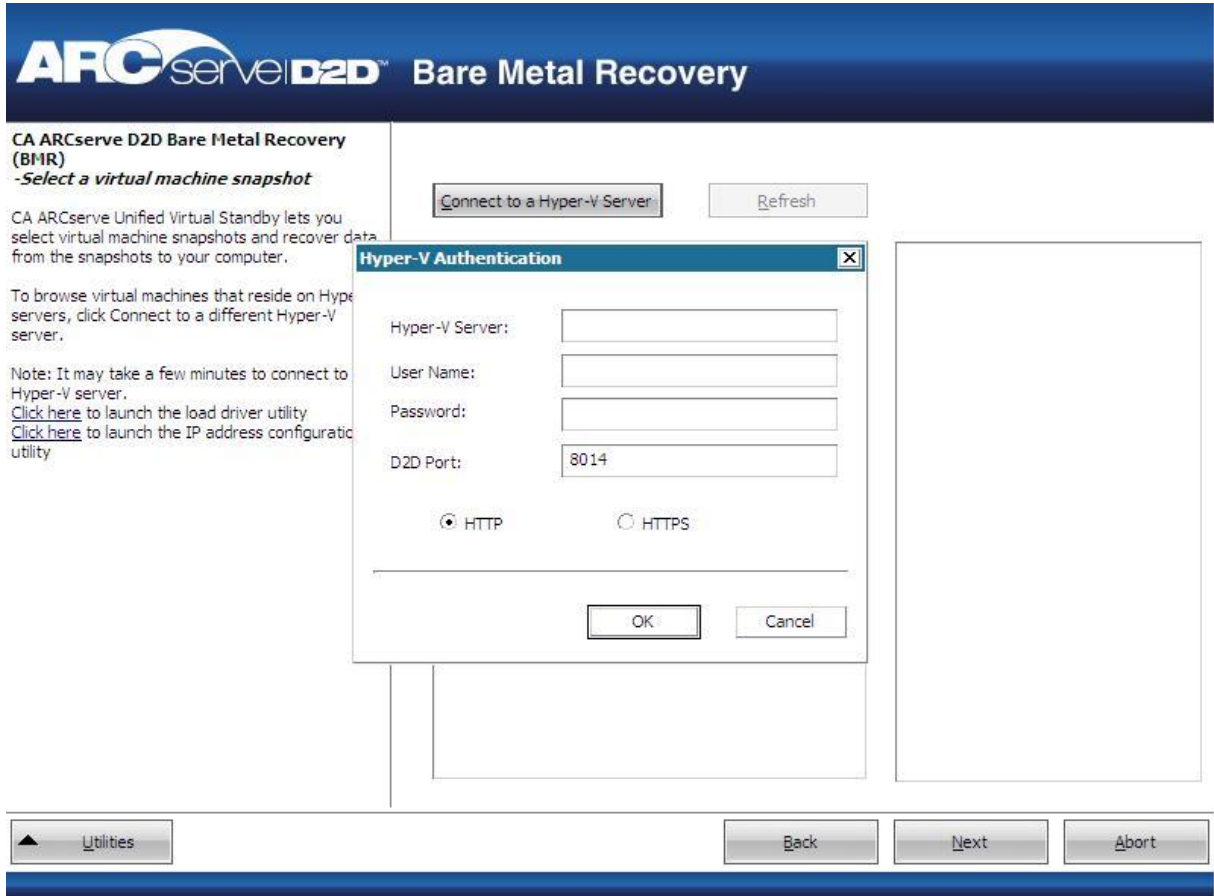
The Bare Metal Recovery process is initiated and the initial BMR wizard screen is displayed.

4. From the select the Type of Bare Metal Recovery (BMR) wizard screen, select the Recover using a Hyper-V Virtual Standby VM option.



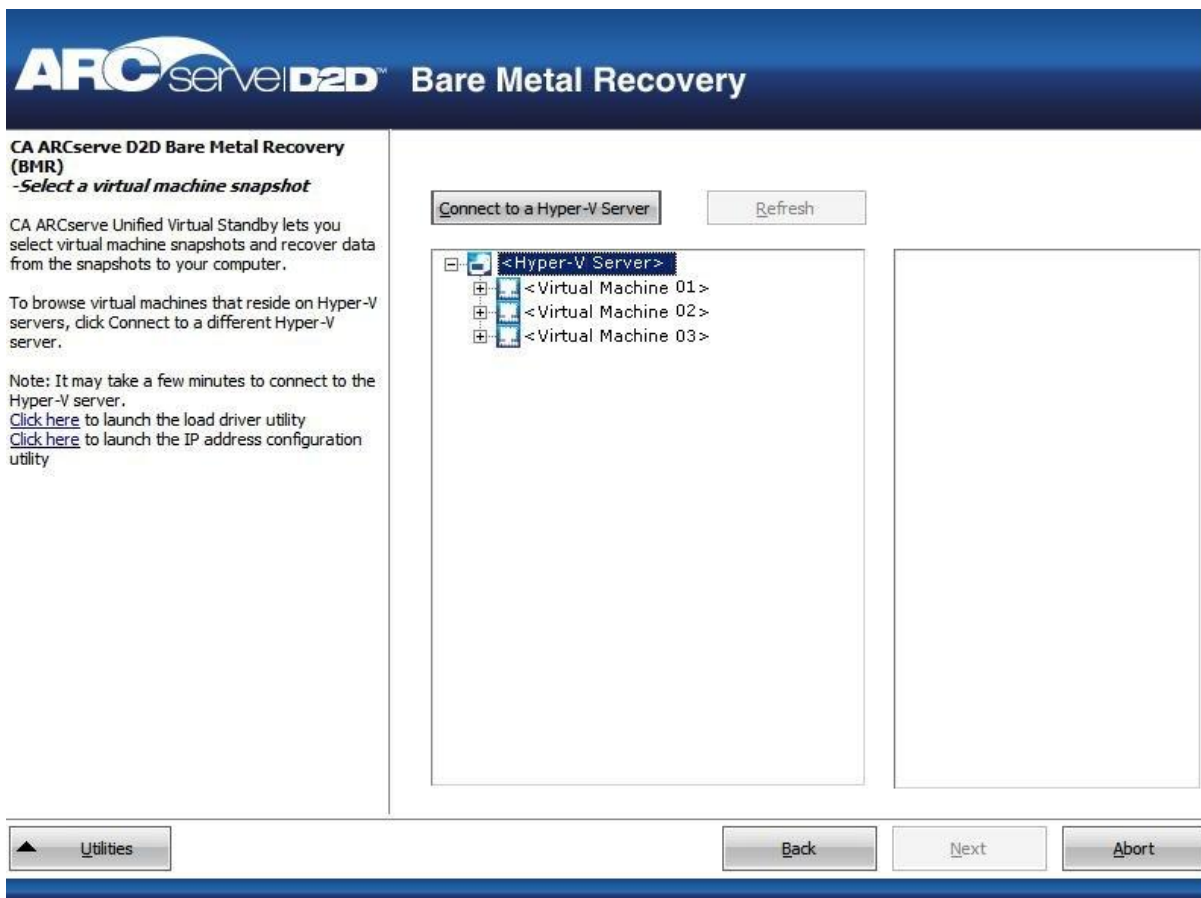
5. Click Next.

The Select a virtual machine snapshot screen is displayed, with the Hyper-V Authentication dialog, prompting you for Hyper-v server details.



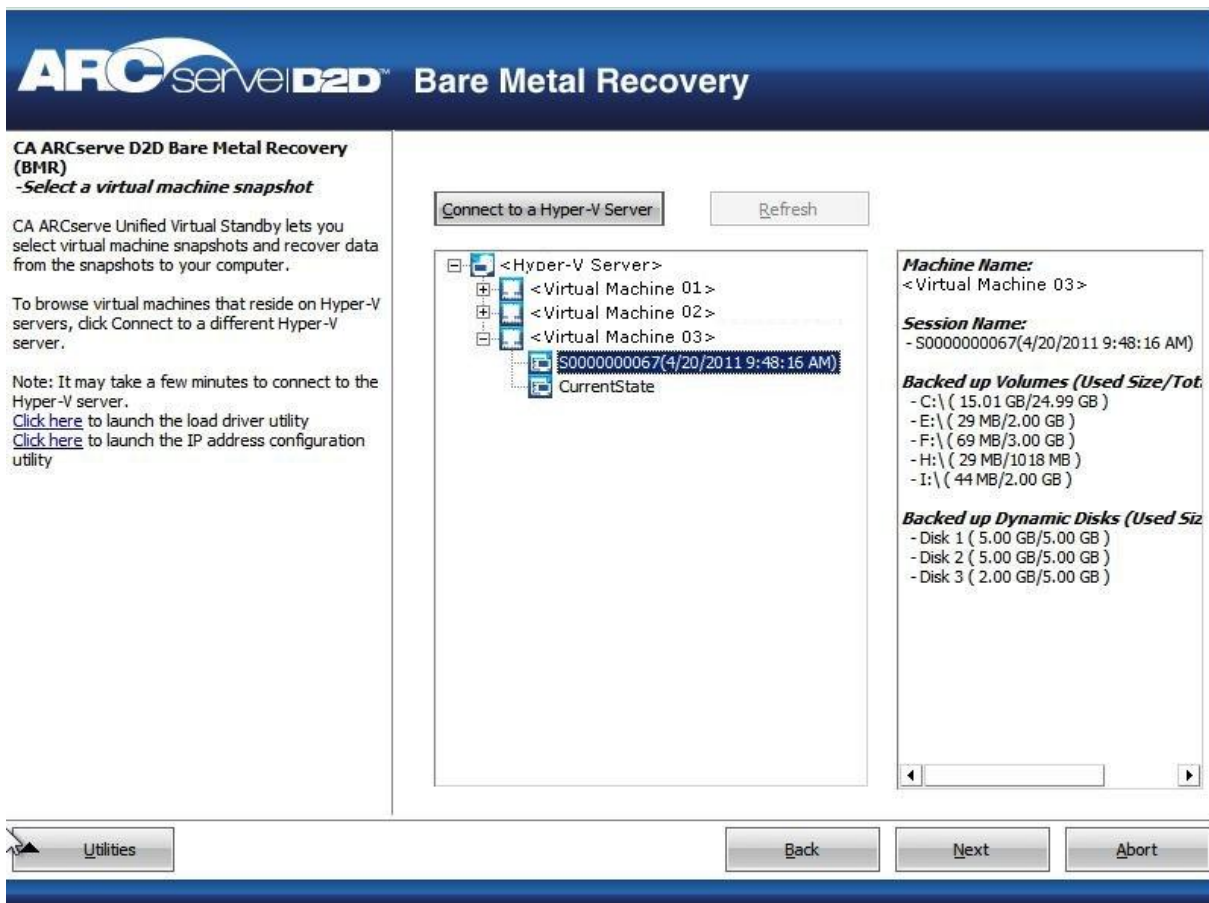
6. Enter the authentication information and click OK.

CA ARCserve D2D detects and displays the Hyper-V Server with a listing of all the virtual machines that are converted to the specified Hyper-V server using CA ARCserve Central Virtual Standby.



7. Select the virtual machine that contains the recovery point snapshots for your backup image.

The backup sessions (recovery point snapshots) for the selected virtual machine are displayed.



8. Select the virtual machine backup session (recovery point snapshot) that you want to recover.

The corresponding details for the selected recovery point snapshot (virtual machine name, backup session name, backed up volumes) are displayed in the right pane.

In addition to selecting one of the listed recovery points, you also have the option to select the "Current State" or the "Latest State" recovery point.

- If the virtual machine that you are recovering from is powered on, the "Current State" recovery point is displayed.
- If the virtual machine that you are recovering from is powered off, the "Latest State" recovery point is displayed.

If you select the "Latest State" recovery point, an error message is displayed to inform you that the recovery point you are recovering from is the Latest (and not the Current) state and requesting that you start the virtual machine before continuing with the recovery process.

9. Verify this is the recovery point that you want to restore and click Next.

A BMR wizard screen is displayed with the available recovery mode options.

10. 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.

