Arcserve® Backup for Windows

Disaster Recovery Option Guide

r16.5

arcserve®

Arcserve Product References

This document references the following Arcserve products:

- Arcserve® Backup
- Arcserve® Unified Data Protection
- Arcserve® Unified Data Protection Agent for Windows
- Arcserve® Unified Data Protection Agent for Linux
- Arcserve® Replication and High Availability

Contact Arcserve

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

https://www.arcserve.com/support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.

You can access other helpful resources appropriate for your Arcserve product.

Documentation Changes

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

- 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.

- Updated the section Recovering from a Disaster Recovery using WinPE (see page 31). This section now contains updated information that describes the operating systems that support recovering from a disaster using Windows PE, the operating systems that support the installation of Windows ADK, and how you can recover computers running Windows 8 and Windows Server 2012 from a disaster.

- Updated the section Recovering Clusters (see page 167). This section now contains updated information that describes how to recover clusters running Windows 8 and Windows Server 2012 from a disaster.

- Updated the section Overview of Windows PE Disaster Recovery (see page 31). This section now contains updated information that describes the installation of AIK (Windows Automated Installation Kit).

Patch 1 Updates:

- Updated the section Overview of Windows PE Disaster Recovery (see page 31). This section now includes support for Windows ADK 8.1.

Contents

Appendix E: Staging Using File System Devices   197

Appendix F: Recovering Servers with StorageTek ACSLS Libraries   199

Appendix G: Recovering Windows 2003 Small Business Server   203

Appendix H: Recovering Data from a Physical to Virtual Machine   211

Appendix I: Recovering Data Without Using a Floppy in Windows 2003 and Windows XP   221

Glossary   237

Index   241

Chapter 1: Introducing Disaster Recovery Option

This section contains the following topics:

Introduction

Disaster recovery is a backup and recovery process used to protect computing environments against the loss of data caused by a catastrophic events or natural disasters. Disasters can be caused by fire, an earthquake, employee sabotage, a computer virus, or a power failure.

There are many time consuming tasks—including installation of the base operating systems and setup of the servers—that would usually have to be manually performed after a disaster. The Arcserve Backup Disaster Recovery option lets you restore your server reliably, making more efficient use of time by taking you from boot media, to backup media, to an operational state and allows users with minimal server configuration experience to recover sophisticated systems.

Disaster Recovery Option

The Disaster Recovery Option is based on the concept of collecting and saving machine-specific information before a disaster strikes. When you submit a full backup job, the option automatically generates and saves emergency data for each protected machine locally on the backup server, on backup media, and, optionally, on a remote computer. In the event of a disaster, the option can recover its protected computers to their most recent backup state.

The option generates or updates information for disaster recovery when it performs a full, synthetic full, incremental or differential backup of a computer or a local backup server whenever the Arcserve Backup database is backed up (when the volume on which it resides is backed up).

Disaster Recovery Methods

This section provides disaster recovery methods for specific versions of Windows.

Windows Server 2008/Windows 7

The Disaster Recovery Option supports local and remote disaster recovery for Windows Server 2008 and remote disaster recovery for Windows 7. The option provides the following boot method:

Bootable CD method: To use this method, you must have the following:

- Windows Server 2008 or Windows 7 installation media

- A Machine Specific Disk (MSD)

- Arcserve Backup CD/DVD

Important! The Windows Server 2008 or Windows 7 installation media that you use to perform disaster recovery must be the same version you used to install before the disaster happened.

Windows XP and Windows Server 2003

The Disaster Recovery Option supports local and remote disaster recovery for Windows Server 2003. The option provides the following boot methods:

Bootable CD Method

This method is built on the Microsoft Windows Automated System Restore (ASR) framework.

To use this method, you must have the following:

- Windows XP or Windows Server 2003 installation media

- Machine Specific Disk (MSD)

- Arcserve Backup CD/DVD

You can also use the reimaged or remastered Bootable CD for this method.

Important! The Window XP or Windows Server 2003 installation media that you use to perform disaster recovery must be the same version you used to install before the disaster happened.

Bootable Tape Method

Rather than booting from a Windows 2003 installation media, you can boot directly from a tape drive. The only required media is the tape media containing the backup data.

More information:

Disaster Recovery Option Support

The following table provides Disaster Recovery Option support information:

Boot Kit Type	Required Media for Disaster Recovery	Supported Operating Systems
Machine Specific Disk (MSD)	Operating System Installation media + Arcserve Backup CD/DVD + Floppy or USB Stick (for Windows Server 2008 only)	■ <win> XP (32-bit) ■ <win> XP (x64) ■ <win> Server 2003 (32-bit) ■ <win> Server 2003 (x64) ■ <win> Server 2008 (32-bit) ■ <win> Server 2008 (x64) ■ <win> Server 2008, Core 32-bit (Remote DR only) ■ <win> Server 2008 Core 64-bit (Remote DR only) ■ Windows 7 32-bit (Remote DR only) ■ Windows 7 x64 (Remote DR only)
Bootable CD for <win> XP/<win> Server 2003 ■ Operating System ■ Disaster Recovery Option ■ MSD ■ Drivers (NIC and SCSI/RAID/FC)	CD + Arcserve Backup CD/DVD + Floppy In <win>XP and <win> Server 2003, you can integrate everything into a single Bootable CD, so no floppy disk is required.	■ <win> XP (32-bit) ■ <win> XP (x64) ■ <win> Server 2003, 32-bit ■ <win> Server 2003 (x64)

Boot Kit Type	Required Media for Disaster Recovery	Supported Operating Systems
Patched Arcserve Backup Disaster Recovery CD	Floppy + <win> Operating System installation media + CD The new Arcserve Backup Disaster Recovery CD will include all device/DR Option/Agent patches applied to Arcserve Backup installation.	■ <win> XP (32-bit) ■ <win> XP (x64) ■ <win> Server 2003 (32-bit) ■ <win> Server 2003 (x64) ■ <win> Server 2008 (32-bit) ■ Windows server 2008 x64
Bootable Tape Image	Tape	■ <win> Server 2003 (32-bit)
Using Microsoft Remote Installation Server (RIS)	None. Disaster Recovery Option boots using PXE	■ <win> XP (both 32-bit and 64-bit) ■ <win> Server 2003 (both 32-bit and 64-bit)
WinPE Disaster Recovery Image	Arcserve Backup CD/DVD	■ <win> Server 2003 (32-bit or x64) ■ <win> Server 2008 (32-bit or x64) ■ <win> Server 2008 R2 ■ <win> 7 32-bit or x64 ■ <win> 8 32-bit or x64 ■ <win> Server 2012

Global Options for Disaster Recovery

The Disaster Recovery option supports two global job options. You can access these options from the Advanced tab of the option's dialog when creating a backup job.

Generate DR information for partially selected nodes

Lets you explicitly force disaster recovery information to be generated when backing up a subset of a machine. By default, disaster recovery information is generated for a machine after every full backup of that machine. A full backup requires that you select the entire machine node by selecting the green marker completely.

Note: This option only takes effect if the version of the Arcserve Backup Client Agent for Windows on your Windows machine is the same as the version of Arcserve Backup running on your server.

Include filtered sessions when generating restore session information

Lets you explicitly force the option to include the filtered sessions. When generating disaster recovery information for a machine, the latest backup sessions of all drive volumes and system states are recorded for the machine. By default, the option skips all sessions set with a filtered flag, so these sessions are never used by the option to recover a machine.

Note: Arcserve Backup sets the filtered flag if any file in a session is not backed up because of a filtering policy on the backup job.

Disaster Recovery on Database Applications

Arcserve Backup has special agents to back up database applications. Some of the commonly used database applications include:

- Oracle

- Microsoft SQL Server

- Microsoft Exchange Server

- Lotus Notes

If you have backed up one or more of these databases using Arcserve Backup database agents, the databases are *not* automatically restored as part of the disaster recovery process.

When Arcserve Backup backs up database sessions, additional media sessions are created, separate from the rest of the machine backup. Disaster recovery does not automatically restore these database sessions. However, after you restore the rest of the server using the Disaster Recovery Option, you can start Arcserve Backup and begin a normal database restore procedure using the corresponding application agent. See the corresponding agent guide for more information.

How Arcserve Backup Protects System Volumes Without a Drive Letter

A system volume is the disk volume that contains the hardware-specific files required to start Windows, such as BOOTMGR. A boot volume is the disk volume that contains the Windows operating system files and its supporting files. A computer contains one system volume; however, there is one boot volume for each operating system in a multiboot system.

The files contained in the system volume can reside in the system drive (c:\), in a volume that does not contain a drive letter, or in a named volume. On Windows Server 2008 R2 systems, the system volume may not necessarily reside in the boot system drive (c:\). By default, the system volume is usually a volume without a drive letter.

The Arcserve Backup protect the system volumes as part of the computer's system state. You can back up the system state explicitly or dynamically.

Note: For information about explicit job packaging and dynamic job packaging, see the *Arcserve Backup Administration Guide*.

Arcserve Backup lets you back up the entire boot volume as part of the system state. To recover one file, several files, or all files from the system state, and data files contained in the boot volume, you must perform a full recovery of the system state. You can then recover the system state, or system volume, as part of the disaster recovery process. To use this approach, you must create a Arcserve Backup Disaster recovery CD.

For more information about how to create disaster recovery CD, see .

Chapter 2: Installing the Disaster Recovery Option

This chapter describes how you can install the Disaster Recovery option. It also provides information on the pre-installation and post-installation tasks.

This section contains the following topics:

Preinstallation Tasks

This section describes the information that you must review before you install, and the software you must have while you configure the option.

Prerequisite Software

Verify that you have Arcserve Backup installed before installing the option. You can install Arcserve Backup and the option in the same session or at different times.

Documentation

Before you install the option, we recommend that you review the following documents:

Readme

Contains the operating system requirements, hardware and software prerequisites, last minute changes, and all known issues with the software. The readme file is provided in HTML format and is located at the root level on the product CD.

Implementation Guide

Provides an overview of product features and functions, basic concepts, installation information, and an introduction to the product. It is provided as a printed document, and in Adobe Portable Document Format (PDF) on the product CD.

Release Summary

Lists new features and changes to the existing features that are included in the release. The Release Summary is provided in PDF format.

Alternate Location for Disaster Recovery Information Configuration

When you back up a local or remote Arcserve Backup client computer, the Arcserve Backup server saves the computer-specific information required to perform disaster recovery tasks.

If the Arcserve Backup server fails, the computer-specific disaster recovery information can be lost as well. To avoid this type of data loss, the option can store machine specific disaster recovery information to a remote location on an alternate computer. This feature allows you access disaster recovery information and create machine specific disks even if the Arcserve Backup server fails.

Note: If you are upgrading or migrating from an earlier version of Arcserve Backup or BrightStor Enterprise Backup, and you had previously configured an alternate location to store disaster recovery information, you can use the same location with the Disaster Recovery Option.

The alternate location used to maintain disaster recovery information has a dedicated folder for each machine protected by the option.

You can enable the alternate location while configuring the option after installation or at a later time. To enable this feature, you must first create a shared folder on the remote computer, and then configure the option to send information to that shared folder.

Set Up Alternate Machine Locations to Replicate Disaster Recovery Information

You can set up alternate locations to replicate disaster recovery information.

Arcserve Backup uses the following process to replicate information:

■ Creates a temporary operating system working environment.