11. Click Next.

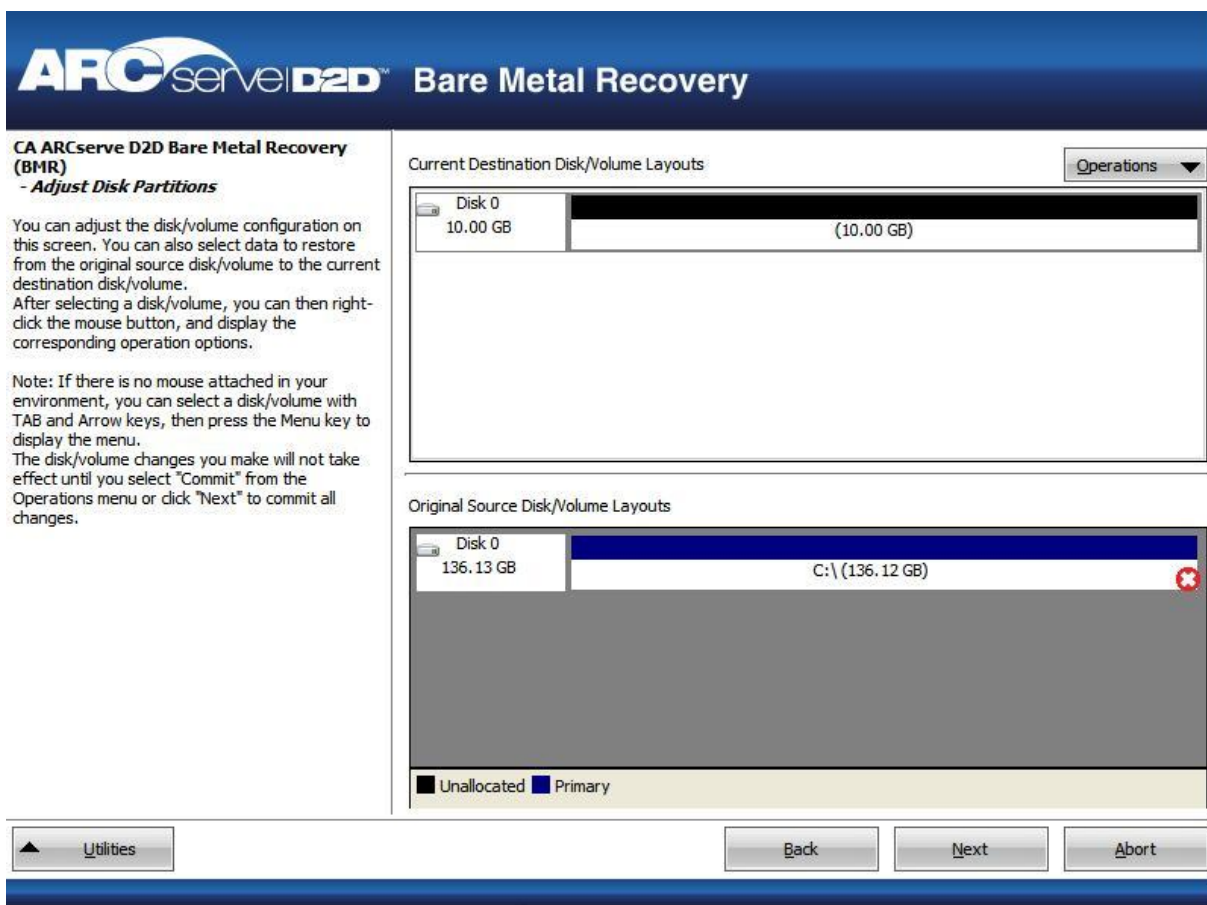
The BMR utility starts locating the machine that is going to be recovered and displays the corresponding disk partition information.

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.

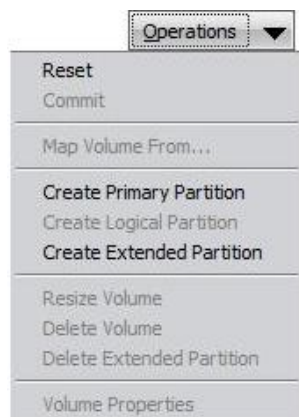


12. If the current disk information you are seeing does not appear correct, you can access the Utilities menu and check for missing drivers.

13. If necessary, on the target volume pane you can click the Operations drop-down menu to display the available options.

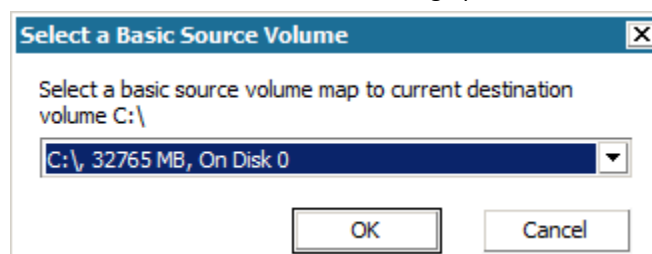
From this menu, you can reset any existing partitions or you can create new partitions to correspond to the disk partitions on the source volume. (Reset means to reload the source and target disk layout information from the configure file and current OS, and discard any user changed disk layout information).

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.



14. 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.

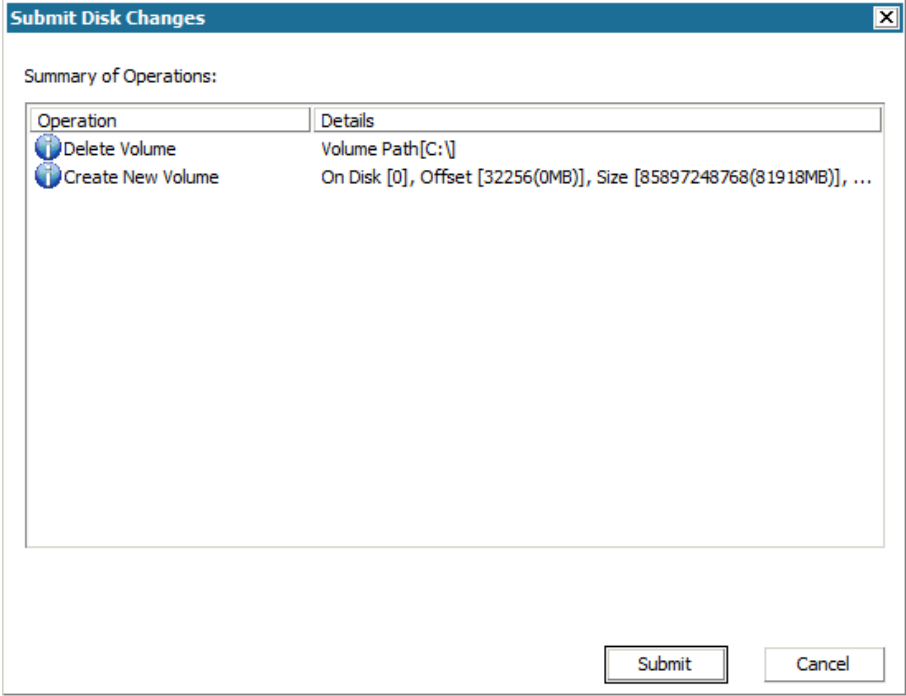
The Select a Basic Source Volume dialog opens.



15. 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.

- 16. 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.



- 17. When you have verified the summary information is correct, click Submit. (If the information is not correct, click Cancel).

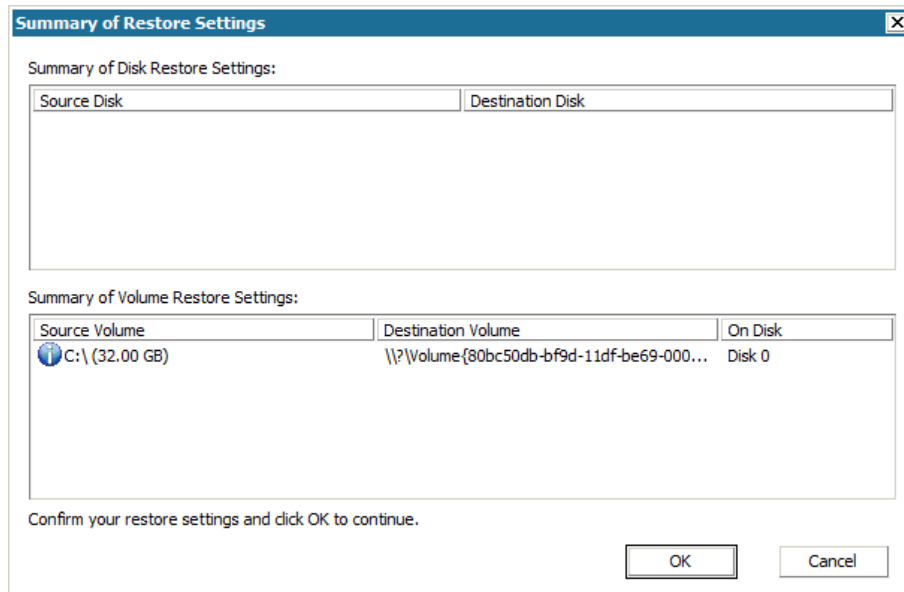
Note: All operations to the hard drive do not take effect until you submit it.

On the target machine, the new volumes are created and mapped to the corresponding source machine.

18. 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.

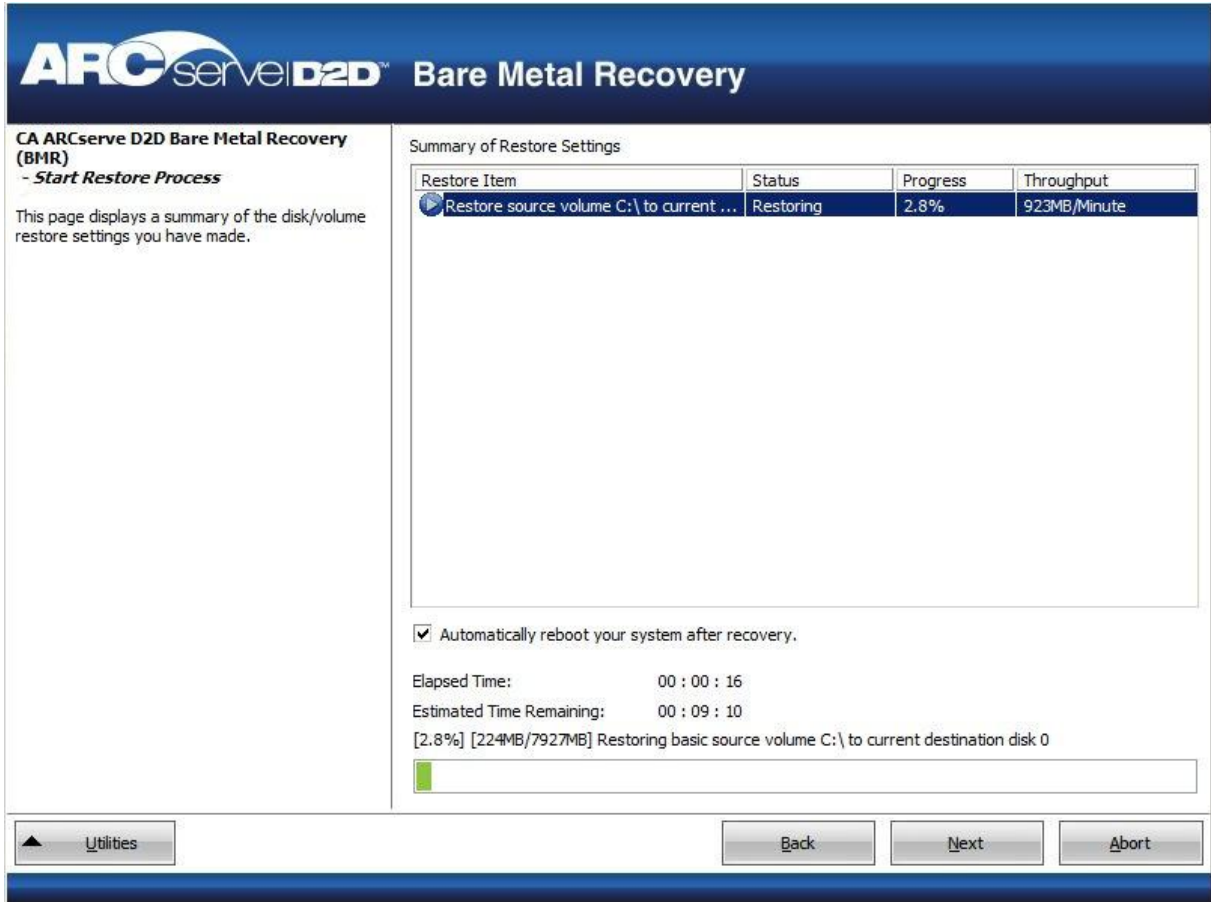
Note: On the bottom of restore summary window, the drive letters listed in "Destination Volume" column are automatically generated from the Windows Preinstallation Environment (WinPE). They can be different from the drive letters listed in "Source Volume" column. However, the data is still restored to proper volume even if drive letters are different.



19. 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.



20. 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.

21. 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.

22. When the BMR process is completed, a confirmation notification is displayed.

Notes: After completion of BMR:

- The first backup that is performed is a Verify Backup.
- Verify that the BIOS is configured to boot from the disk on which the boot volume was restored to.
- When the machine has been rebooted, you may need to configure the network adapters manually if you restored to dissimilar hardware.
- For dynamic disks, if the status of the disk is offline, you can manually change it to online from the disk management UI (accessed by running the Diskmgmt.msc control utility).
- For dynamic disks, if the dynamic volumes are in a failed redundancy status, you can manually resynchronize the volumes from the disk management UI (accessed by running the Diskmgmt.msc control utility).

Recover Source Servers Using Data From VMware Virtual Standby Virtual Machines

The application lets you recover source servers using CA ARCserve D2D data that was converted to VMware Virtual Standby virtual machines.

Note: The application uses the bare metal recovery process to recover source servers from VMware virtual machines. For more information, see [Recovering Source Servers Using Bare Metal Recovery](#) (see page 116).

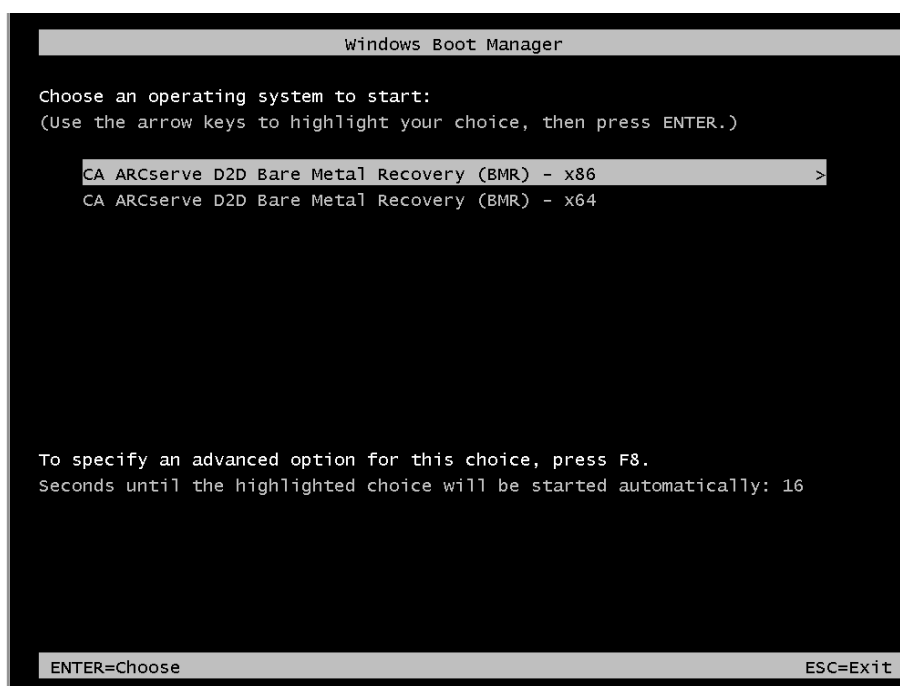
To recover source servers using data from VMware Virtual Standby virtual machines

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.



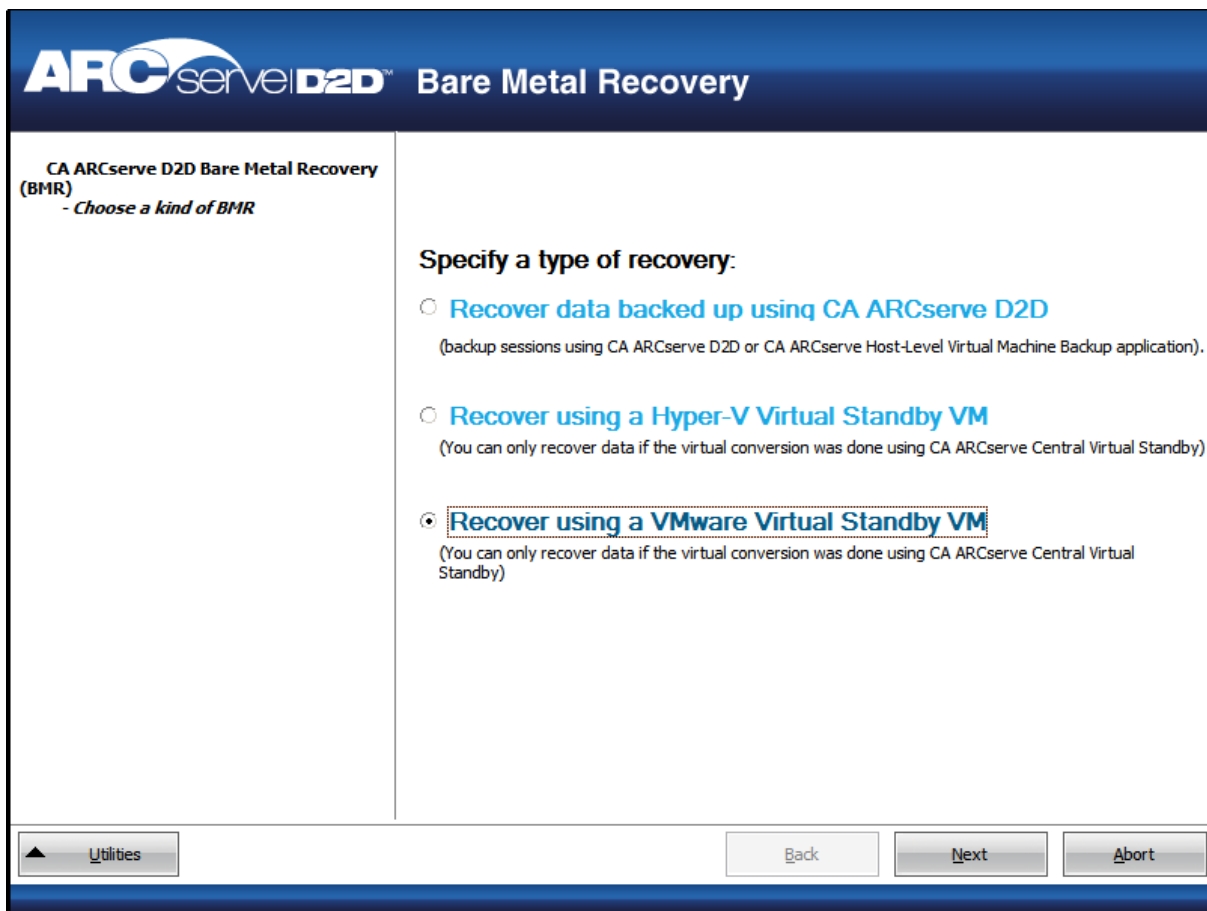
3. The CA ARCserve D2D language select screen is displayed. Select a language and press "Next" to continue.

Note: If you perform BMR with a BMR USB stick and a Windows 7/Windows Vista/Windows 2008/Windows 2008 R2 installation media (CD/DVD) not supported with a Multilingual User Interface (MUI), the language select screen is suppressed.



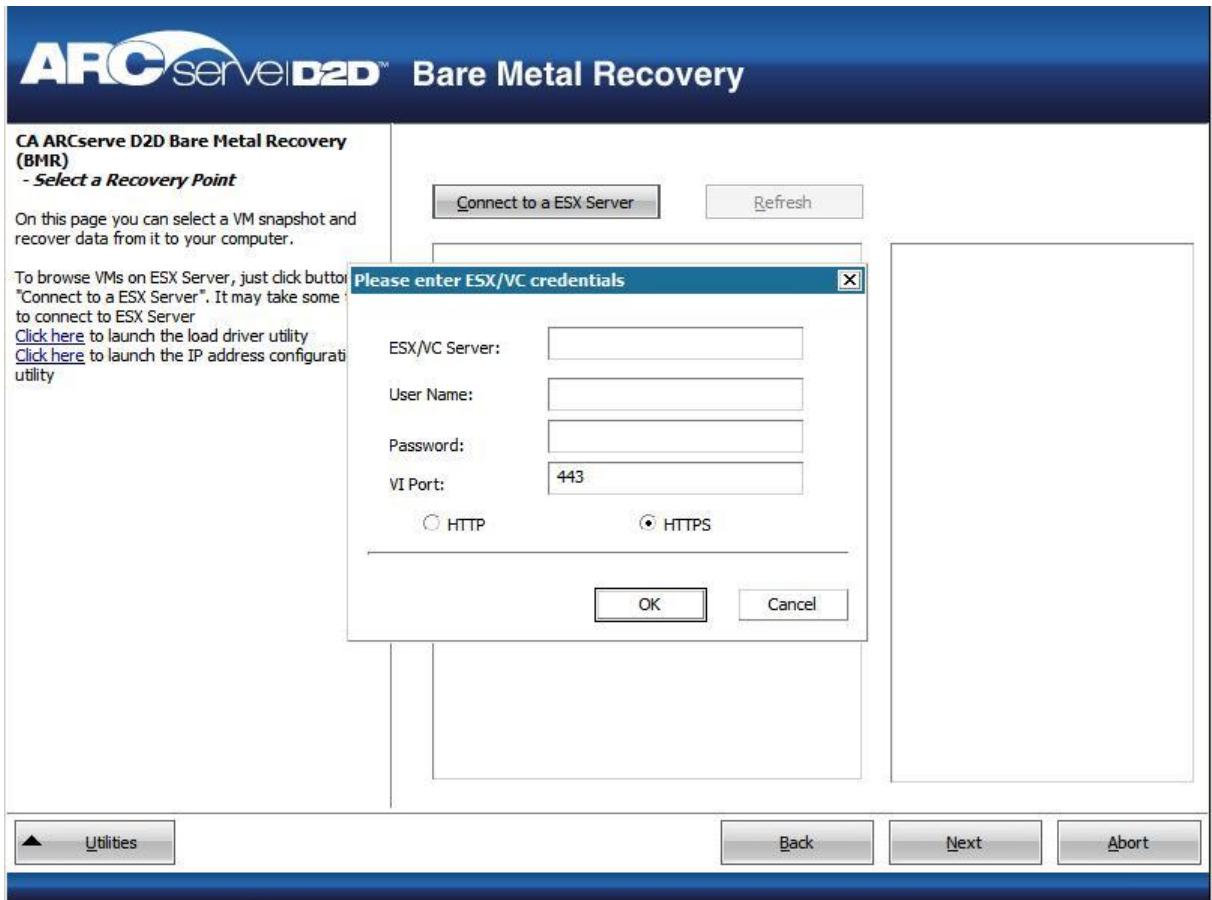
The Bare Metal Recovery process is initiated and the initial BMR wizard screen is displayed.

4. From the select the Type of Bare Metal Recovery (BMR) wizard screen, select the Recover using a VMware Virtual Standby VM option.



5. Click Next.

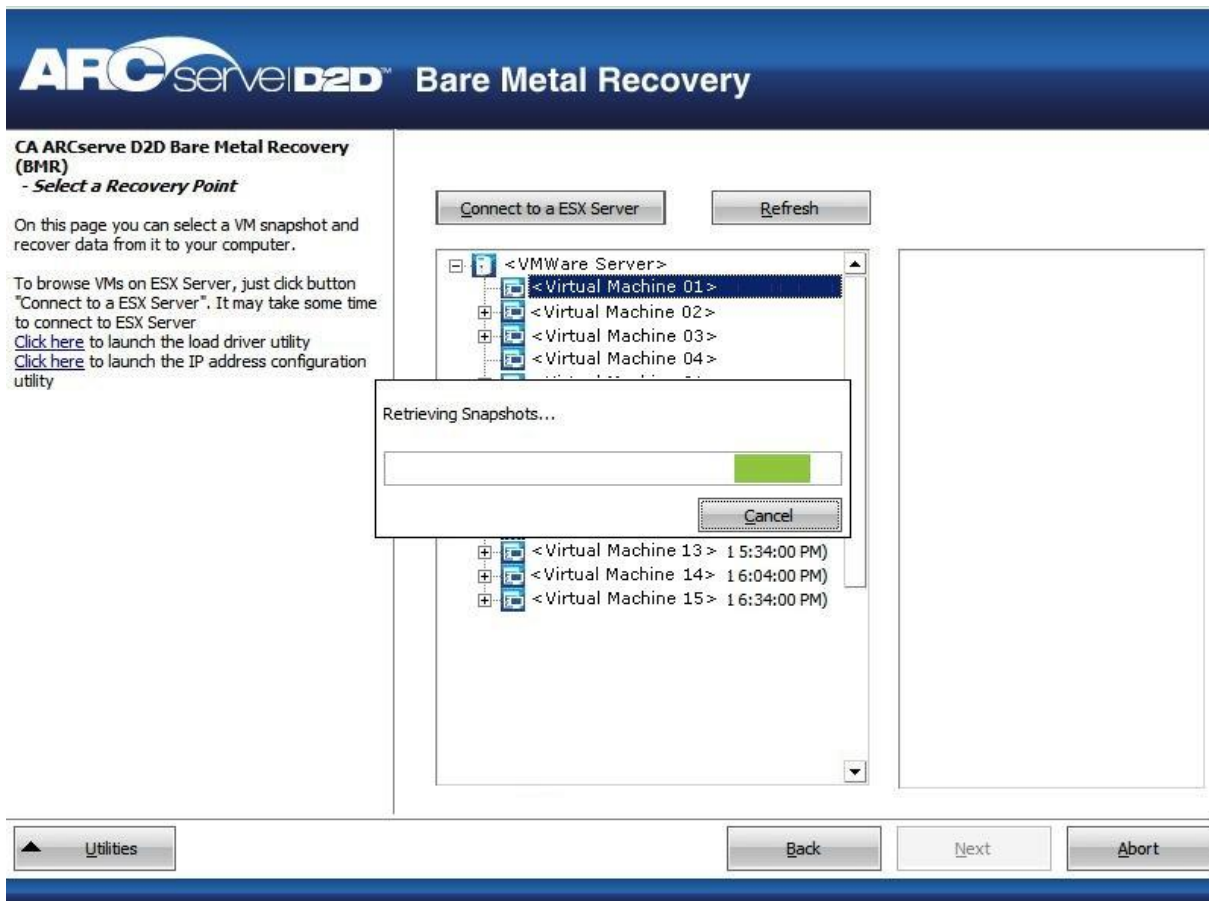
The Select a Recovery Point screen is displayed with the ESX/VC Credentials dialog.