■ Sets the environment's configuration to be the same as the disk and the network.

■ Restores data to the system so that the computer can return to its latest backup state.

These operations cannot be executed automatically if there is no record of the original system settings. Therefore, the relevant system information must be gathered during backup operations for disaster recovery purposes.

When you perform a full backup of a client computer, specific disaster recovery information is generated for that computer. This information is stored on the backup server and is used to create the disaster recovery media to recover the protected computer in the event of a disaster.

Important! We recommend that you set up an alternate location for disaster recovery to allow you to replicate the information to a remote computer as backup copies. If the backup server itself fails, you can recover it automatically using disaster recovery.

To set up an alternate location for disaster recovery information

1. Create a shared folder on the remote computer to receive the replicated information.

2. Click Config on the Create Boot Kit wizard dialog.

   The Alternate Location for DR dialog opens.

3. Enter information to set the alternate location.

4. Run the Create Boot Kit wizard to continue the disaster recovery process.

More information:

Create Shared Folders for Disaster Recovery Alternate Locations (see page 20)

Create Shared Folders for Disaster Recovery Alternate Locations

You can create shared folders to replicate disaster recovery information in alternate locations.

To create the shared folder

1. Create a folder and give it an appropriate name.

    You can create this folder anywhere on the system where shared folders are allowed.

    Note: The volume must be located on a fixed disk.

2. Right-click the folder and select Properties from the pop-up menu.

    The Properties dialog opens.

3. Click the Sharing tab.

4. Select the Share this folder option and enter the share name.

5. Set the User limit you require and click Permissions.

    The Permission dialog opens.

    Note: We recommend that you specify the Maximum Allowed option.

6. Click Add to add the user account you used when you set up your alternate location for disaster recovery information to the Share Permissions list.

    You can add this account explicitly or you can specify a user group to which the account belongs (this information also applies if you add a domain account):

    Add Account Explicitly

    If the user account exists on the machine and is part of a local user group, you can add that specific user account to add it explicitly.

    Add User Account Implicitly

    If the user account exists on the machine and is part of a local user group, you can add the entire local user group to add the user account implicitly.

7. Click the boxes in the Allow column to specify Full Control on the share folder.

8. Click Apply, and then click OK.

9. In the Properties dialog, click the Security tab.

    Edit the security list on this tab to ensure the user account used during the setup of the alternate location has Full Control on permissions. The user account can be added explicitly or implicitly (as part of a user group) as described in the previous steps.

10. Click Apply and click OK.

11. Verify that the shared folder works properly. To do so, from a remote computer, try to connect or map to the shared folder with the user account you used when setting up the alternate location and, when connected, verify that you can create, modify, and remove files and directories on the shared folder.

Set Up Alternate Locations with the Disaster Recovery Wizard

The Config option in the Disaster Recovery wizard lets you specify information about the alternate location where you store information about the disaster recovery. You can also set up an alternate location for disaster recovery information when you install the Disaster Recovery Option.

To set up an alternate location using the Disaster Recovery Wizard

1. Click Config.

   The Alternate Location for DR Information dialog opens.

This dialog contains the following fields:

Alternate Machine Name

The hostname of the machine where the shared folder resides. The IP address of this machine can also be used but we do not recommend this, particularly in DHCP environments.

Windows Domain

If the user account used is part of a domain, enter the domain name. If a local account is used, enter the name of the local machine.

Note: Ignore this field if you specified domain information in the User Name field.

User Name

The user account used to connect to the machine on which the alternate location resides. The domain part of the user name is optional. For example, if the full user account name is domainX\userX, you can enter userX.

Password

The password for the specified user account.

Path

The path for the shared folder in which to store the replicated disaster recovery information.

2. When you have specified all of the required information, click OK.

Create Machine Specific Disks from Alternate Locations in Windows Server 2008

You can create machine specific disks from alternate locations for Windows Server 2008.

To create a machine specific disk from an alternate location

1. Prepare an empty floppy disk. Format the disk, if necessary, so it can be used by the operating system.

2. In the alternate location configured to store the disaster recovery information, locate the folder for the machine for which the recovery disk needs to be created.

   The name of this folder should be the same as the name of the machine that needs to be recovered.

3. Copy all the files from within the machine specific folder, identified in step 2, to the floppy disk.

   Note: Ensure you copy the file, not the directory.

4.   Run the following steps to recover the Windows Server 2008:

For Windows Server 2008 (32-bit)

a.   Locate the folder drpatch.xp in the alternate location configured to store the disaster recovery information.

b.   Copy drlaunch.ex_ and drlaunchres.dl_from the drpatch.xp directory to a floppy disk.

c.   Create a new file on floppy disk and name it DRCOPYFILES.BAT.

The DRCOPYFILES.BAT file is created.

d.   Write following text into DRCOPYFILES.BAT file:

```
expand -r %~dp0\drlaunch.ex_ x:\windows\system32\
expand -r %~dp0\drlaunchres.dl_ x:\windows\system32\
exit
```

e.   Locate the folder DRPATCH.W2K8 in the alternate location and copy Autounattend.xml to a floppy disk.

Note: Ensure that you copy the files, and not the directory.

For Windows Server 2008 (x64-bit)

f.   Locate the folder drpatch.xp\X64 in the alternate location configured to store the disaster recovery information.

g.   Copy drlaunch.ex_ and drlaunchres.dl_from the drpatch.xp directory to a floppy disk.

h.   Create a new file on floppy disk and name it DRCOPYFILES.BAT.

The DRCOPYFILES.BAT file is created.

i.   Write following text into DRCOPYFILES.BAT file:

```
expand -r %~dp0\drlaunch.ex_ x:\windows\system32\
expand -r %~dp0\drlaunchres.dl_ x:\windows\system32\
exit
```

j.   Locate the folder DRPATCH.W2K8 in the alternate location and copy autounattend_amd64.xml to a temporary directory. Rename the xml file to autounattend.xml, then copy it to a floppy disk.

Note: Ensure that you copy the files, not the directory.

Create Machine Specific Disks from Alternate Locations for Windows Server 2003

You can create machine specific disks from alternate locations for Windows Server 2003.

To create a machine specific disk from an alternate location

1. Prepare an empty floppy disk. Format the disk, if necessary, so it can be used by the operating system.

2. In the alternate location configured to store the disaster recovery information, locate the folder for the machine for which the recovery disk needs to be created.

    The name of this folder should be the same as the name of the machine that needs to be recovered.

3. Copy all the files from within the machine specific folder, identified in step 2, to the floppy disk.

    Note: Ensure you copy the file, not the directory.

4. Run the following steps to recover the Windows Server 2003:

    a. In the alternate location configured to store the disaster recovery information, locate the folder drpatch.xp.

    b. Copy drlaunch.ex_ and drlaunchres.dl_ under the drpatch.xp directory to the floppy disk.

    c. Copy the file drlaunchres.dl under the drpatch.xp\ENU directory to a temporary directory, rename it as drlaunchenu.dl_, and then copy it to the floppy disk.

    Note: Ensure that you copy the file, and not the directory.

General Considerations

Consider the following points when setting up an alternate location for disaster recovery information:

■ Although you can set up an alternate location for disaster recovery information on the local backup server and replicate this information locally, we recommend that you use a remote machine.

- Although this is not recommended, when specifying the shared folder name in the Disaster Recovery Wizard, you can use a shared drive and any folder or subfolder on that drive to specify that disaster recovery information is to be replicated to that folder. If you must do so, ensure that the folder itself and all parent folders, including the shared drive, have proper security and permission settings for the user account being used.

- Connection to the remote shared folder is established using Windows network services. This is fully supported by Microsoft but the service itself has a limitation. If a connection already exists to the remote machine hosting the shared folder, the wizard cannot verify and use the user account information you provide. The replicating operation relies on the existing connection and the credential supplied there.

  Note: For information, see the Microsoft Knowledge Base article at http://support.microsoft.com/

Install and Configure the Option

You must install Arcserve Backup before you install the Disaster Recovery Option. You cannot install the option if Arcserve Backup has not been installed. You can, however, install the option with Arcserve Backup in the same session.

For more information about installing Arcserve Backup, see the *Implementation Guide*.

To install and configure the option

1. In the Select Product dialog, choose Disaster Recovery Option and click Next.

   The option is installed in the same directory as the base product.

2. If you are installing Arcserve Backup and the option at the same time, then select your database, set your password, and enter system account information.

   The Product List opens.

3. Verify the components to be installed, and then click Install.

   The licensing information opens.

4. Click Continue.

   A summary of the components that have been installed opens. This summary identifies the components you are installing that require configuration. The summary identifies the option as one of the components requiring configuration.

5. Click Next.

6. Configure an alternate location on a remote computer in which to store a backed up copy of your disaster recovery information.

   We strongly recommend that you use the alternate location feature, to let you create machine specific disks even after a disaster on your backup server.

7. Select the Alternate Location for DR information by clicking the Config option.

8. Fill up information for alternate machine name, the Windows domain, user name, password, and the name of the shared folder on the remote server where the disaster recovery information will be stored.

   Note: To use an alternate location on a remote computer to store disaster recovery information, you must have previously created a shared folder on the remote computer in which to store this information. If you have not previously created this shared folder, you can enable this feature at any time after configuring the option. To configure alternate location, start the Disaster Recovery Configuration Wizard and click Config.

   The option is now installed.

How to Perform Disaster Recovery Using the Incremental and Differential Sessions

You can perform disaster recovery using the incremental and differential sessions. This can be done after all backups are run or after every incremental or differential backup. This process works for all the Windows platforms.

To perform disaster recovery using incremental and differential sessions

1. Run series of full and incremental and differential backups using the GFS rotation or custom rotation methods.

   The full, incremental, and differential sessions can reside on different media or the same media.

2. Create a machine specific disk after all backups are run or after every incremental or differential backup.

   The machine specific disk would have information about all backups (full, incremental or differential) that were performed before the MSD was created.

   If you configure an alternate location, you can also create machine specific disks before you perform disaster recovery.

3. Run the disaster recovery process.

   Note: The Disaster Recovery Option will not automatically scan any additional sessions that are backed up after you create machine specific disks.

   The Disaster Recovery Option will automatically restore all the sessions, including full, incremental, and differential sessions shown in the list.

Perform Disaster Recovery Using a Synthetic Full Backup Session

You can perform disaster recovery using a synthetic full backup session. This can be done after the synthetic full backup is run since a synthetic full backup synthesizes a previous full backup session and all incremental sessions to a full session, without the need to utilize previous incremental or differential backups.

Note: Synthetic full backup is only supported on r16 or higher Windows Client Agents.

To perform disaster recovery using a synthetic full backup session

1. Run a synthetic full backup using the GFS rotation or custom rotation methods.

2. Create a machine-specific disk after the synthetic full backup is run.

   The machine-specific disk will contain information about the backup that was performed before the MSD was created.

   If you configure an alternate location, you can also create machine-specific disks before you perform disaster recovery.

3. Run the disaster recovery process.

   Note: The Disaster Recovery Option will not automatically scan any additional sessions that are backed up after you create machine specific disks.

   The Disaster Recovery Option automatically restores the session shown in the list.