6. Enter the credential information and click OK.

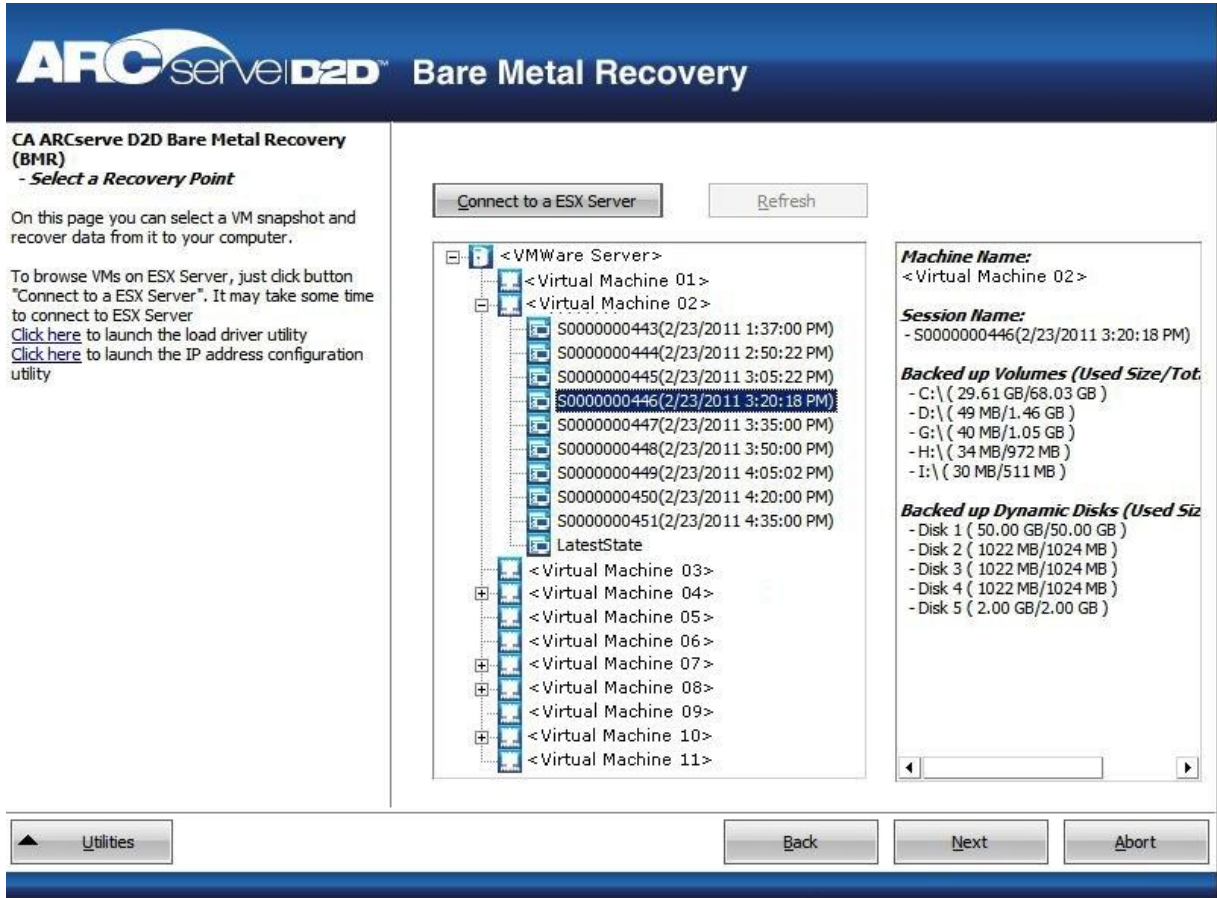
The Select a Recovery Point screen is displayed.

CA ARCserve D2D then retrieves all the recovery point snapshots for the selected VMware server and displays the VMware Server in the left pane, with a listing of all the virtual machines that are hosted on the selected VMware server.



7. Select the virtual machine which contains recovery points for your backup image.

The backup sessions (recovery point snapshots) for the selected virtual machine are displayed.



8. Select the virtual machine backup session (recovery point snapshots) that you want to recover.

The corresponding details for the selected recovery point snapshot (virtual machine name, backup session name, backed up volumes, backed up dynamic disks) are displayed in the right pane.

In addition to selecting one of the listed recovery points, you also have the option to select the "Current State" or the "Latest State" recovery point.

- If the virtual machine that you are recovering from is powered on, the "Current State" recovery point is displayed.
- If the virtual machine that you are recovering from is powered off, the "Latest State" recovery point is displayed.

If you select the "Latest State" recovery point, an error message will be displayed to inform you that the recovery point you are recovering from is the Latest (and not the Current) state and requesting that you start the virtual machine before continuing with the recovery process.

9. Verify this is the recovery point that you want to restore and click Next.

A BMR wizard screen is displayed with the available recovery mode options.



10. 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.

11. Click Next.

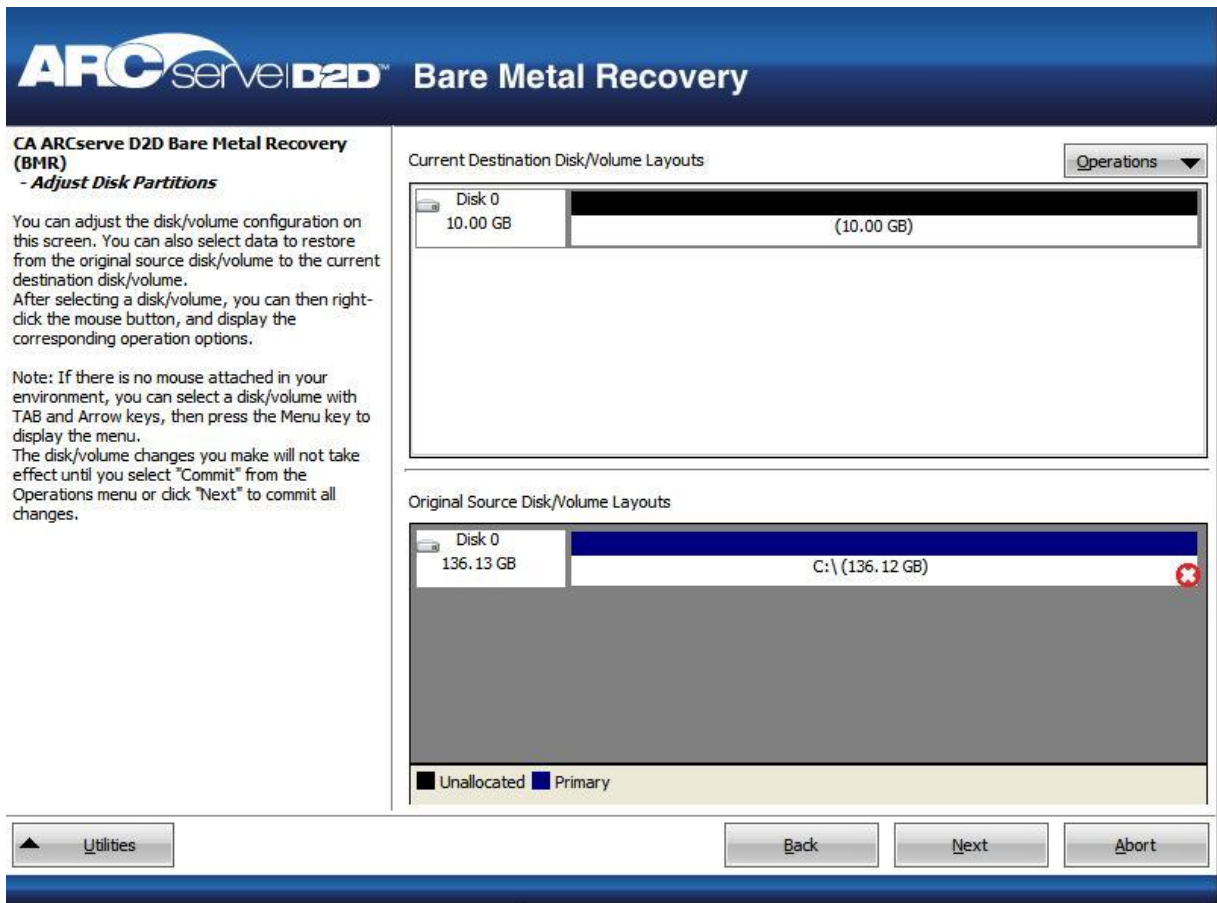
The BMR utility starts locating the machine that is going to be recovered and displays the corresponding disk partition information.

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.

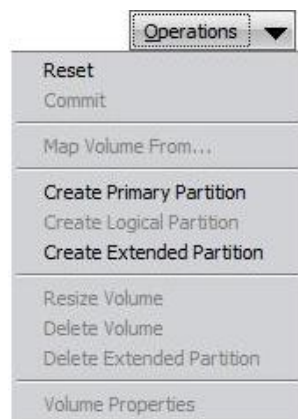
Note: When restoring to another disk/volume, the capacity of new disk/volume must be the same size or larger than original disk/volume. In addition, disk resizing is for basic disks only, and not for dynamic disks.



12. If the current disk information you are seeing does not appear correct, you can access the Utilities menu and check for missing drivers.
13. If necessary, on the target volume pane you can click the Operations drop-down menu to display the available options.

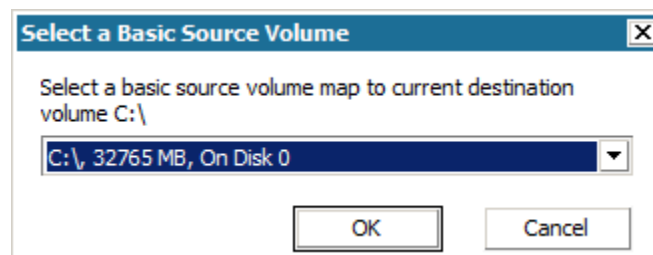
From this menu, you can reset any existing partitions or you can create new partitions to correspond to the disk partitions on the source volume. (Reset means to reload the source and target disk layout information from the configure file and current OS, and discard any user changed disk layout information).

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.



14. 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.

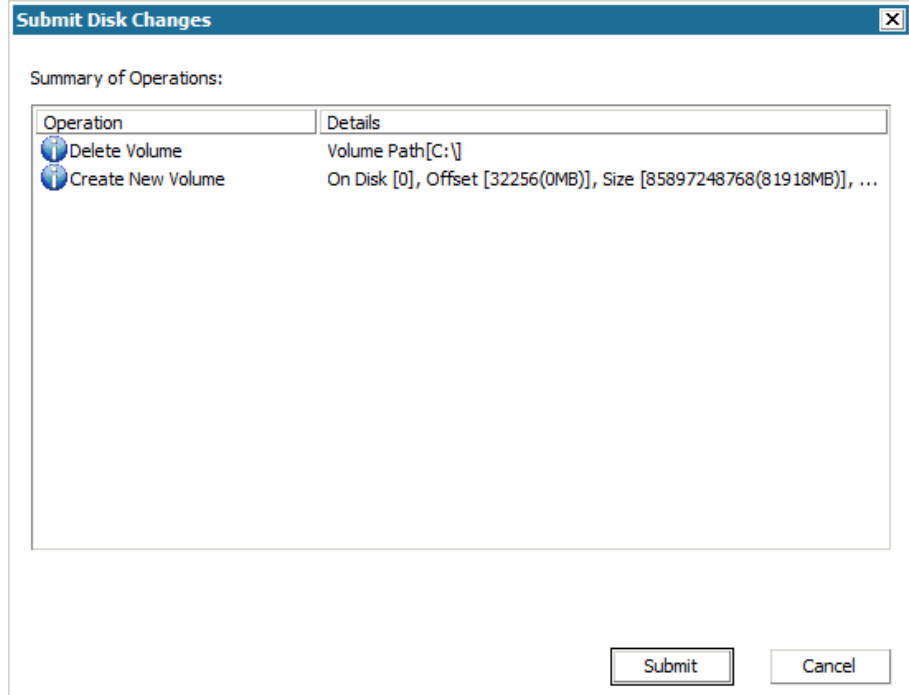
The Select a Basic Source Volume dialog opens.



15. 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.

16. 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.



17. When you have verified the summary information is correct, click Submit. (If the information is not correct, click Cancel).

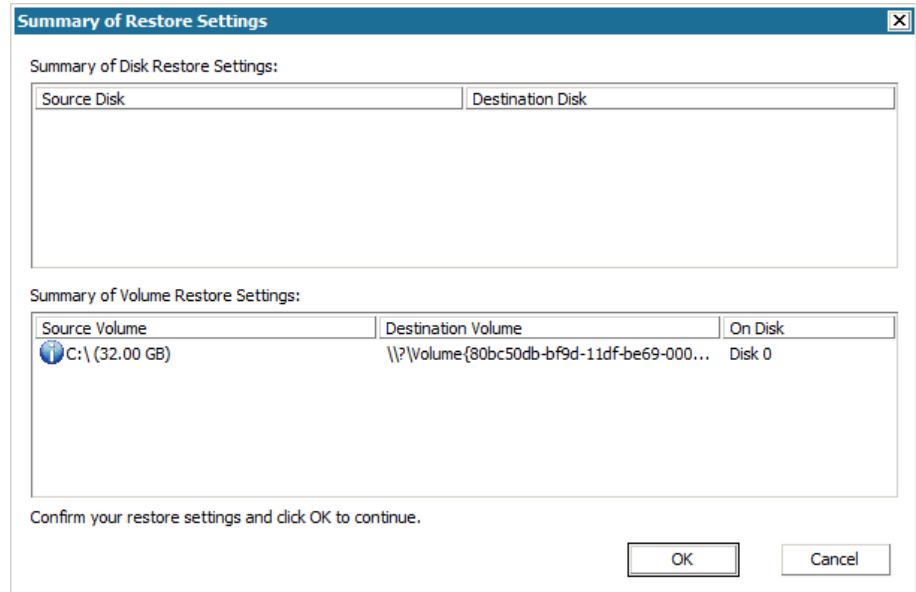
Note: All operations to the hard drive do not take effect until you submit it.

On the target machine, the new volumes are created and mapped to the corresponding source machine.

18. 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.

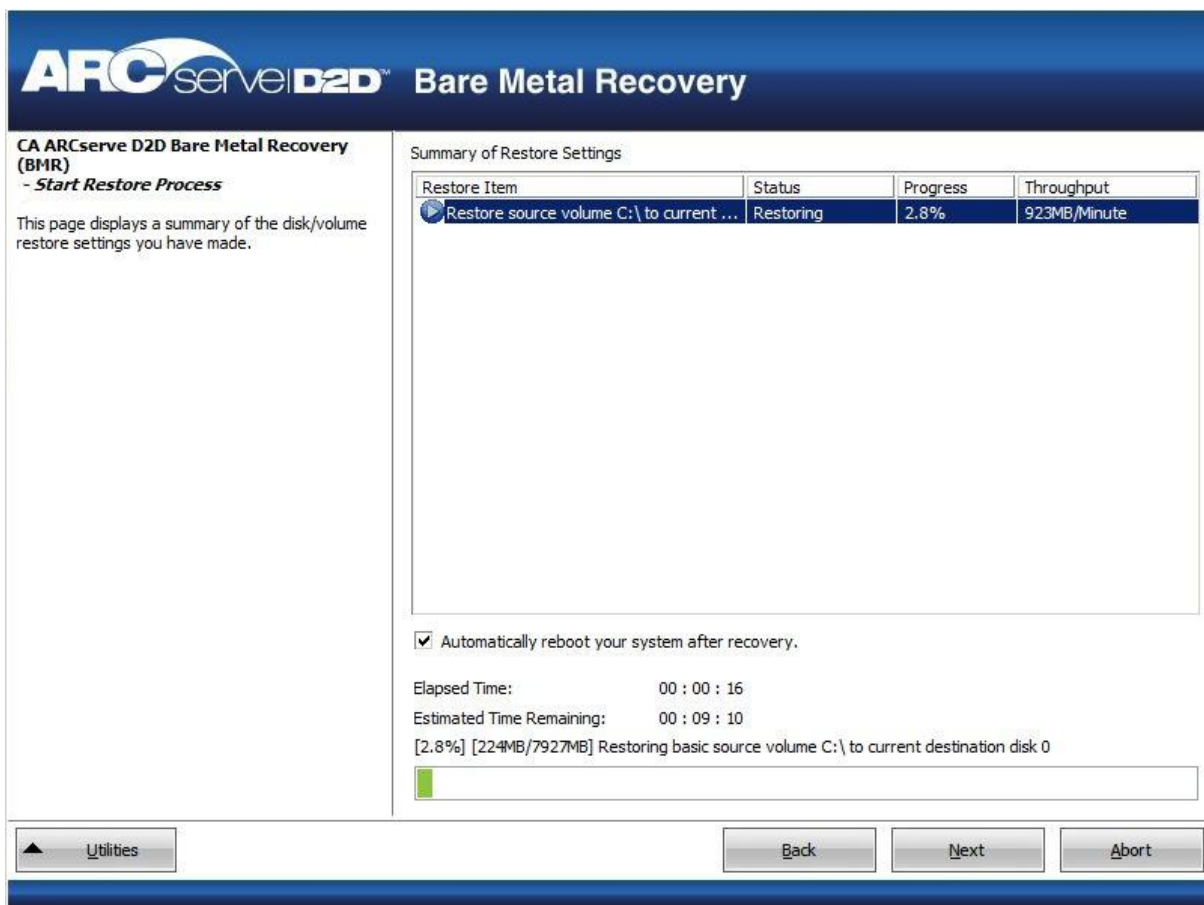
Note: On the bottom of restore summary window, the drive letters listed in "Destination Volume" column are automatically generated from the Windows Preinstallation Environment (WinPE). They can be different from the drive letters listed in "Source Volume" column. However, the data is still restored to proper volume even if drive letters are different.



19. 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.



20. 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.

21. 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.

22. 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).

Restore Microsoft Exchange Email Messages

Virtual Standby lets you restore Microsoft Exchange Data from CA ARCserve D2D recovery points. From the recovery points you can recover or restore mailboxes, mailbox folders, and individual email messages.

Note: To perform granular restores of Exchange server data, your account must have the required access permissions. For more information, see the *CA ARCserve D2D User Guide*.

To restore Microsoft Exchange email messages

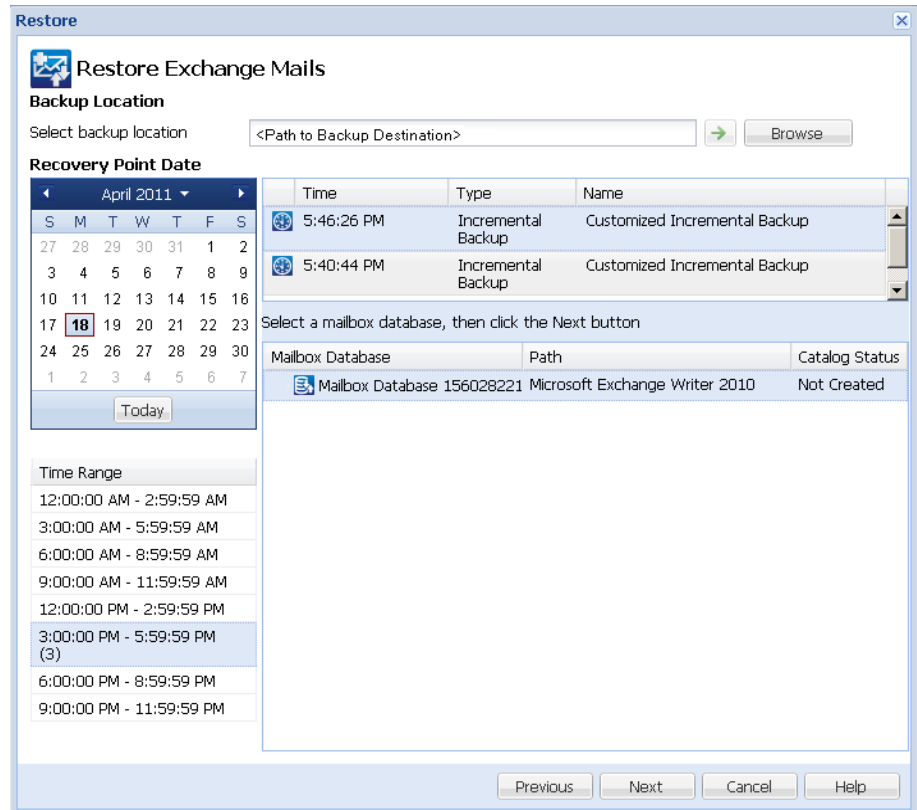
1. Log in to the application and click Node on the Navigation bar.

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 Restore Exchange Mails.

The Restore Exchange Mails dialog opens.



- Specify the backup location. You can either specify a location or browse to the location where your backup images are stored. If necessary, enter the User name and Password credentials to gain access to that location. You can click green arrow validate icon to verify proper access to the source location.

The calendar view will highlight (in green) all dates during the displayed time period that contain recovery points for that backup source.

- Select the calendar date for the backup image you want to restore.

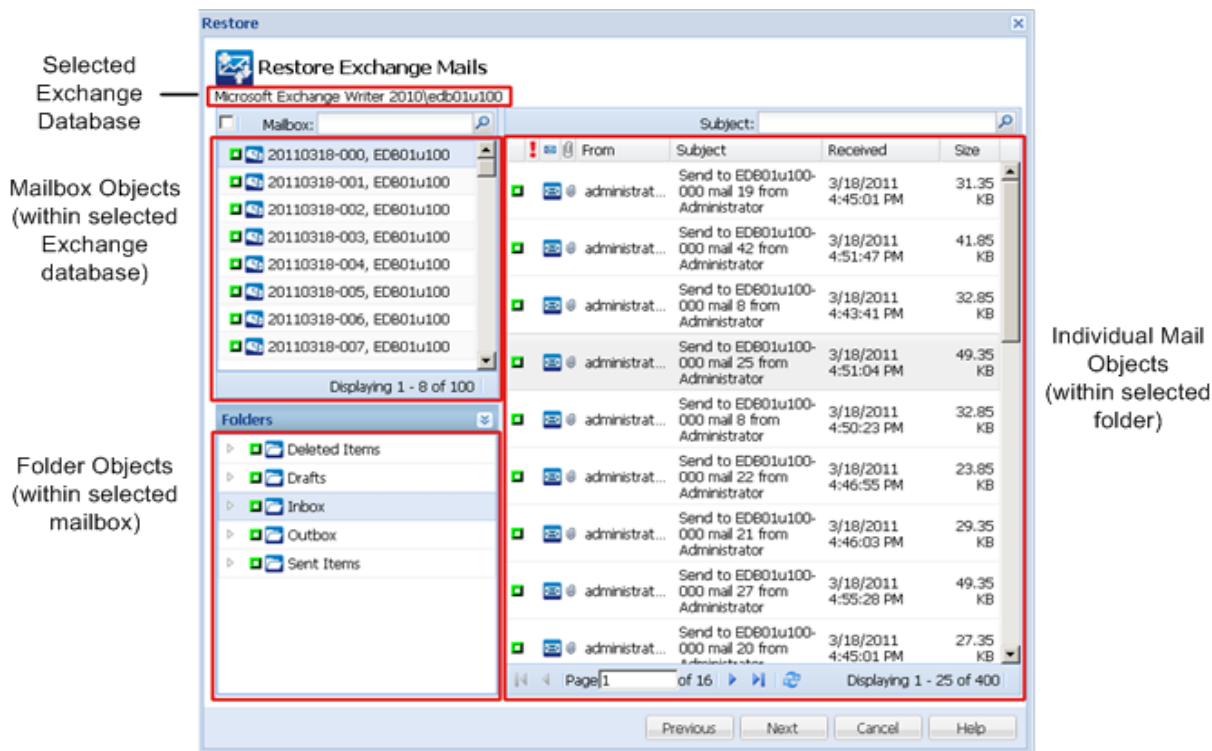
The corresponding Exchange mailbox databases for that date are displayed, along with the time of the backup, the type of backup that was performed, and the name of the backup.

- Select a Exchange mailbox database that you want to restore and click Next.

Note: If you did not enable the Exchange Granular Restore option during backup (no catalog generated), a notification message will be displayed asking you if you want to generate an Exchange Granular Restore catalog at this time. If you select No for generating a catalog now, you will not be able to browse to or select a granular recovery point. As a result you will only be able to perform full database restore from the Browse Recovery Points Restore dialog.

The Restore Exchange Mails dialog is updated to display a listing of the mailbox content for the selected database.

Note: Exchange Granular Restore supports email restores only. Calendar, Contacts, Notes and Tasks restores are not supported.



6. Select the level of Exchange object(s) to be restored (mailbox, folder, or individual mail).

You can select the entire content or partial content of the Exchange object to restore. You can select multiple Exchange objects to restore.

Note: CA ARCserve D2D does not support granular recovery of Exchange public folder objects. You need to use Application Restore to recover the entire public folder database and then extract the specific Exchange object you need.

Note: When using CA ARCserve D2D to restore individual mailbox/mail objects from the Exchange mailbox database, the operating system used for the restore must be same as used when it was backed up (including the same Windows Version number and Service Pack level and also the related version of the visual C++ redistributable package required to support it).

Note: During browse and restore of emails from the CA ARCserve D2D UI, the "From" field property of the message may not display in the UI for mailboxes which have never logged in to the exchange server. However, if this occurs the emails will still be correctly restored.

- a. You can select a mailbox database.

If you select a mailbox database, all of the mailboxes in that database will be restored.

- b. You can select the mailbox (or mailboxes) to be restored.

If you select a mailbox level, all corresponding content (folders and individual mail) within that mailbox will be restored.

- c. You can select a folder(s) within a selected mailbox to be restored.

If you select the mailbox folder level, all corresponding mail content within that folder will be restored.

- d. You can select the individual mail(s) to be restored.

If you select the individual mail level, only the selected mail object(s) will be restored.

Note: For Exchange 2003 only, if the individual mail to be restored was sent using any email client other than Outlook and the mail had some type of flag status marker attached to it when it was backed up, the mail itself will be restored, but the attached marker will not be included with the restored mail.

- When the Exchange objects to be restored are specified, click Next.