Disaster Recovery Utilities

Disaster Recovery Utilities is composed of a set of options that help you perform disaster recovery. You can access these utilities from the disaster recovery Choose Mode dialog.
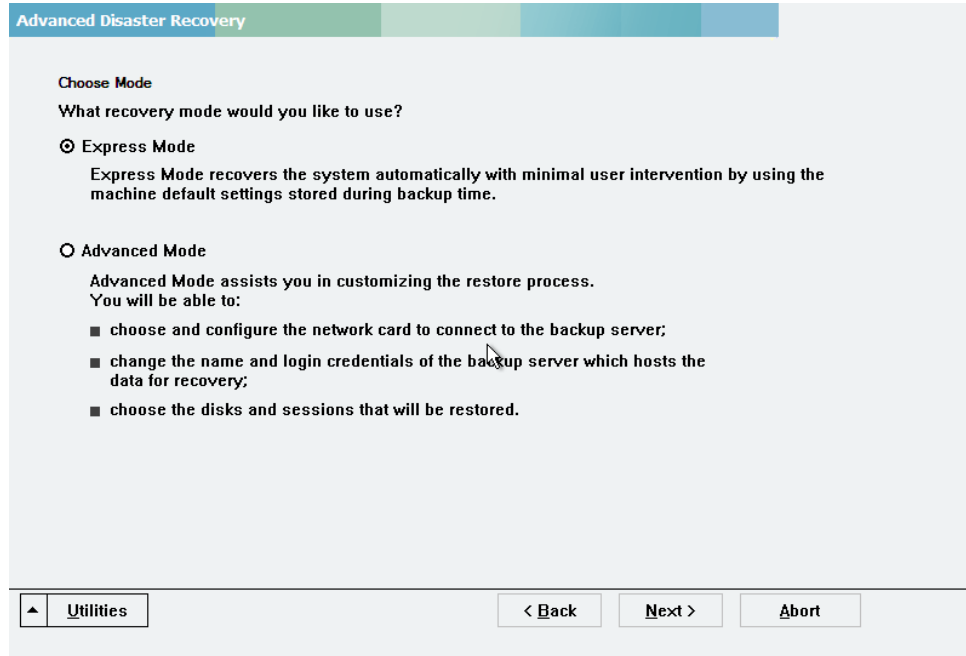
The Disaster Recovery Utilities displays the following options:

Load Driver Utility

Lets you load the third-party drivers. The attached devices are categorized as follows:

– Storage devices

– Network devices

– Other devices and

– Unknown devices

You can select any device listed in the unknown devices catogory and install drivers. Also, you can specify a folder to help the Disaster Recovery wizard to find a driver for the selected device.

Note: During disaster recovery only SCSI, FC, and NIC drivers are required.

IP Configuration Utility

Lets you configure the Network IP address. You can select a network adapter and configure the IP address. This utility can be launched anytime during the disaster recovery process.

Note: While loading DR information, Disaster Recovery wizard will reset the IP address according to the one recorded in the DR information. So if you configure IP address before loading DR information, the IP address might change. System reboot can change the IP address.

Troubleshooting Utility

Displays the default troubleshooting dialog that you can use to resolve errors.

Run Utility

Provides access to the command-line interface to execute commands.

Post-installation Tasks

The online help provides field descriptions, step-by-step procedures, and conceptual information related to the product dialogs. Online help provides a quick and convenient way to view information while you are using the product. In addition, you can obtain diagnostic help for error messages. To access the diagnostic help, double-click the message number in the Activity log.

Chapter 3: Recovering from a Disaster using WinPE

This section contains the following topics:

Overview of Windows PE Disaster Recovery

WinPE (Windows Preinstallation Environment) is a minimal operating system that lets you prepare computers for Windows installations, copy disk images from network shared folders, and initiate Windows setup. Arcserve Backup lets you recover computers running the following operating systems from a disaster using Windows PE recovery CDs:

■ Windows Server 2003

■ Windows Server 2008

■ Windows 7

■ Windows Server 2008 R2

■ Windows 8

■ Windows Server 2012

To create Windows PE recovery disks, Windows Assessment and Deployment Kit 8.1 (Windows ADK 8.1) or Windows Automation Installation Kit (Windows AIK) must be installed on the Arcserve Backup primary server or stand-alone server.

Be aware of the following considerations:

■ When you install Windows ADK on computers running Windows 8, verify that the following Windows ADK features are selected:

   – Deployment Tools

   – Windows Preinstallation Environment (WinPE)

- The installation of Windows Assessment and Deployment Kit (Windows ADK) is not supported on Windows Server 2003 operating systems. As a result, you cannot generate Windows PE recovery CDs on Arcserve Backup servers running Windows Server 2003.

- You can use traditional disaster recovery methods (for example, using machine specific disks) to recover computers running Windows Server 2003, Windows 7, Windows Server 2008, and Windows Server 2008 R2 from a disaster.

- You cannot use traditional disaster recovery methods on computers running Windows 8 and Windows Server 2012. You must use Windows PE recovery CDs to recover computers running these operating systems from a disaster.

- It is required to install Windows Automated Installation Kit (AIK) when you use the WinPE image to restore virtual machines on VMware Workstation 7 or ESX Server 4.0/4.1. You can download AIK from http://www.microsoft.com/en-us/download/details.aspx?id=5753.

  The following operating systems that AIK supports are:

  - Microsoft Windows Server 2003 with Service Pack 2

  - Microsoft Windows Vista SP1

  - Microsoft Windows Server 2008 family

  - Microsoft Windows 7 family

  - Microsoft Windows Server 2008 R2 family

  Note: By default, if both ADK and AIK are installed, the Create Bootable Image utility uses AIK to create WinPE images.

- When you use WinPE to perform a disaster recovery, you may not be able to connect to the backup server or the disaster recovery information (DRIF) location through the network. To correct this behavior, perform one of the following tasks:

  - Copy the following directory from the primary or stand-alone backup server to a USB drive.

    ASBU_Home\DR\PrimaryServerName\AgentName

    Then complete the disaster recovery process and select the DRIF from the USB drive.

  - Copy the following directory from the primary or stand-alone backup server to a machine-specific disk (MSD).

    ASBU_Home\DR\PrimaryServerName\AgentName

    Then complete the disaster recovery process and select the DRIF from the MSD.

  Note: When the MSD does not contain sufficient free disk space (1.44 MB) to copy the DRIF, do not copy the directory named DRV to the MSD.

WinPE Disaster Recovery Limitations

Consider the following limitations when performing a WinPE Disaster Recovery:

- The option does not support recovering from a disaster using the WinPE recovery method on systems running 64-bit versions of StorageTek ACSLS.

- The option does not support Windows Server 2003 iSCSI initiator using the WinPE disaster recovery method, however Arcserve Backup supports iSCSI disks for Windows Server 2003 when you copy the iSCSI initiator binaries from the Windows Server 2008 system.

- The option does not support Disaster Recovery for devices from the Cloud.

- The option does not support recovering Itanium-based operating systems from a disaster.

WinPE Requirements on Windows 8 and Windows Server 2012

To perform disaster recovery operations effectively on computers running Windows 8 or Windows Server 2012, Windows Assessment and Deployment Kit (Windows ADK) must be installed on the Arcserve Backup primary server or stand-alone server. Windows ADK is a Microsoft tool that lets you deploy Windows operating systems to computers. For more information about Windows ADK, see Windows Assessment and Deployment Kit (ADK) for Windows 8 on the Microsoft website.

You can install Windows ADK on backup servers running the following operating systems:

- Windows 7

- Windows Server 2008

- Windows Server 2008 R2

- Windows 8

- Windows Server 2012

You can install Windows ADK using either of the following methods:

- Download the installation media from the Microsoft website and install it on the backup server.

  Note: For more information, see Installing the Windows ADK on the Microsoft website.

■ Use the Arcserve Backup Create Boot Kit Wizard to create bootable media. When you use the wizard to create bootable media, click the option Customize WinPE DR image on the Select Disaster Recovery Boot Kit Type dialog.
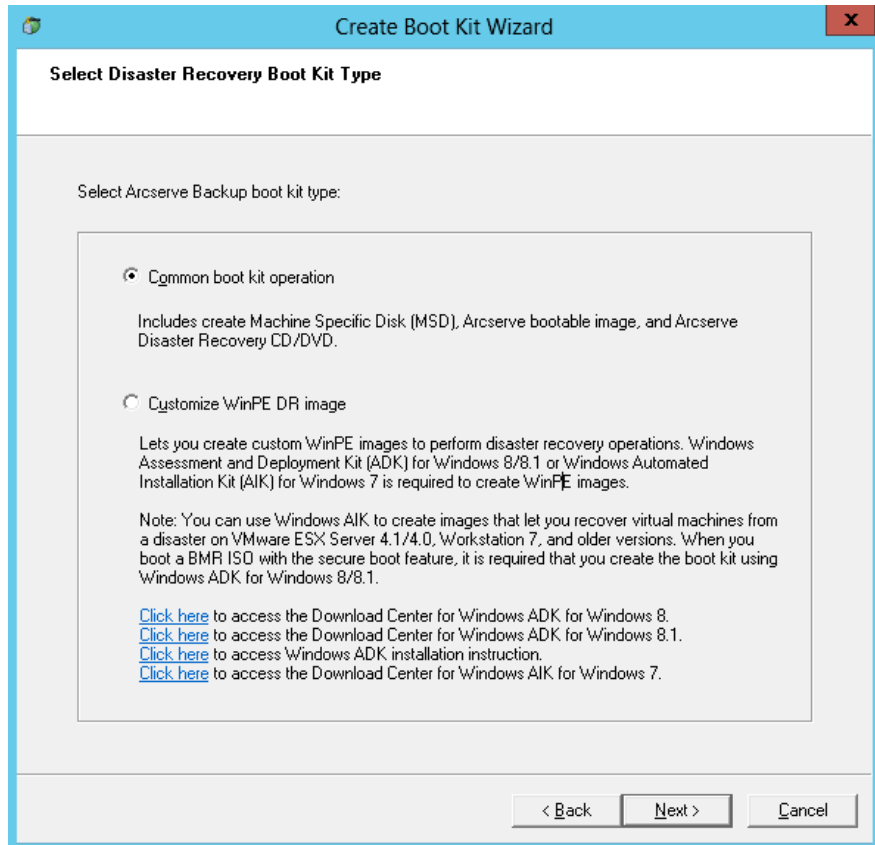
Then click the link on the dialog to open the Microsoft website so that you can download the kit and install it on the backup server. After you install the kit, click Next to continue creating the boot kit