Restore

Restore Options

Destination
Select the restore destination

Restore to original location

User Name

Password

Dump email items

How should CA ARCserve D2D resolve duplicate mails

Rename Overwrite

Restore to alternate location

Enter the account, then click the Browse button to choose the destination.

User Name

Password

Destination

Notes:

For Exchange Server 2010 systems, the user name must be a domain account with Exchange Organization management role.

- Select the destination for the restore.

The available options are to restore to the original location of the backup or restore to a different location.

Note: For Exchange 2010, archived mailbox items cannot be restored to the original location. Archived mailbox items can only be restored to an alternate location or to a local disk. In addition, regular mailbox items cannot be restored to archive mailboxes.

Restore to Original Location

Restores the mails to the original location from where the backup image was captured. Mails will retain the same hierarchy and be restored to its original mailbox and original folder.

- If current machine is not the active Exchange server, CA ARCserve D2D will detect the location of the active server and then restore the mails to that active server.
- If mailbox has been moved to another Exchange server, but still in the same organization, CA ARCserve D2D will detect the new Exchange server where the original mailbox resides, and then restore to that new server.
- If the display name of the mailbox was changed, any attempt to restore the mailbox (from an earlier backup session) to its original location will fail because CA ARCserve D2D will not be able to find the changed name. To solve this problem, you can specify to restore this mailbox to an alternate location.

Note: When restoring a mailbox or mail to the original location, make sure the destination mailbox is available, or else the restore will fail. CA ARCserve D2D only validates the destination when the restore job is submitted.

Dump File Only

Restores the mails to a disk. This disk location can be local or a remote machine. The restored mails will maintain the same hierarchy as they had in the corresponding Exchange Mailbox. The file name will become the subject of mail.

Note: If the mail subject, folder name, or mailbox name includes any of the following characters, the character will be replaced by hyphen (-) in file name: \ / : * ? " < > |

For this option, you also need to specify what you want CA ARCserve D2D to do to resolve a conflict situation. In Exchange, you can have multiple mail objects with the same name under the same folder. However in a File System, two files with the same name cannot co-exist under the same folder.

There are two options to resolve this conflict situation:

- **Rename** - If on the disk, there is a file with the same name as the mail subject, CA ARCserve D2D will still name the mail subject, but will append a number at the end of the mail subject.
- **Overwrite** - If on the disk, there is a file with the same name as the mail subject, CA ARCserve D2D will overwrite that file.

Note: When you select individual mail objects to restore to the disk (dump), by default the format of the restored mail object will be an Outlook Message (.MSG) file and not a Personal Storage Table (.PST) file.

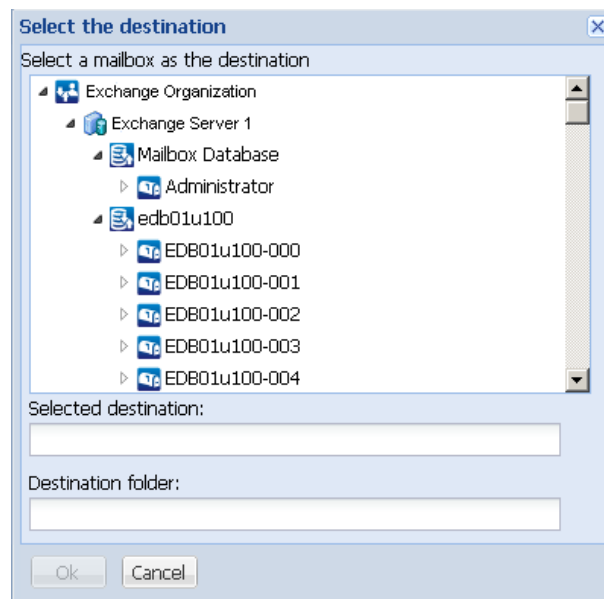
Restore to Alternate Location:

Restores the mails to a specified location or lets you browse to the location where your backup images will be restored. The destination must be a mailbox in the same Exchange organization, and a new folder name is required. (If you are attempting to restore mails to an alternate location, the destination cannot be a public folder).

Note: When restoring mail to an alternate location, if the specified destination folder already exists, the restore will continue. However, if the specified folder does not exist, then CA ARCserve D2D will create the folder first and then continue the restore.

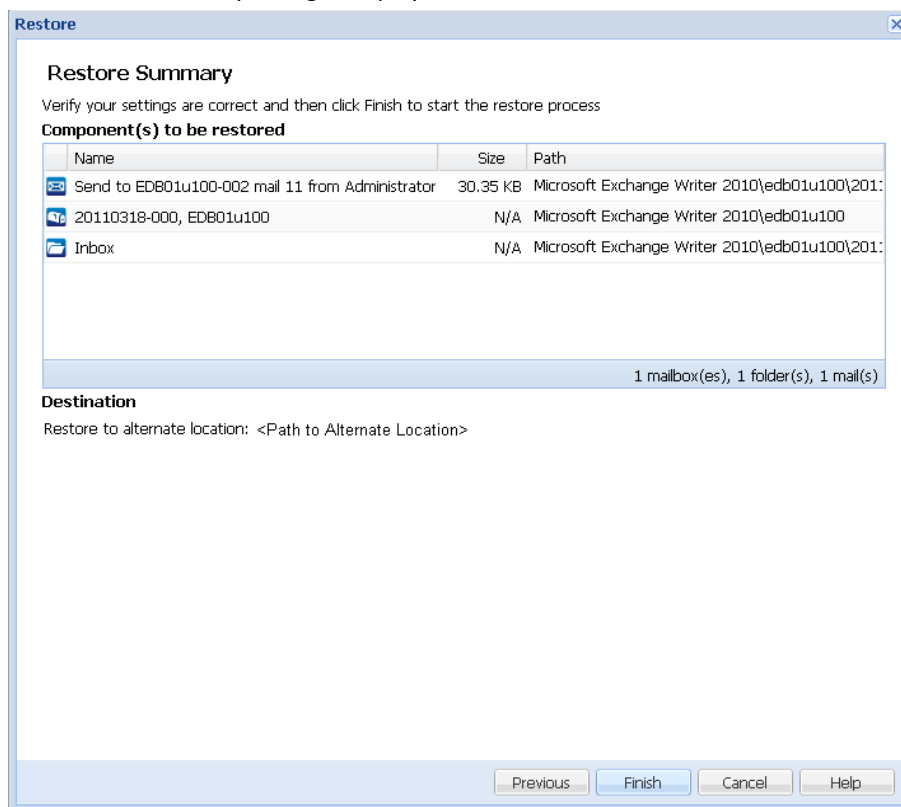
After inputting the User Name and Password, you can click the Browse button to navigate through a list of all Exchange Servers, Storage Groups, Exchange Databases, and Mailboxes in the current organization.

Select any mailbox as the destination.



9. When the restore options are selected, click Next.

The Restore Summary dialog is displayed.



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.

Note: When the Catalog and Restore Job for Exchange Granular Restore is in progress, the backup session will be in a mounted state. Do not perform any operation (format, change drive letter, delete partition, etc.) on this mounted volume.

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.

Chapter 5: Troubleshooting CA ARCserve Central Virtual Standby

This section provides troubleshooting information to help you identify and resolve problems that you can encounter when using CA ARCserve Central Virtual Standby.

This section contains the following topics:

[Cannot Connect to Specified Server Messages Appear When Attempting to Add Nodes](#) (see page 170)

[Blank Webpages Appear or Javascript Errors Occur](#) (see page 172)

[How to Troubleshoot Page Loading Problems](#) (see page 174)

[Web Pages Do Not Load Properly When Logging in to CA ARCserve D2D Nodes and Monitoring Servers](#) (see page 175)

[Garbage Characters Appear in Browser Windows When Accessing CA ARCserve Central Applications](#) (see page 176)

[CA ARCserve D2D Web Service Fails on CA ARCserve D2D Nodes](#) (see page 177)

[The CA ARCserve D2D Web Service Runs Slowly](#) (see page 180)

[CA ARCserve Central Virtual Standby Cannot Communicate with the CA ARCserve D2D Web Service on Remote Nodes](#) (see page 182)

[Certificate Error Appears When You Log In to the Application](#) (see page 183)

[Invalid Credentials Message Appears When Adding Nodes](#) (see page 184)

[Invalid Credentials Messages on Windows XP](#) (see page 185)

[Access Denied Errors Occur when Adding a Node by IP/Name](#) (see page 185)

[Nodes Do Not Appear on the Node Screen After Changing the Name of the Node](#) (see page 187)

[Operating System Not Found Errors Occur](#) (see page 187)

[Virtual Standby Jobs to Hyper-V Systems Fail](#) (see page 188)

[Virtual Standby Jobs Fail Due to Internal Errors](#) (see page 188)

[Virtual Standby Jobs Fail Using the hotadd Transport Mode](#) (see page 191)

[Virtual Standby Jobs End with No Sessions Warning Messages](#) (see page 192)

[Backup and Recovery Jobs Do Not Use the SAN Transport Mode](#) (see page 193)

[Backup and Recovery Jobs Using the hotadd Transport Mode Cannot Mount Disks](#) (see page 194)

[Troubleshooting Error Numbers](#) (see page 195)

[Add New Tab Link Not Launching Properly for Internet Explorer 8, 9, and Chrome](#) (see page 195)

[Add New Tab Link, RSS Feeds, and Social Networking Feedback Not Launching Properly on Internet Explorer 8 and 9](#) (see page 197)

[Cannot Specify an Asterisk or Underscore as a Wildcard in Filter Fields Using Japanese Keyboards](#) (see page 198)

[Virtual Machines Do Not Power On Automatically](#) (see page 198)

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

Valid on Windows platforms.

Symptom:

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

Cannot connect to specified server.

Solution:

If the preceding 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 Virtual Standby 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 Virtual Standby 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 Virtual Standby 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 Virtual Standby server and the source virtual machine (node).

1. Log in to the CA ARCserve Central Virtual Standby 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 Virtual Standby 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.

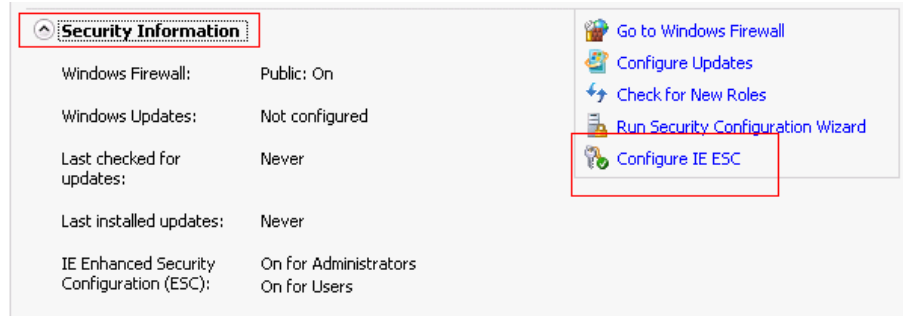
Solution:

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:



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.

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.

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

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 and Monitoring Servers 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.

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.

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.

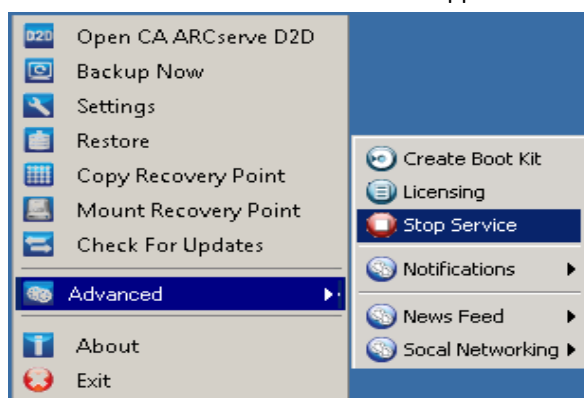
Solution:

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.

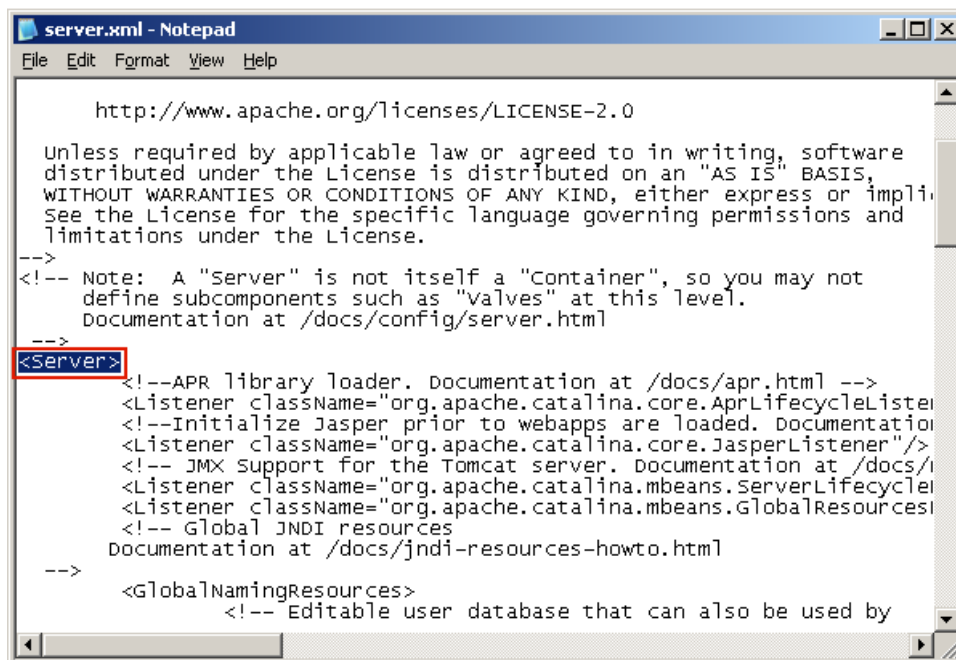


2. Access the Tomcat server.xml file to edit/configure the behavior of Tomcat.

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.