Note: Optionally, you can start the wizard from the Arcserve Backup installation media.
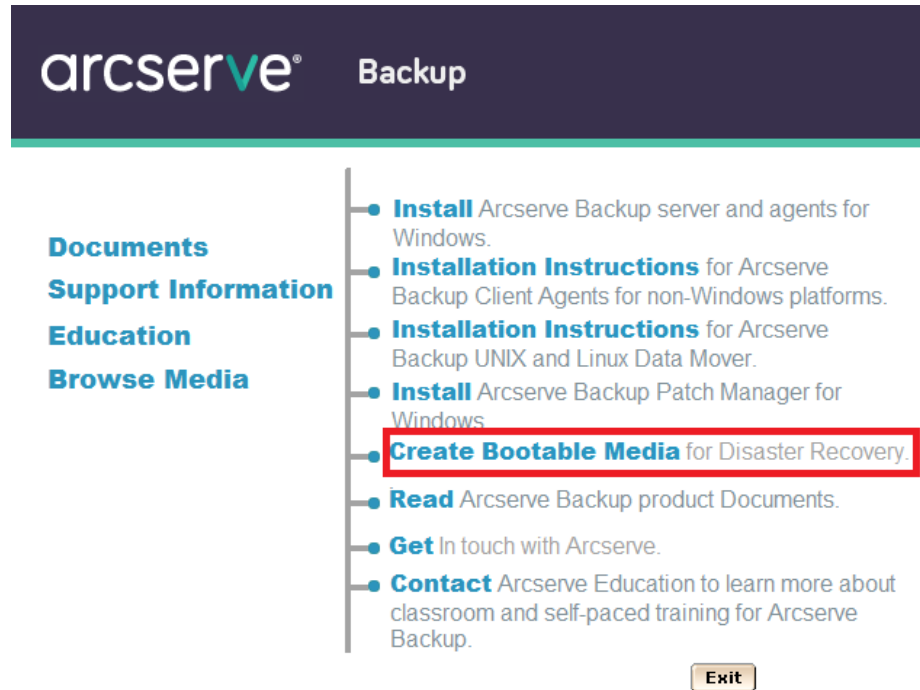
Note: When you install Windows ADK on computers running Windows 8, verify that the following Windows ADK features are selected:

- Deployment Tools
- Windows Preinstallation Environment (WinPE)

Recover Windows Server 2003, Windows Server 2008, Windows 7, Windows Server 2012, and Windows 8 Systems from a Disaster using WinPE

This section describes the process of recovering the following operating systems from a disaster using WinPE (Windows Pre-installation Environment) recovery CD:

■ Windows Server 2003

■ Windows Server 2008

■ Windows 7

■ Windows Server 2012

■ Windows 8

Note: Arcserve Backup Disaster Recovery provides various utilities on each screen that help you resolve problems that you encounter during this process. For more details on these utilities, see How to use Disaster Recovery Utilities (see page 49).

Be aware of the following:

■ The WinPE Disaster Recovery image is not integrated with the Arcserve Backup installation media. You create the WinPE Disaster Recovery image (or disk) manually. To create WinPE recovery disks, Windows Assessment and Deployment Kit (Windows ADK) must be installed on the Arcserve Backup primary server or stand-alone server.

    Note: For more information, see Installing the Windows ADK on the Microsoft website.

■ Use the WinPE recovery image (or disk) to recover computers from a disaster. You can obtain disaster recovery information from the backup server, network, and local locations, such as local disks, MSD or USB sticks.

■ When you perform disaster recovery of a guest operating system that resides on a Hyper-V server, create the WinPE disaster recovery image using Windows Automated Installation Kit (WAIK) for Windows 7.

Note: After a full backup, you can save the disaster recovery information to the location where it can be used during the disaster recovery process.

Follow these steps:

1. Insert the WinPE recovery disk into the computer that you want to recover to open the Windows Boot Manager screen.

2. Select the preferred language and keyboard layout and click Next to open the Select DR Information screen.

3. Select one of the following options to locate the disaster recovery information:

   ■ **Select DR Information from any location**--With this option, browse and select Disaster Recovery Information from your local drive or enter the remote shared folder path in the appropriate field if it is shared on a network and then click ⇨.
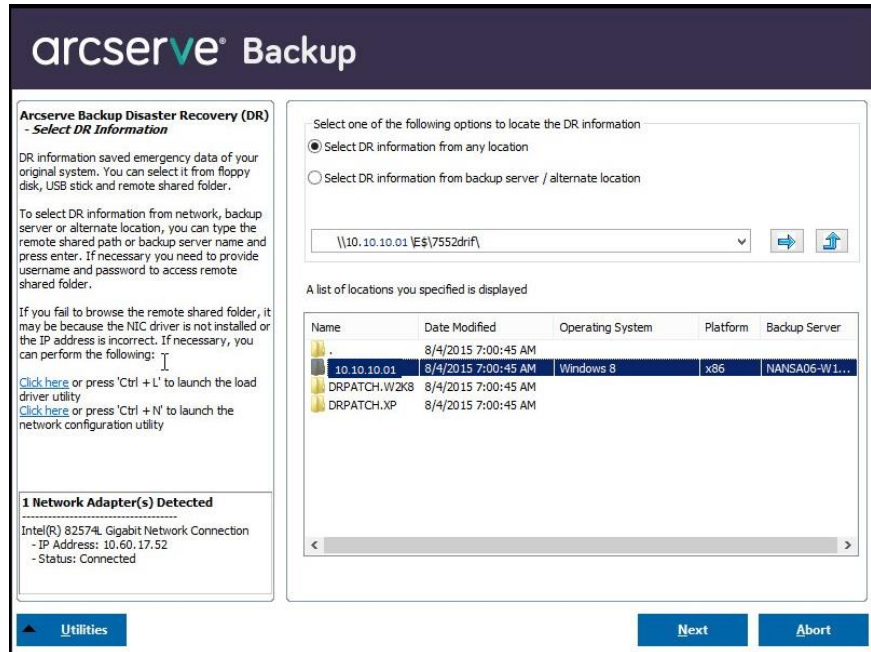
■ **Select DR Information from backup server / alternate location**--With this
option, enter the name of the backup server and then click ➡. A list of Disaster
Recovery Information you specified is displays.
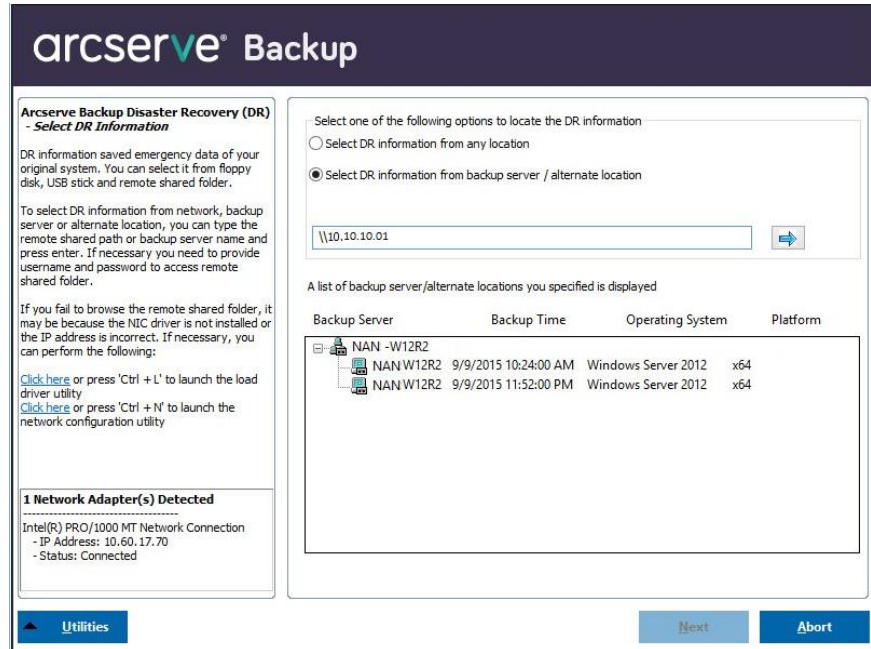
Be aware of the following:

■ You must provide a Windows user name and password to browse network
shared folders.

To browse network shared folders, do the following:

– Verify that the device drivers for the network adapters are installed on the
computer that you want to recover from a disaster.

– Verify that the IP addresses for the network adapters are configured
properly.

Note: To verify that the device driver and IP address are configured properly,
click on the appropriate link from the left pane on any Arcserve Backup Disaster
Recovery screen.

4. Click Next to open the Pre-flight Check screen.

This screen provides a configuration list for you to detect and resolve potential environment issues. Essentially, for each item selected from the Configuration list, a description of that item is displayed at the bottom of the screen describing the issue.

Note: For an updated status of the Configuration List, click Rescan Status.
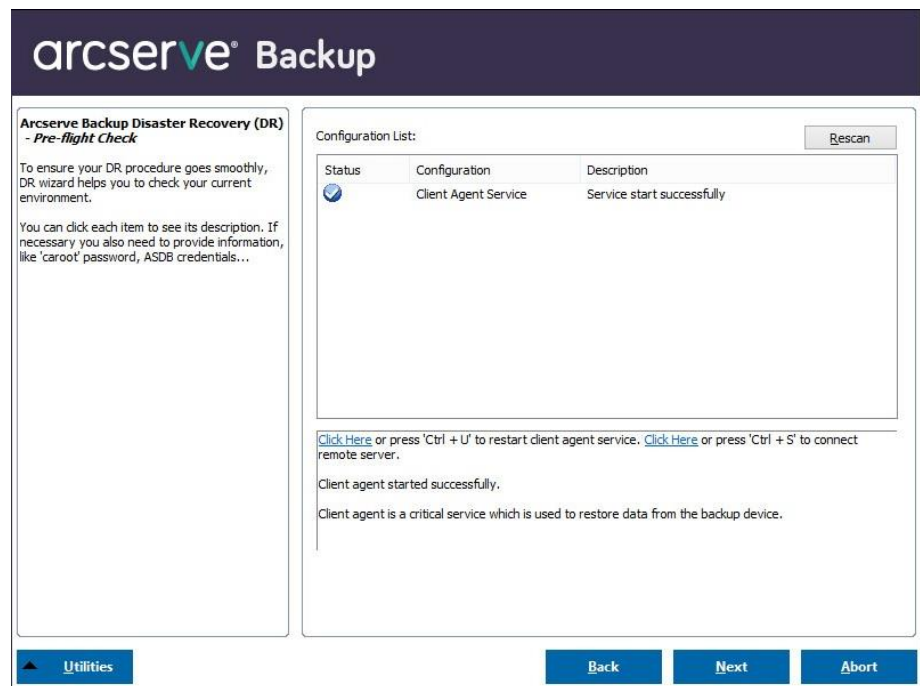
Based on the disaster recovery information selected, the following items display on the screen:

■ **Network Status**

This item displays the status of the network connection.

– If there is no network connection for Disaster Recovery, this item will be displayed on the Pre-Flight Checking page with one of the following statuses:

-- **Error** for remote disaster recovery

-- **Warning** for local disaster recovery

– If the network connection for Disaster Recovery is remote, the status indicates an error.

– If the network connection for Disaster Recovery is local, the status indicates a warning.

– If the network connection for Disaster Recovery is OK, this item will not be displayed.

■ **Hard Disk Status**

This item displays the status of a hard disk.

- If a hard disk is not available, the status indicates an error.

- If a hard disk is available, this item will not be displayed.

■ **Password Management**

If Password Management is used during backup time, a Click Here link appears for you to open the Enter caroot password screen.

■ **iSCSI Configuration**

If iSCSI disks are configured during backup time, a Click Here link appears for you to open the iSCSI disk connection configuration screen to help you configure iSCSI connections.

In this screen, the Original backup system iSCSI information section displays the iSCSI connections during backup time and the Current system connected iSCSI target section displays iSCSI connections during disaster recovery time.
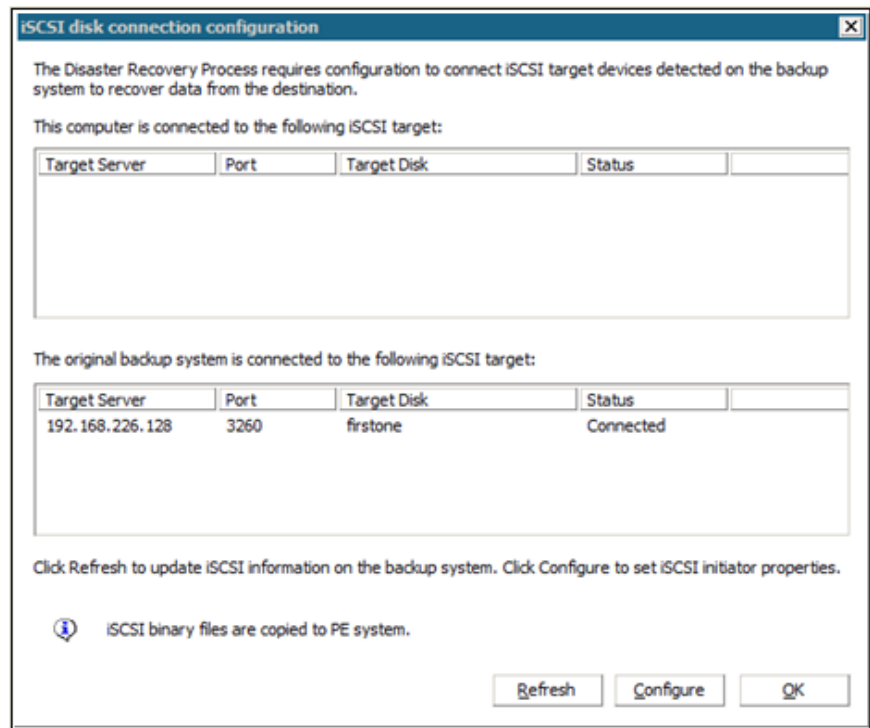
Click Configure to open the iSCSI Initiator Properties screen.
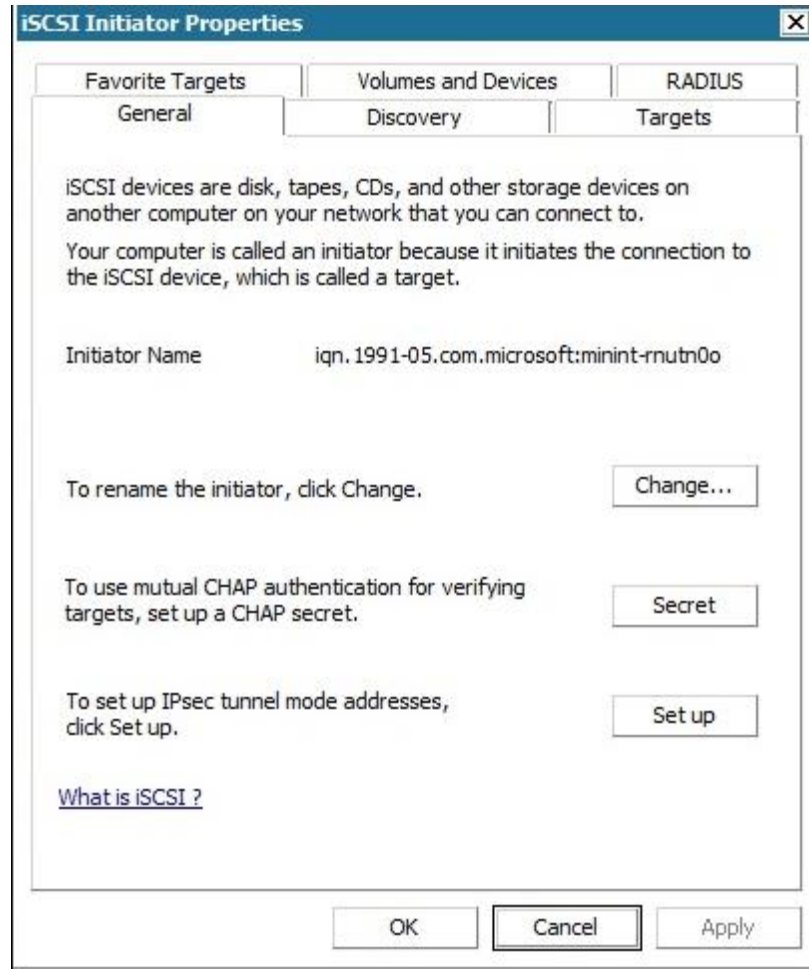
Note: The iSCSI configuration and related binaries are saved as part of the disaster recovery information in which disaster recovery restores them by default. If disaster recovery fails to detect iSCSI binaries, then you will have to select a path that contains iSCSI binaries and copy them to the WinPE environment.

■ **ASDB Recovery Configuration**

If you are recovering a primary or standalone server with Arcserve Backup Database locally installed, then the below ASDB Recovery Configuration screen opens and lets you recover your sessions automatically. You will need to enter your Arcserve Backup Database credentials.
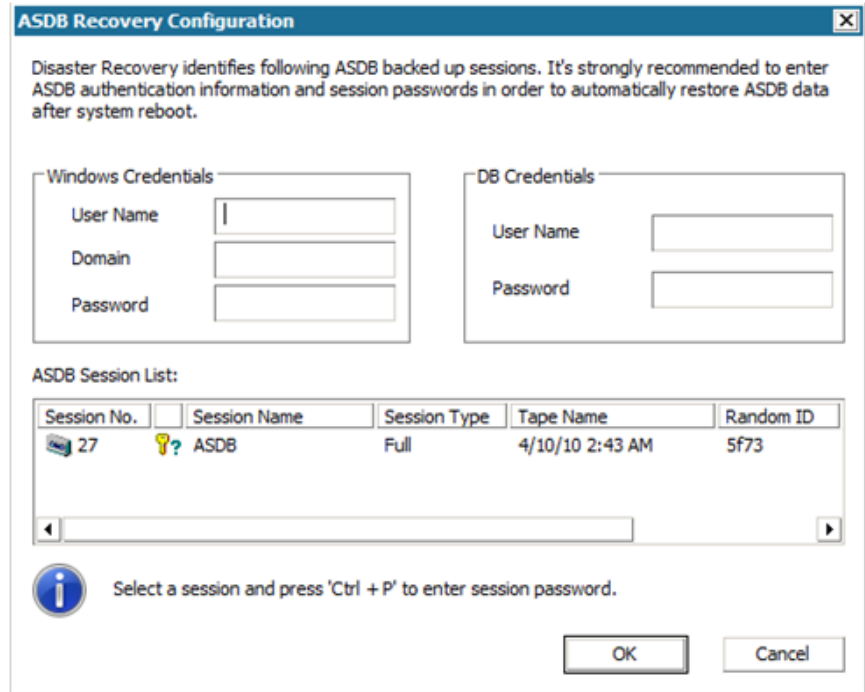
The following icons appear next to each Arcserve Backup Database session. They are as follows:

– ⚷ Indicates that the session was encrypted. You must provide a password to restore the session.

– ⚷? Indicates that Disaster Recovery cannot verify whether the session was encrypted or not. You may or may not need to provide a password to restore the session.

– ⚷✓ Indicates that the session was encrypted and was provided with a password. You do not need to provide a password to restore the session.

■ **ACSLS Configuration**

If ACSLS (StorageTek Automated Cartridge System Library Software) was configured during backup time, all related ACSLS configurations and binaries are saved as part of the Disaster Recovery information. Disaster Recovery restores the ACSLS configuration information automatically.

Be aware of the following:

– If Disaster Recovery fails to detect ACSLS binaries, you must specify a directory path that contains ACSLS binaries.

– WinPE does not support WOW (Windows on Windows), therefore WinPE does not support 64-bit ACSLS.

■ **Cluster Configuration**

Cluster Configuration display if the backup server is a cluster node. If it is a cluster node, WinPE searches for an available cluster virtual node. If the cluster virtual node is available, WinPE DR omits the restore process of the cluster shared disk; otherwise Disaster Recovery will restore the cluster shared disk.

■ **USB Backup Device Configuration**

The USB Backup Device Configuration is used during backup time where you configure backup devices (for example, tape drives, Iomega changers, and digital storage drives. For some USB backup devices, you may need to install additional drivers.

■ **Client Agent Service**

The Client Agent Service is a critical service used to communicate with backup servers for data recovery. Disaster Recovery will always start this service if the disaster recovery is local. If disaster recovery is remote, you can maintain the connection by clicking the link "Click Here" in the bottom pane of the screen to restart the Client Agent Service.

■ **Tape Engine Service**

The Tape Engine Service is used only for local Disaster Recovery (DR).

Note: If a file system device (FSD) or data deduplication device (DDD) was used during backup time, Disaster Recovery checks for available remote FSDs or DDDs during the start of the Tape Engine Service. If there are remote FSDs or DDDs, you can maintain the connection by clicking the link "Click Here" in the bottom pane of the screen to restart the Tape Engine Service. If FSDs or DDDs are not available, you can configure an FSD or DDD in the Device Authentication screen.

5. Click Next to restore the disk partitions and open the Restore Disk Partition screen.
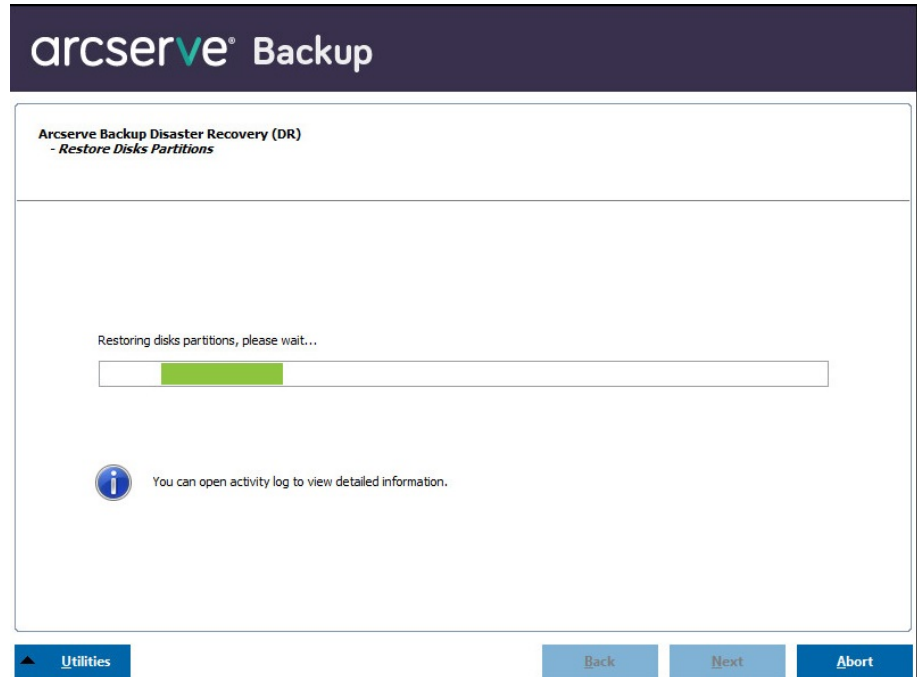
Arcserve Backup Disaster Recovery automatically restores your disk partitions according to the saved disk layout information.