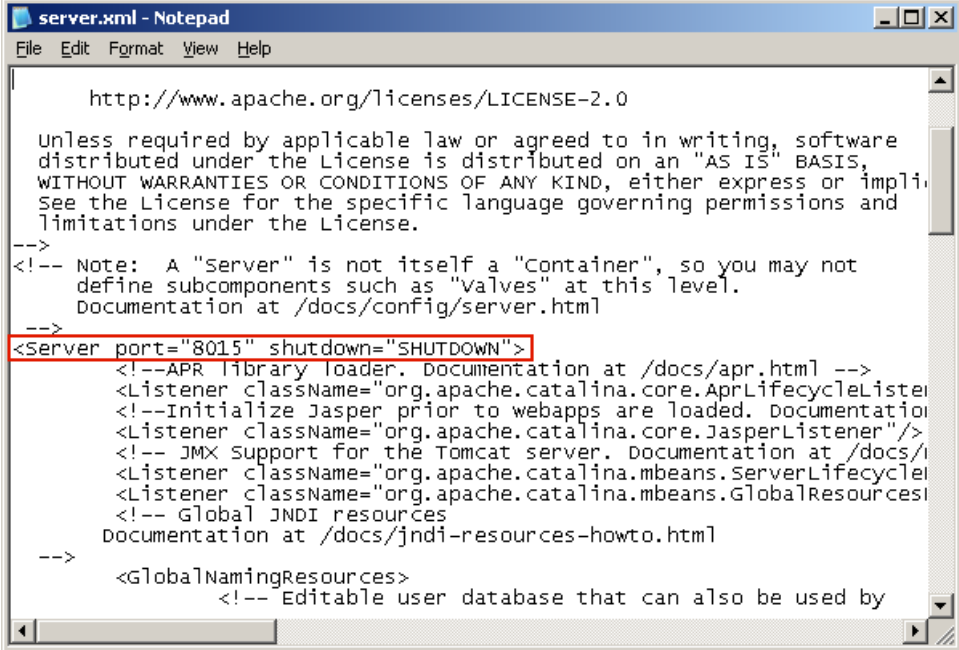
4. Edit the <Server> tag as follows:

From:

```
<Server>
```

To:

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



```
server.xml - Notepad
File Edit Format View Help

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.AprLifecycleLister
  <!--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.GlobalResource
  <!-- 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.

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-stderr*.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.

CA ARCserve Central Virtual Standby Cannot Communicate with the CA ARCserve D2D Web Service on Remote Nodes

Valid on Windows operating systems.

Symptom:

CA ARCserve Central Virtual Standby cannot communicate with the CA ARCserve D2D web service on remote nodes.

Solution:

The following table describes reasons why CA ARCserve Central Virtual Standby 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.

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

Invalid Credentials Message Appears When Adding Nodes

Valid on Widows platforms.

Symptom:

The following message appears when you try to add nodes to the Nodes screen:

Invalid credentials.

Solution:

This problem occurs under the following scenarios:

- The credentials specified on the Add Nodes dialog are incorrect.
- The time on the node is not the same as the time on the application server.

To correct this problem, do the following:

1. Log in to the application server and then log in to the application.
2. From the home page, select Node on the Navigation bar.

The Node screen displays.

3. From the Node toolbar, click Add, and then click Add Node by IP/Name on the pop-up menu.

The Add Node by IP/Name dialog opens.

4. Complete the following fields on the Add Node by IP/Name dialog:
 - **IP/Node Name**--Lets you specify the IP address or the name of the node.
 - **Description**--Lets you specify a description for the node.
 - **User Name**--Lets you specify the user name that is required to log in to the node.
 - **Password**--Lets you specify the password that is required to log in to the node.

Click Validate.

5. If the message Invalid credentials appears, do the following:
 - a. Verify that you specified the correct credentials on the Add Nodes dialog and then click Validate.
 - b. If the message Invalid credentials appears, verify that the operating system time on the application server is the same as the operating system time on the node.

Note: The operating system times can reside in different time zones. However, the operating system times cannot be different dates. Specifically, verify that the operating system date on the node is no more than one calendar day plus or minus the operating system date on the application server.

Invalid Credentials Messages on Windows XP

Valid on computers running Windows XP operating systems.

Symptom:

When you add Windows XP-based nodes from the Node screen, the following message appears:

Invalid user credentials.

Solution:

Under various conditions, CA ARCserve Central Virtual Standby cannot add Windows XP-based nodes that have the Windows, Use simple file sharing, Folder Option specified. To correct this problem, do the following:

1. Log in to the Windows XP node and open Windows Explorer.
2. From the Tools menu, click Folder Options.
The Folder Options dialog opens.
3. Click View and scroll to Use simple file sharing (Recommended).
4. Clear the checkmark next to Use simple file sharing (Recommended) and click OK.
Simple file sharing is disabled.
5. Log in to the CA ARCserve Central Virtual Standby server and then add the node.

Access Denied Errors Occur when Adding a Node by IP/Name

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:

When you add nodes from the Add node by IP/Name dialog using a new Windows user account that is a member of the administrators group, the following message displays:

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 add 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 node 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 your 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 monitor server and the CA ARCserve D2D node or the backup proxy system:
 - 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 Virtual Standby 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.

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 Virtual Standby retains the name of the node as it was added from the node screen. When you rename the node, Virtual Standby 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 52) that was renamed.
3. [Add the node](#) (see page 27) using its new name.

Operating System Not Found Errors Occur

Valid on Windows platforms.

Symptom:

The following message appears when the power on Virtual Standby virtual machine operation fails:

Operating System Not Found.

Solution:

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, update the BIOS on the recovered virtual machine to match that of the source.

Note: Use (0:1) to represent the first IDE disk.

Virtual Standby Jobs to Hyper-V Systems Fail

Valid on Windows operating systems.

Symptom:

Virtual Standby jobs fail to Hyper-V systems. The following message appears in the Activity Log:

Virtual Standby job failed to get the Hyper-V VM.

Solution:

Virtual Standby jobs fail under the following conditions:

- The Virtual Standby web service is unable to retrieve information about the virtual machine from the Hyper-V system. Communication problems between the CA ARCserve Central Virtual Standby server and the Hyper-V system occur when the required Hyper-V services are not running on the Hyper-V system.

Solution: Verify that all of the required Hyper-V services are running on the Hyper-V system.

- The Hyper-V system does not contain a sufficient amount of free disk space that is required to create the Virtual Standby virtual machine or to create a snapshot of the Virtual Standby virtual machine.

Solution: Consider reconfiguring the Hyper-V system to allow more free disk space in the system volume.

Note: If you discover other possible causes, contact CA Support.

Virtual Standby Jobs Fail Due to Internal Errors

Valid on Windows operating systems.

Symptom 1:

Virtual standby jobs fail. One of the following messages appears in the Activity Log:

Failed to convert virtual disk
An internal error occurred, contact technical support

In addition, VDDK reports the following error message:

Unknown Error.

Solution 1:

To correct this problem, consider the following solutions:

- Conversion operations can fail when there is not enough free disk space on the data store that is specified in the Virtual Standby policy. VDDK returns the message because the VDDK API (currently) does not support the capability to detect the amount of free disk space on the data store. To correct this problem, free the amount of disk space on the original data store that is required to complete the operation and then resubmit the job.
- Network disturbance and high network traffic can cause the conversion operations to fail. To correct this problem, verify that source node and the ESX Server system or the vCenter Server system can communicate with each other through the network, and 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.

This problem is the result of a VMware VDDK 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
- ESXi 5: Limited by a transfer buffer for all NFC connections and enforced by the host; the sum of all NFC connection buffers to an ESXi host cannot exceed 32MB. 52 connections through vCenter Server which includes the per-host limit.

Note: 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.

- 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 then resubmit the job.

Symptom 2:

Virtual standby jobs fail. One of the following messages appears in the Activity Log:

Failed to convert virtual disk
An internal error occurred, contact technical support

In addition, VDDK reports the following error message:

Open vmdk failed with error File not found.

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.

Symptom 3:

Virtual standby jobs fail. One of the following messages appears in the Activity Log:

Failed to convert virtual disk
An internal error occurred, contact technical support

In addition, VDDK reports the following error message:

Open vmdk failed or "The server refused connection" error message

Solution 3:

This problem is the result of a VMware VDDK 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

Note: 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.

Virtual Standby Jobs Fail Using the hotadd Transport Mode

Valid on Windows platforms.

Symptom:

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

An unknown error has occurred. Contact technical support.

In addition, VDDK reports the following error message:

Unknown Error.

Solution:

Recovery operations fail using the hotadd transport mode when the disk settings are not configured properly.

To configure the disk, do the following:

1. Log in to the backup proxy system using an account with administrative privileges.

Open Windows Command Line.

2. From the command line, type the following command

```
diskpart
```

Press Enter.

Type SAN and then press Enter.

The current SAN policy displays.

3. Type the following command:

```
SAN POLICY = OnlineAll
```

Press Enter.

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

4. 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

5. 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, do the following:

1. Log in to the backup proxy system using an account with administrative privileges.
Open Windows Control Panel and double-click Administrative Tools.
The Administrative Tools window opens.
2. From the Favorites list, double-click Computer Management.
The Computer Management opens.
3. Expand Storage and click Disk Management.
The disks display.
4. Right-click the disk that you want to mount and click Online.
The disk is mounted and you can resubmit the job.

Virtual Standby Jobs End with No Sessions Warning Messages

Valid on Windows platforms.

Symptom:

The Virtual Standby jobs end and one of the following messages appear in the Activity Log:

Virtual Standby job ends with no session(s).

Virtual Standby was unable to detect backup sessions on the CA ARCserve D2D server to create recovery point snapshots. There may be no backup sessions on the CA ARCserve D2D server that can be converted.

Solution:

You will encounter problems of this type under the following conditions:

- You used CA ARCserve Central Protection Manager to apply the CA ARCserve D2D backup policy to the node and one of the following.
 - The CA ARCserve D2D backup source settings were changed from the Select individual volumes to back up option to the Back up the entire machine option, and a full backup was not submitted or did not complete using the updated backup settings after Virtual Standby policy was deployed to the node.

Solution: Submit a full backup of the CA ARCserve D2D node.

- The CA ARCserve D2D backup source settings were changed from the Back up the entire machine option to the Select individual volumes to back up option after the Virtual Standby policy was deployed to the node.

Solution: Change the CA ARCserve D2D backup source settings from the Select individual volumes to back up option to the Back up the entire machine option, and then submit a full backup of the CA ARCserve D2D node.

Backup and Recovery Jobs Do Not Use the SAN Transport Mode

Valid on Windows platforms.

Symptom:

Backup and recovery jobs do not use the [SAN transport mode](#) (see page 208). The jobs revert to the [NBD transport mode](#) (see page 207) or the [NBDSSL transport mode](#) (see page 207). The Transport Mode field on the Backup Status Monitor dialog displays the mode that is used.

Solution:

The symptoms described above can occur when the SAN LUN is not properly configured on the backup proxy system. However, if Windows Disk Management detects the SAN LUN and the problem persists, the disk could be off line or the read attribute for the disk is not correct. To prevent this behavior from occurring, reconfigure the disk.

To configure the disk, do the following:

1. Log in to the source node or the Monitor server 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.

Backup and Recovery Jobs 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 source node or the monitor server. In addition, the following message appears in the Activity Log:

```
Failed to open VMDK file %1!s!. Please refer to debug log AFBackend.Log for more detail. Contact technical support.
```

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 from the proxy system, if disks were attached during the conversion job.
4. Resubmit the job.

Troubleshooting Error Numbers

The following table describes error numbers that display as pop-up messages when adding or updating nodes using CA ARCserve Central Virtual Standby.

Error Number	Description	Possible Solution
12884901933	Cannot connect to the CA ARCserve D2D service on *** and error number is 12884901933. Verify that all entries for the node is correct and the CA ARCserve D2D service is running.	Verify the following: <ul style="list-style-type: none"> ■ The CA ARCserve D2D service is running on the node. ■ The host name, IP address, and communication protocol specified for the node is correct. ■ The CA ARCserve D2D web service on the node is running, and not blocked because the DNS cannot resolve the IP address for the node. ■ The CA ARCserve D2D web service on the node is running, and the Windows firewall, or any other firewall, is not blocking communication. ■ The network cable that is connected to the node is functioning properly. ■ The user that is logged in to the node obtained the permissions that are required to communicate using a wireless network.

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

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.

Virtual Machines Do Not Power On Automatically

Valid on Windows.

Symptom:

Virtual machines do not power on automatically. The value of the Recovery, Stand-in setting is defined as Automatically start the Virtual Machine.

Solution:

This is expected behavior. The application cannot automatically power on virtual machines that were added from CA ARCserve Central Host-Based VM Backup servers. As a result, when you deploy policies that contain a recovery method that is defined as Automatically start the virtual machine to nodes that are protected by Host-Based VM Backup, Virtual Standby changes the value of the recovery method to Manually start the virtual machine.

The solution to this behavior is to protect the virtual machine using CA ARCserve D2D or CA ARCserve Central Protection Manager.

Chapter 6: Applying Best Practices

This section contains the following topics:

[How the Installation Process Affects Operating Systems](#) (see page 199)

[How CA ARCserve Central Virtual Standby Licensing Works](#) (see page 204)

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, upgrade, or uninstall 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 and uninstall 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.
CallPreUninstall	Lets the uninstallation process perform various tasks relating to uninstallation. For example, un-registering CA ARCserve Central Applications from the Windows Registry.

Component	Description
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
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
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications

Binary Name	Source
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

How CA ARCserve Central Virtual Standby Licensing Works

CA ARCserve Central Virtual Standby contains the following licenses:

- CA ARCserve Central Virtual Standby-Physical
- CA ARCserve Central Virtual Standby-VMware
- CA ARCserve Central Virtual Standby-Hyper-V

All of the licenses are count-based. CA ARCserve Central Virtual Standby verifies and grants licenses to CA ARCserve D2D nodes based on the following criteria:

- CA ARCserve Central Virtual Standby applies CA ARCserve Central Virtual Standby-Physical licenses to all CA ARCserve D2D nodes that you add by Name/IP address or import from a file. CA ARCserve Central Virtual Standby grants CA ARCserve Central Virtual Standby-Physical licenses to the nodes after you apply a policy to the nodes and start the virtual conversion process.

Note: This is the default behavior for CA ARCserve Central Virtual Standby licensing.

- CA ARCserve Central Virtual Standby applies CA ARCserve Central Virtual Standby-VMware licenses to all CA ARCserve D2D nodes that you add by Name/IP address or import from a file, and are VMware virtual machines that reside on ESX Server systems or vCenter Server systems. However, before CA ARCserve Central Virtual Standby can apply the CA ARCserve Central Virtual Standby-VMware licenses to the nodes, you must associate the nodes with a specific ESX Server system or vCenter Server system.

Note: For more information, see [Specify the ESX Server or vCenter Server System for VMware-Based Nodes](#) (see page 29).

CA ARCserve Central Virtual Standby grants the CA ARCserve Central Virtual Standby-VMware licenses to each ESX Server system after you apply a policy to the nodes and start the virtual conversion process.

- CA ARCserve Central Virtual Standby applies CA ARCserve Central Virtual Standby-VMware licenses to all virtual machine nodes that you import from a CA ARCserve Central Host-Based VM Backup system. CA ARCserve Central Virtual Standby grants the CA ARCserve Central Virtual Standby-VMware licenses to virtual machine nodes after you apply a policy to the nodes and start the virtual conversion process.
- CA ARCserve Central Virtual Standby applies CA ARCserve Central Virtual Standby-Hyper-V licenses to all CA ARCserve D2D nodes that you add by Name/IP address or import from a file and reside on a Hyper-V hypervisor. CA ARCserve Central Virtual Standby detects the presence of the Hyper-V server when you add by the nodes by Name/IP address or import the nodes from a file. CA ARCserve Central Virtual Standby grants the CA ARCserve Central Virtual Standby-Hyper-V licenses to CA ARCserve D2D nodes after you add the nodes by Name/IP address or import the nodes from a file.

Count Mechanism

The following table describes the quantity of CA ARCserve Central Virtual Standby licenses required for a given scenario.

Type of D2D Node	License Required	Count Mechanism
Physical node	CA ARCserve Central Virtual Standby-Physical	One license for each node
VMware virtual machine	CA ARCserve Central Virtual Standby-VMware	One license for each ESX/vCenter Server system
Hyper-V virtual machine	CA ARCserve Central Virtual Standby-Hyper-V	One license for each Hyper-V system

Examples

- CA ARCserve Central Virtual Standby is protecting five physical CA ARCserve D2D nodes. Five CA ARCserve Central Virtual Standby-Physical licenses are required.
- CA ARCserve Central Virtual Standby is protecting three VMware virtual machines that reside on one ESX Server system. One CA ARCserve Central Virtual Standby-VMware license is required.
- CA ARCserve Central Virtual Standby is protecting 100 VMware virtual machines distributed on ten ESX Server systems. Ten CA ARCserve Central Virtual Standby-VMware licenses are required.
- CA ARCserve Central Virtual Standby is protecting 20 Hyper-V virtual machines distributed on five Hyper-V systems. Five CA ARCserve Central Virtual Standby-Hyper-V licenses are required.
- CA ARCserve Central Virtual Standby is protecting three Hyper-V virtual machines that reside on one Hyper-V system and three VMware virtual machines that reside on one ESX Server system. One CA ARCserve Central Virtual Standby-VMware license is required and one CA ARCserve Central Virtual Standby-Hyper-V license is required.
- CA ARCserve Central Virtual Standby is protecting five VMware virtual machines that were imported from CA ARCserve Central Host-Based VM Backup and reside on one ESX Server system. One CA ARCserve Central Virtual Standby-VMware license is required.

Glossary

Heartbeat

A heartbeat is an electronic signal that source nodes send to monitor servers to identify the status of the node.

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.

Monitor Server

A monitoring server is a server that verifies the status of source servers in CA ARCserve Central Virtual Standby environments.

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.

Recovery Point

A recovery point 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.

Recovery Point Snapshot

A Recovery Point Snapshot is VMware Virtual Disk (VMDK) or Microsoft Virtual Hard Disk (VHD) files that CA ARCserve Central Virtual Standby creates from CA ARCserve D2D recovery points. CA ARCserve Central Virtual Standby lets you power on virtual machines using Recovery Point Snapshots when the source servers that are running CA ARCserve D2D in your production environment fail.

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.

Virtual Conversion

Virtual conversion is the process where CA ARCserve Central Virtual Standby converts CA ARCserve D2D recovery points from source nodes to virtual machine data files named recovery point snapshots.

Index

A

- Access Denied Errors Occur when Adding a Node by IP/Name • 185
- Add Links to the Navigation Bar • 75
- Add New Tab Link Not Launching Properly for Internet Explorer 8, 9, and Chrome • 195
- Add New Tab Link, RSS Feeds, and Social Networking Feedback Not Launching Properly on Internet Explorer 8 and 9 • 197
- Add Node Groups • 28
- Add Nodes by IP Address or Node Name • 27
- Add Nodes from CA ARCserve Central Host-Based VM Backup Servers • 48
- Application Configuration Tasks • 68
- Applying Best Practices • 199
- Assign Nodes to a Policy • 38

B

- Backup and Recovery Jobs Do Not Use the SAN Transport Mode • 193
- Backup and Recovery Jobs Using the hotadd Transport Mode Cannot Mount Disks • 194
- Binary Files Containing Incorrect File Version Information • 201
- Binary Files that Do Not Contain an Embedded Manifest • 201
- Binary Files that have a Privilege Level of Require Administrator in Manifest • 202
- Blank Webpages Appear or Javascript Errors Occur • 172

C

- CA ARCserve Central Applications Bookshelf • 14
- CA ARCserve Central Virtual Standby Cannot Communicate with the CA ARCserve D2D Web Service on Remote Nodes • 182
- CA ARCserve Central Virtual Standby Monitoring Tasks • 81
- CA ARCserve D2D Web Service Fails on CA ARCserve D2D Nodes • 177
- CA Technologies Product References • 3
- Cannot Connect to Specified Server Messages Appear When Attempting to Add Nodes • 170

- Cannot Specify an Asterisk or Underscore as a Wildcard in Filter Fields Using Japanese Keyboards • 198
- Certificate Error Appears When You Log In to the Application • 183
- Change Server Communication Protocol • 167
- Configure Automatic Updates • 69
- Configure Email Settings • 68
- Configure Proxy Settings • 70
- Configure Social Networking Preferences • 72
- Contact CA • 3
- Create Policies • 30

D

- Delete Activity Log Records • 91
- Delete Node Groups • 57
- Delete Nodes • 52
- Delete Policies • 67
- Deploy Policies • 40
- Documentation Changes • 5

E

- Edit or Copy Policies • 58

F

- Filter Node Groups • 57

G

- Garbage Characters Appear in Browser Windows When Accessing CA ARCserve Central Applications • 176
- Getting Started With CA ARCserve Central Virtual Standby • 25

H

- Heartbeat • 207
- HOTADD Transport Mode • 207
- How CA ARCserve Central Virtual Standby Licensing Works • 204
- How CA ARCserve Central Virtual Standby Works • 12
- How the Installation Process Affects Operating Systems • 199

How to Protect Virtual Standby Virtual Machines • 100
How to Troubleshoot Page Loading Problems • 174
How to Use the Servers List • 77
How to Use the Virtual Standby Summary Screen • 76

I

Import Nodes from a File • 46
Install CA ARCserve Central Virtual Standby • 17
Install CA ARCserve Central Virtual Standby Silently • 20
Installation Considerations • 16
Installing CA ARCserve Central Virtual Standby • 15
Introducing CA ARCserve Central Virtual Standby • 11
Introduction • 11
Invalid Credentials Message Appears When Adding Nodes • 184
Invalid Credentials Messages on Windows XP • 185

L

Log in to CA ARCserve Central Virtual Standby • 26
Log In to CA ARCserve D2D Nodes • 43
Log in to Monitor Servers • 44

M

Modify Node Groups • 55
Modify the Administrator Account • 73
Monitor Server • 207
Monitor the Status of Virtual Conversion Jobs • 79

N

NBD Transport Mode • 207
NBDSSL Transport Mode • 207
Node • 207
Node Group • 207
Node Group Management Tasks • 55
Node Maintenance Tasks • 45
Nodes Do Not Appear on the Node Screen After Changing the Name of the Node • 187

O

Operating System Not Found Errors Occur • 187

P

Pause and Resume Heartbeats from the Nodes • 83

Pause and Resume Heartbeats from the Virtual Standby Server • 81
Pause and Resume Virtual Standby Jobs from the Nodes • 85
Pause and Resume Virtual Standby Jobs from the Virtual Standby Server • 84
Policy • 207
Power on Virtual Standby Virtual Machines from Hyper-V Manager • 87
Power on Virtual Standby Virtual Machines from Recovery Point Snapshots • 86
Power on Virtual Standby Virtual Machines from VMware vSphere Client • 88
Prerequisite Installation Tasks • 15

R

Recover Source Servers Using CA ARCserve D2D Backup Data • 118
Recover Source Servers Using Data from Hyper-V Virtual Standby Virtual Machines • 133
Recover Source Servers Using Data From VMware Virtual Standby Virtual Machines • 146
Recovering Source Servers Using Bare Metal Recovery • 116
Recovery Point • 207
Recovery Point Snapshot • 208
Release Licenses from Nodes • 52
Restore Data from CA ARCserve D2D File Copies • 107
Restore Data from CA ARCserve D2D Recovery Points • 102
Restore Data Using Find Files/Folders to Restore • 112
Restore Microsoft Exchange Email Messages • 160

S

SAN Transport Mode • 208
Specify the ESX Server or vCenter Server System for VMware-Based Nodes • 29
Stop Monitoring Nodes from the Monitor Server • 54

T

The CA ARCserve D2D Web Service Runs Slowly • 180
Troubleshooting CA ARCserve Central Virtual Standby • 169
Troubleshooting Error Numbers • 195

U

- Unassign Nodes from Policies • 66
- Uninstall CA ARCserve Central Virtual Standby • 19
- Uninstall CA ARCserve Central Virtual Standby Silently • 22
- Update Nodes • 50
- Update Nodes and Policies After Changing the Host Name of the CA ARCserve Central Applications Server • 54
- Using CA ARCserve Central Virtual Standby • 43

V

- Verify That the CA ARCserve Central Virtual Standby Server Can Communicate With the Nodes • 25
- View Activity Log Data about Jobs • 89
- View Information About Policies Assigned to CA ARCserve D2D Nodes • 95
- View Logs • 74
- View Status Information About Virtual Standby Jobs from the Nodes • 93
- View Status Information About Virtual Standby Jobs from the Virtual Standby Server • 92
- View Summary Information about the Latest Virtual Standby Job • 77
- View the Recovery Point Snapshots List • 80
- View Virtual Standby Settings for Source Servers • 80
- Virtual Conversion • 208
- Virtual Machines Do Not Power On Automatically • 198
- Virtual Standby Home Page • 75
- Virtual Standby Jobs End with No Sessions Warning Messages • 192
- Virtual Standby Jobs Fail Due to Internal Errors • 188
- Virtual Standby Jobs Fail Using the hotadd Transport Mode • 191
- Virtual Standby Jobs to Hyper-V Systems Fail • 188
- Virtual Standby Policy Management Tasks • 58
- Virtual Standby Settings • 96
- Virtual Standby Status Monitor • 94

W

- Web Pages Do Not Load Properly When Logging in to CA ARCserve D2D Nodes and Monitoring Servers • 175