6. When the disk partitions are restored, click Next to restore Arcserve Backup Disaster Recovery sessions and open the Select sessions to restore screen.
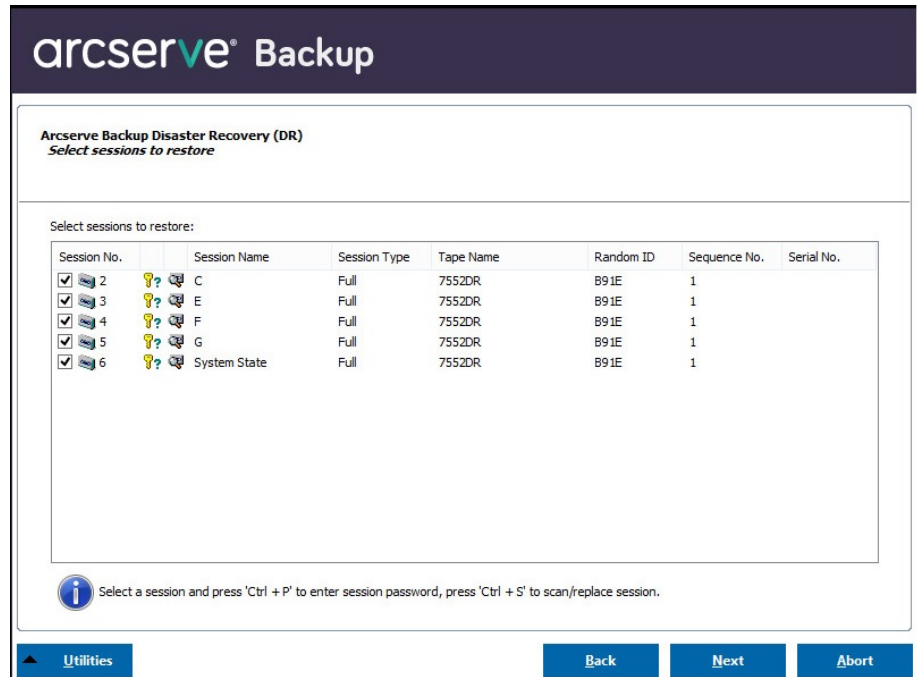
Arcserve Backup Disaster Recovery lets you specify sessions allocated to each drive, in hard disk, and also helps assign a session password. You can also recover incremental/differential backup sessions simultaneously.

Based on the session encryption status, you will find four types of icons in the Select sessions to restore screen:

– Indicates that the session was encrypted. You must provide a password to restore the session.

– Indicates that Disaster Recovery cannot verify whether the session was encrypted or not. You may or may not need to provide a password to restore the session.

– Indicates that the session was encrypted and was provided with a password. You do not need to provide a password to restore the session.

– Lets you scan or replace an existing session. Click this icon or press Ctrl+S to open the Scan and Replace Session screen.

Note: This dialog opens for full sessions only.
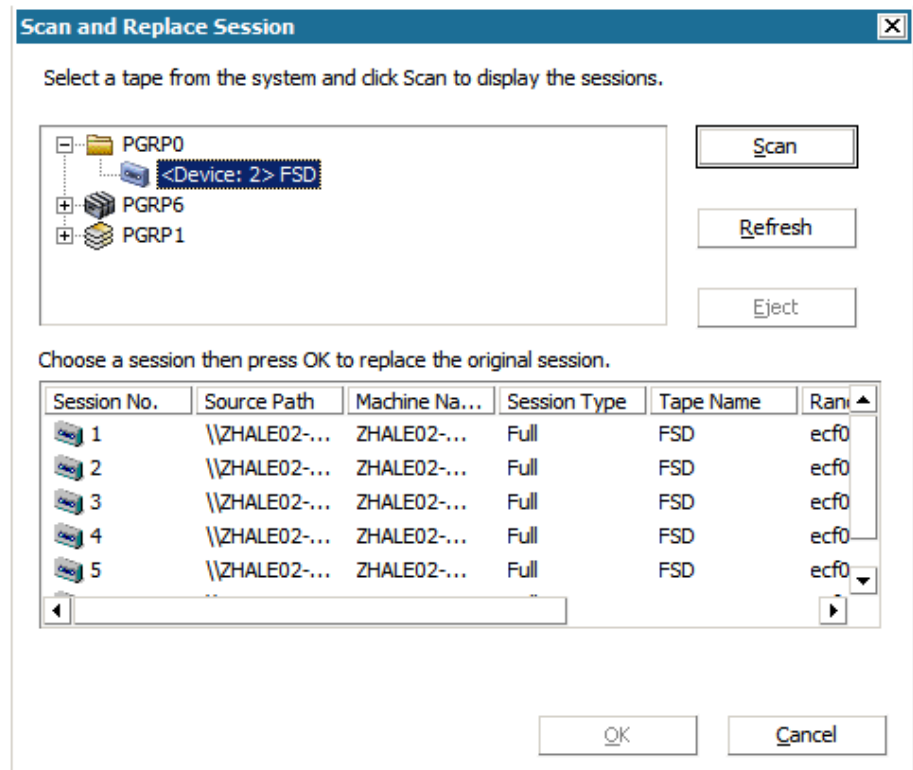
Note: The Eject button is used only for removable disk drives, like an RDX drive but some removable disk drives cannot be ejected in Disaster Recovery mode where you will have to switch media.

Important! You must restore volume C and System State sessions under the Session Name column, otherwise disaster recovery fails.

7. Click Next to open the Summary of Session Restore screens.

Note: This screen confirms the sessions you selected.
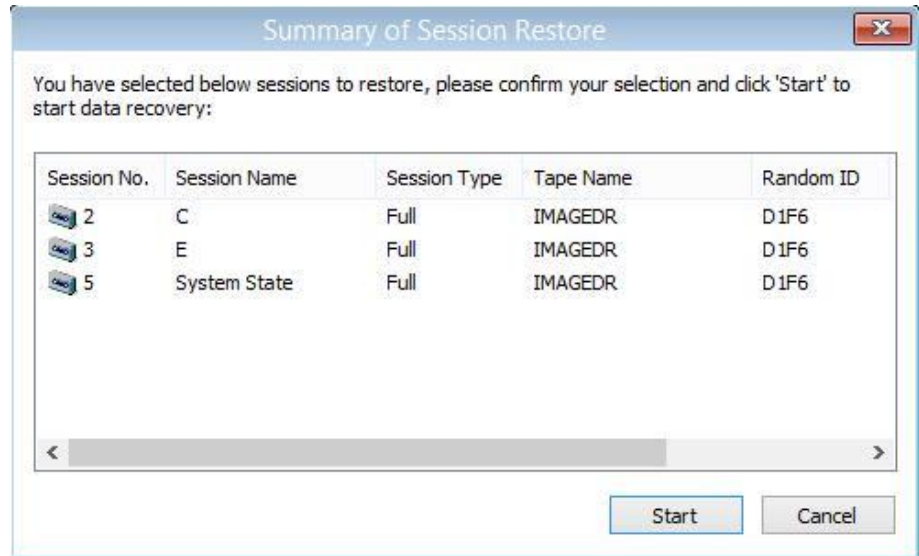
8. Click Start to start the data restore process and open the Start Restore Process screen.

This screen displays a progress bar on the estimated time remaining of the data recovery.

Note: During data recovery, if your session password was not set, you will need to provide the password. Arcserve Backup allows three attempts to enter your password. After three attempts, the session will fail to restore.

9. Click Next to reboot the computer and open the Prepare to Reboot screen.

   Note: This screen automatically reboots in 30 seconds or gives you 30 seconds to cancel if the option on the Start Restore Process screen: Automatically reboot after all sessions restored successfully, is selected. If the option is not selected, Arcserve Backup Disaster Recovery lets you reboot or cancel manually.
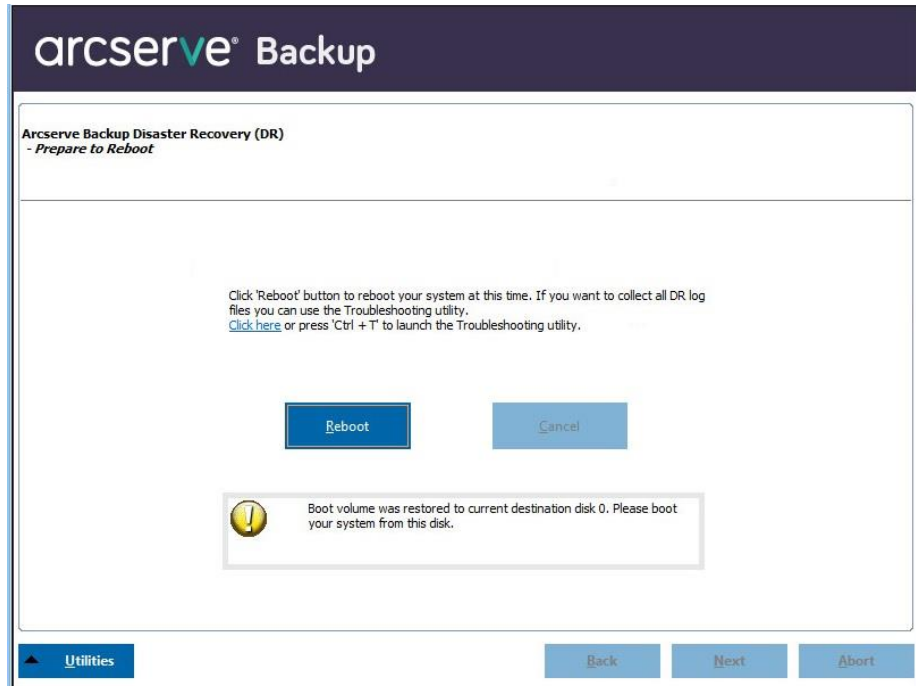
After the computer restarts, Arcserve Backup Database Recovery Wizard opens to help you restore Arcserve Backup Database sessions.

Be aware of the following:

■ Arcserve Backup Database recovery wizard only appears when you are restoring a Primary or Standalone backup server with Arcserve Backup Database installed locally. The recovery wizard automatically restores your sessions based on the information you entered on the Pre-flight Check screen.

■ If you did not enter any Arcserve Backup Database credentials or what you entered is incorrect in the ASDB Recovery Configuration screen, you need to follow the prompts and complete the required fields on the Arcserve Backup Database Recovery Wizard screens to complete the recovery.

How to use Arcserve Backup Disaster Recovery Utilities

Arcserve Backup contains various Disaster Recovery utilities that you can use to resolve issues you encounter during the Disaster Recovery process. You can find the Utilities button on the bottom of each Arcserve Backup Disaster Recovery screen.

The Disaster Recovery utilities are as follows:

- Load Driver Utility--Lets you load NIC/SCSI/FC drivers. For example, if the network driver is unavailable or your hard disks and cannot be detected, you can use this utility to load the drivers for you.

  In the Load Driver Utility screen, a list of Unknown Devices displays. You can select a device and click Install Driver. This will let you search for the best driver to load or specify a driver for the particular device.
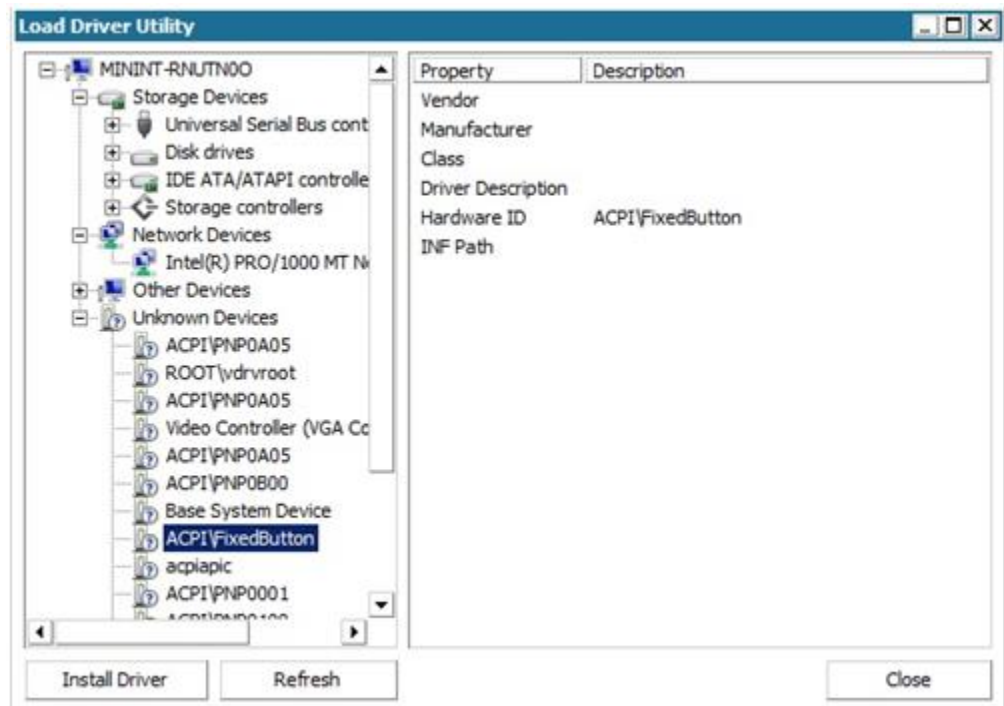
- Network Configuration Utility--Lets you configure IP addresses.

- iSCSI Configuration Utility--Lets you check and configure iSCSI connections for disaster recovery on your current environment.

  From the iSCSI disk connection configuration screen, you can configure the current system to connect to your iSCSI target remotely. In this screen, the Current system connected iSCSI target section displays iSCSI connections during disaster recovery time.
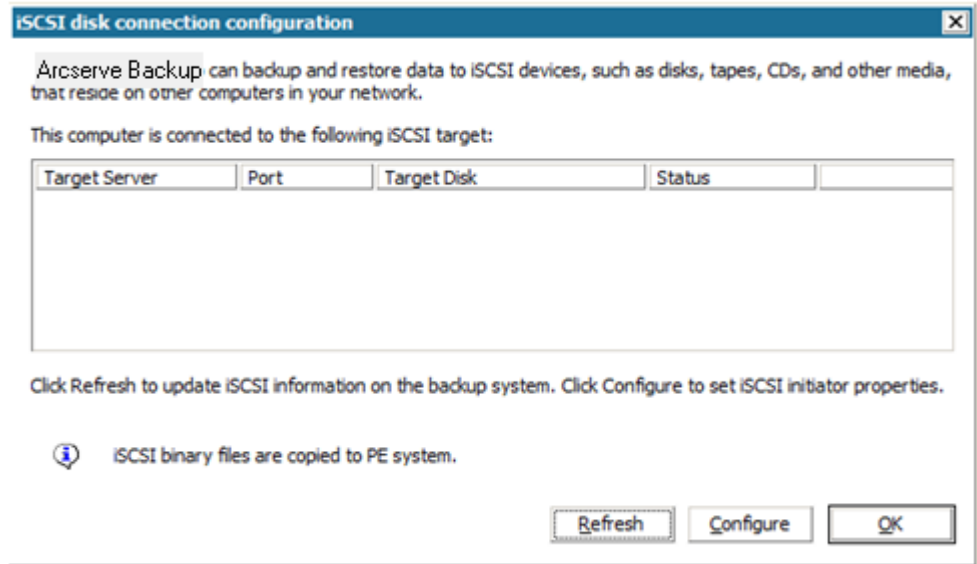
Click Configure to open the iSCSI Initiator Properties screen.
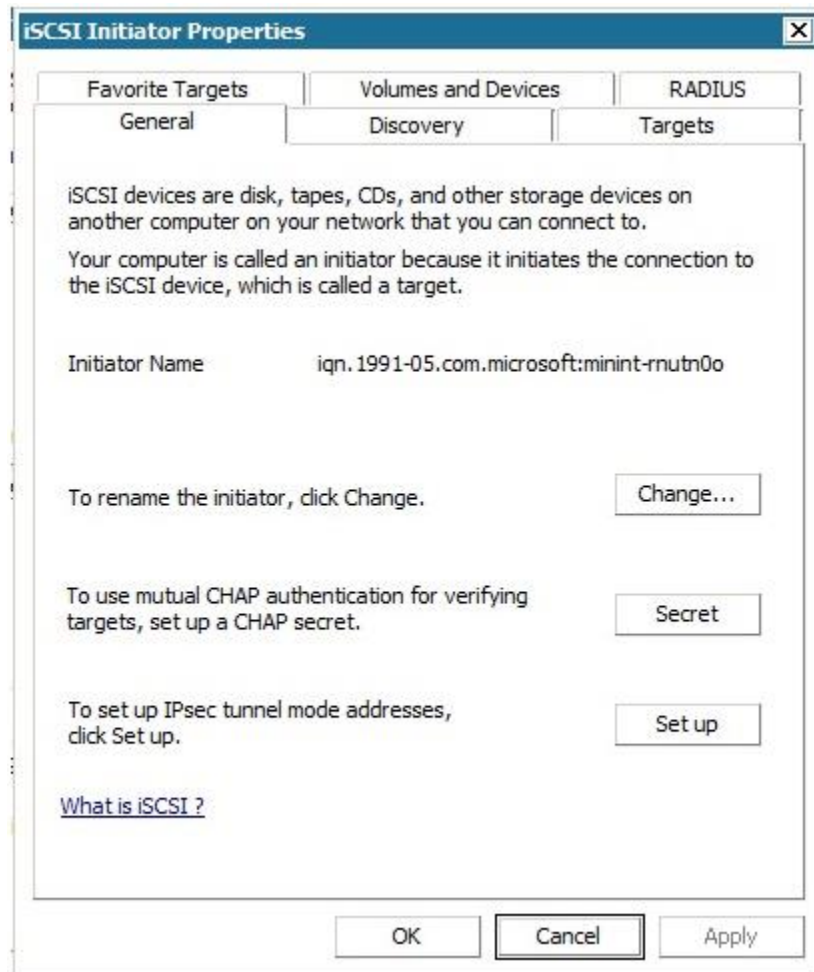
- Activity Log--Lets you view all Disaster Recovery activities.

- Troubleshooting Utility--Lets Arcserve Support investigate issues that you encounter during the Disaster Recovery processes (for example, How to set log levels, How to collect log files).

- Run Utility--Lets you run other applications on the Disaster Recovery environment. A dialog box opens for you to enter the name of a program you would like to launch.

Create Customized WinPE Disaster Recovery Images

Arcserve Backup lets you create customized WinPE Disaster Recovery (DR) images using the Boot Kit Wizard utility. The utility integrates NIC, FC, SCSI, RAID drivers, iSCSI programs, and Disaster Recovery patches into the created ISO image.

Be aware of the following:

- To complete this task, Windows ADK must be installed on the backup server.

- When you perform disaster recovery of a guest operating system that resides on a Hyper-V server, create the WinPE disaster recovery image using Windows Automated Installation Kit (WAIK) for Windows 7.

Follow these steps:

1. From the Quick Start menu on the Home Page, select Utilities and click Create Boot Kit to open the Create Boot Kit Wizard.

   Note: You can also select Create Boot Kit from the Arcserve Backup installation media, the Utilities menu on the home page or the Navigation Bar, and from the Start menu.

2. Confirm the appropriate server and domain details. Enter the domain user name, password, and click Next to open the Select disaster recovery boot kit type screen.

3. Select Customize PEDR image and click Next to open the Select disaster recovery image platform and location screen.

4. Select the platform and location where you want to store the WinPE DR image.

   There are two platforms available:

   – WinPE DR Image for x86 Platform

   – WinPE DR Image for x64 Platform

   Important! You must select the platform that corresponds to the platform that is running on the source machine that you are recovering. For example, if you are recovering a computer that is running an x64-based operating system, you must select a WinPE DR Image for an x64 platform.

   Click Next to open the Select Arcserve Backup installation source path screen.

5. Specify the path for the Arcserve Backup installation source.

   To create a customized WinPE Disaster Recovery image, you must copy the Disaster Recovery programs from the Arcserve Backup Installation DVD.

   a. Insert the Arcserve Backup Installation DVD into the CD/DVD ROM to copy Disaster Recovery programs.

      Select the drive where the installation DVD is mounted from the drop-down list and click Next to open the Select disaster recovery options screen.

b. Select one of the following drivers and updates to recover your Windows system:

■ **Integrate NIC/SCSI/FC/RAID drivers:** With this option, you do not have to install the drivers again manually during the Disaster Recovery process.

Click Next to open the Specify the drivers to be integrated into the PE image screen.

Note: By default, a list of available drivers from the existing Disaster Recovery information displays. To add other drivers from another location, click Add Driver

■ **Integrate Microsoft iSCSI initiator:** With this option, you do not have to install the iSCSI configuration tool manually during the Disaster Recovery process.

Note: As a best practice, you should specify this option if you backed up data using iSCSI disks.

Click Next to open the Specify Microsoft iSCSI Initiator binary files screen.

Note: The Boot Kit Wizard utility detects iSCSI programs on your current system. When they are detected, the Specify Microsoft iSCSI Initiator binary files screen will not open and you will be directed to confirm your settings. However, when the wizard does not detect the iSCSI programs, you must specify the location where the iSCSI programs are installed.

Click Next.

A message appears to confirm your settings.

6. Click OK to create the customized WinPE DR image.

7. Click Finish to exit the Boot Kit Wizard.

Chapter 4: Disaster Recovery on Windows XP, Windows Server 2003, Windows Server 2008 and Windows 7

The following sections describe how you can prepare for a disaster and recover from a disaster on Windows XP, Windows Server 2003, Windows Server 2008, and Windows 7 using Arcserve Backup disaster recovery procedures.

This section contains the following topics:

Disaster Recovery Methods on Windows Server 2003 and Windows XP

Disaster Recovery on Windows Server 2003 supports both the Bootable CD method and Bootable Tape method also known as One Button Disaster Recovery (OBDR) and Windows XP supports the Bootable CD method. The Bootable CD method supports the protected client computer and the backup server. The Bootable Tape method can be used to protect only the backup server. Both methods are built on the Windows ASR framework.

Bootable CD Method for Windows XP and Windows Server 2003

This section describes how you can use the Bootable CD method to protect local and remote Windows Server 2003 computers and recover from disaster. The Windows XP and Windows Server 2003 Bootable CD method uses a single disk containing configuration information for the specific computer you want to recover, the Windows XP or Windows Server 2003 CD, and the Arcserve Backup CD/DVD.

Note: Windows XP does not support local disaster recovery using the Bootable CD method.

Machine Specific Disks

Verify that you have performed the following tasks before you proceed:

- Install Arcserve Backup Server and the option locally or on another server in preparation for remote disaster recovery.

- Install the agent on the client computer, for remote disaster recovery.

- Perform a full backup of the computer for which you want to create a machine-specific recovery disk.

- Label a formatted, floppy disk as Arcserve Backup Machine Specific Disk.

Note: The Machine Specific Disk (MSD) is also called the Machine Specific Recovery Disk.

Create Machine Specific Disks for Disaster Recovery

The machine specific disk is the recovery disk used with the Windows XP or Windows Server 2003 installation media and the Arcserve Backup CD to perform disaster recovery using the Bootable CD method.

To create a machine specific disk

1. Insert the disk labeled Arcserve Backup machine specific disk into the server's disk drive.

2. From the Quick Start menu in the Home Page, select Utilities and then click Create Boot Kit Wizard.

    The Create Boot Kit Wizard dialog opens.

3. Confirm the appropriate server and domain details. Enter the domain user name and password, and then click Next.

   The Select Client Server screen opens. In this pane, the Create Boot Disk Wizard displays a list of computers that have been backed up by Arcserve Backup. The panel appears blank if Arcserve Backup has not backed up a computer.
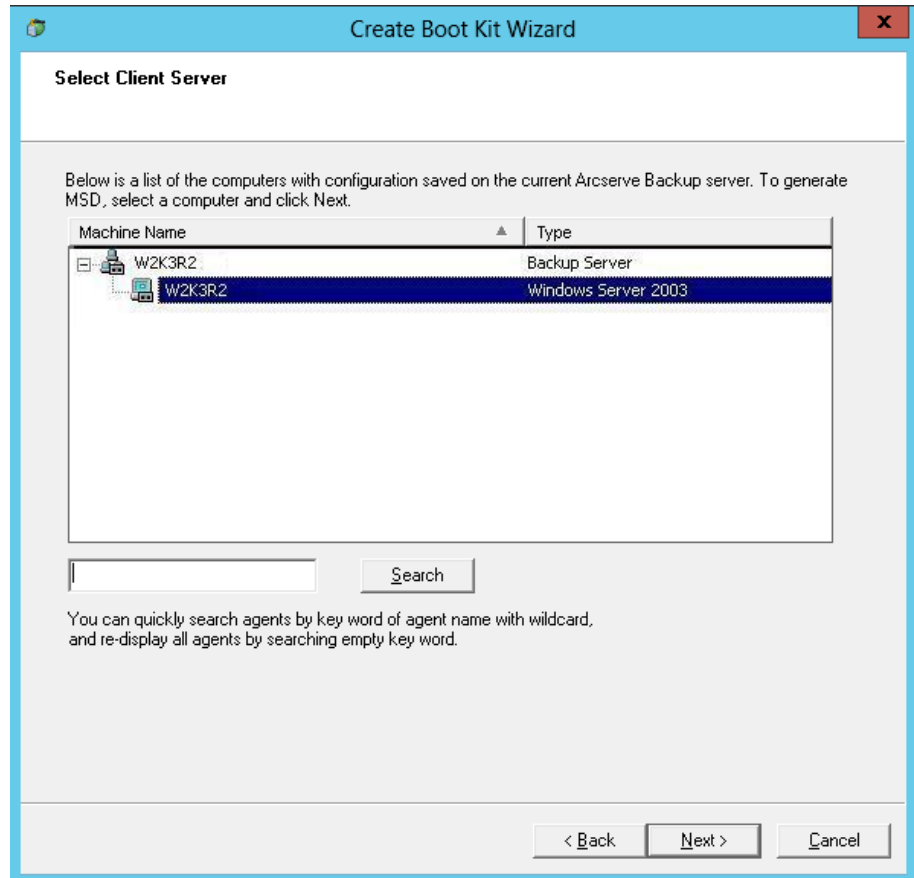
4. Choose the appropriate computer and click Next.

5. Select Machine Specific Disk, and then click Next.
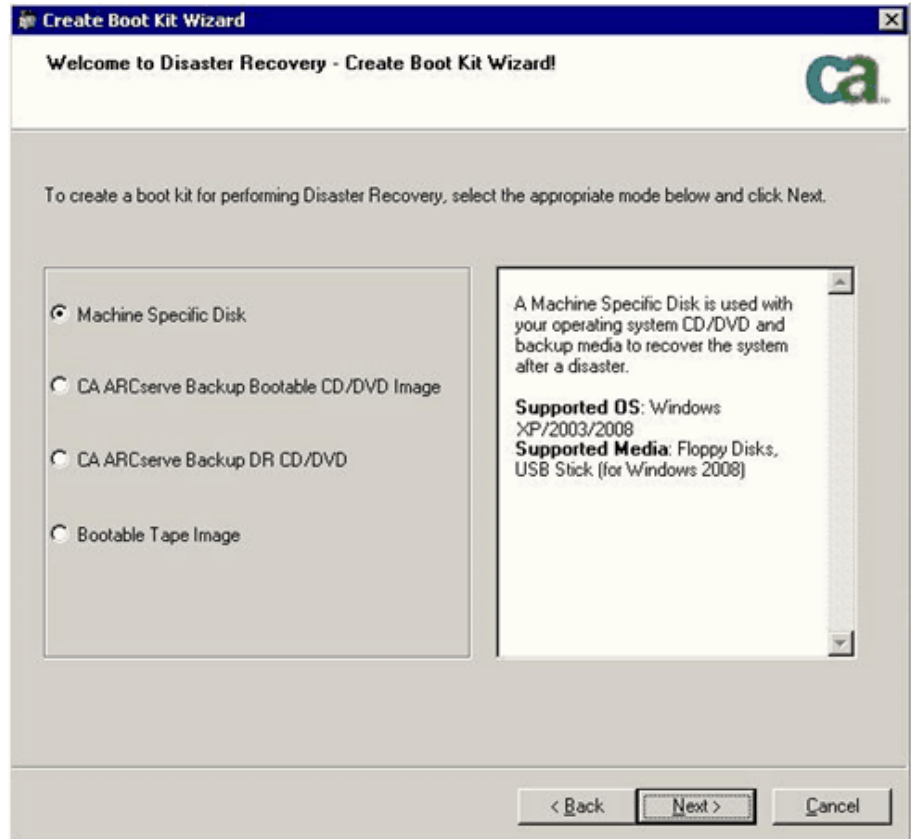
The Summary of Backup Information dialog opens.

6. Verify the available list of sessions that must be recovered, and then click Next.
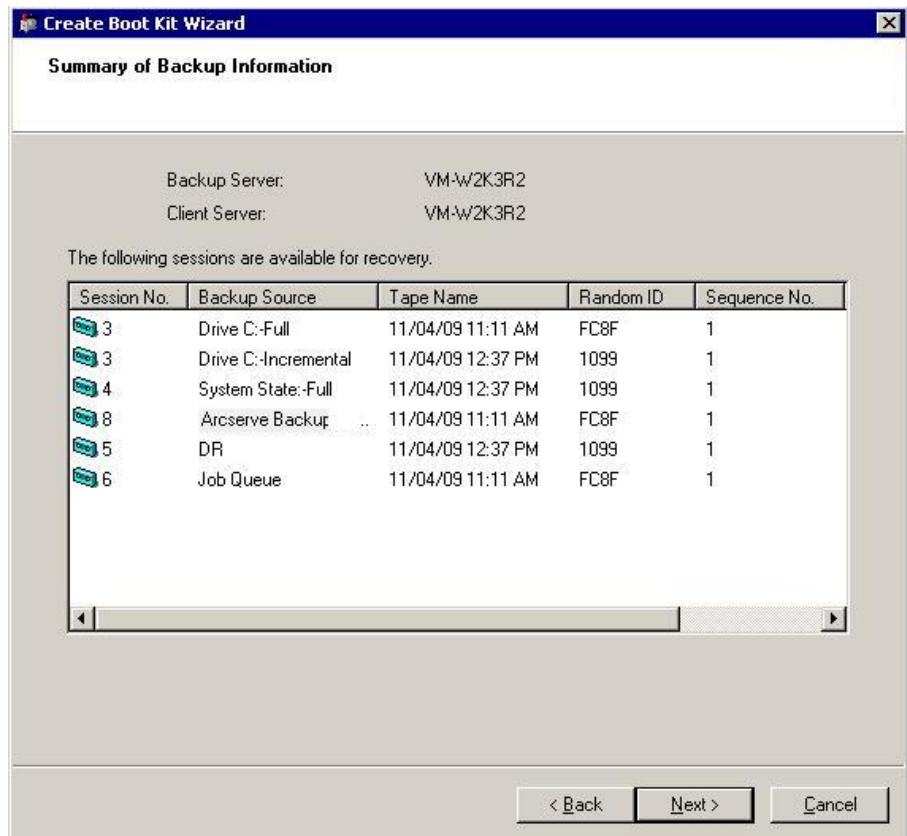
7. Insert a blank floppy disk.

    The Create Boot Floppy Disk dialog opens.
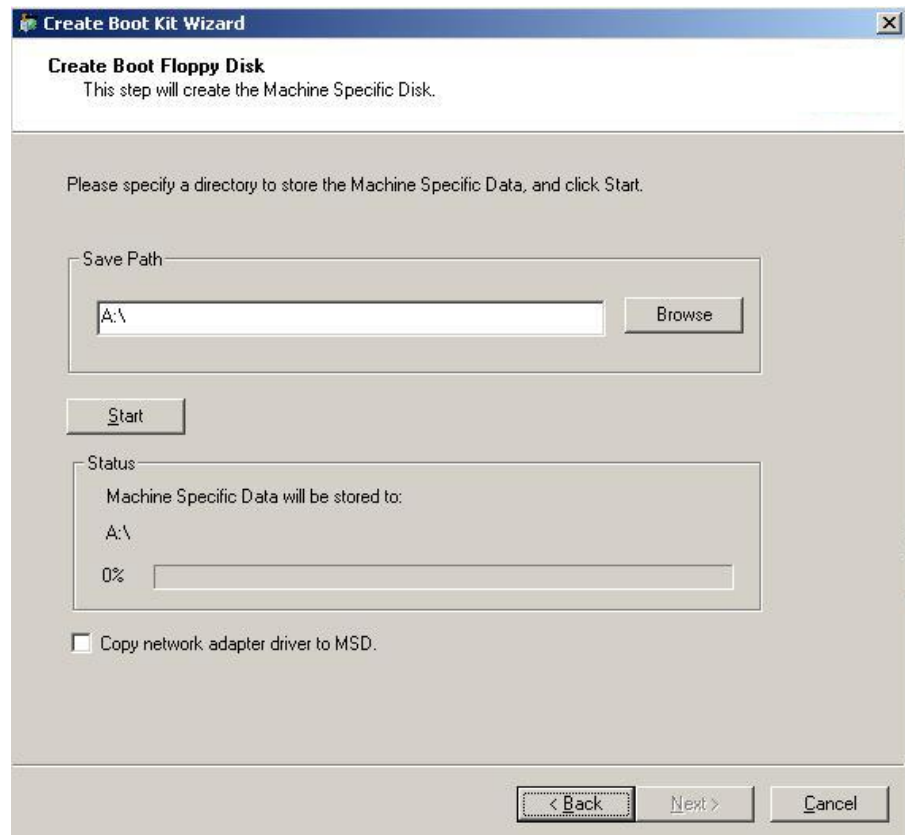
8. If you are performing disaster recovery in the following environments, enable Copy Network Adapter driver to MSD:

    ■   Disaster recovery of a remote computer

    ■   Disaster recovery using remote FSD

    ■   Disaster recovery of member servers in a SAN environment

9. Click Start.

    The files are copied to your machine-specific recovery disk.
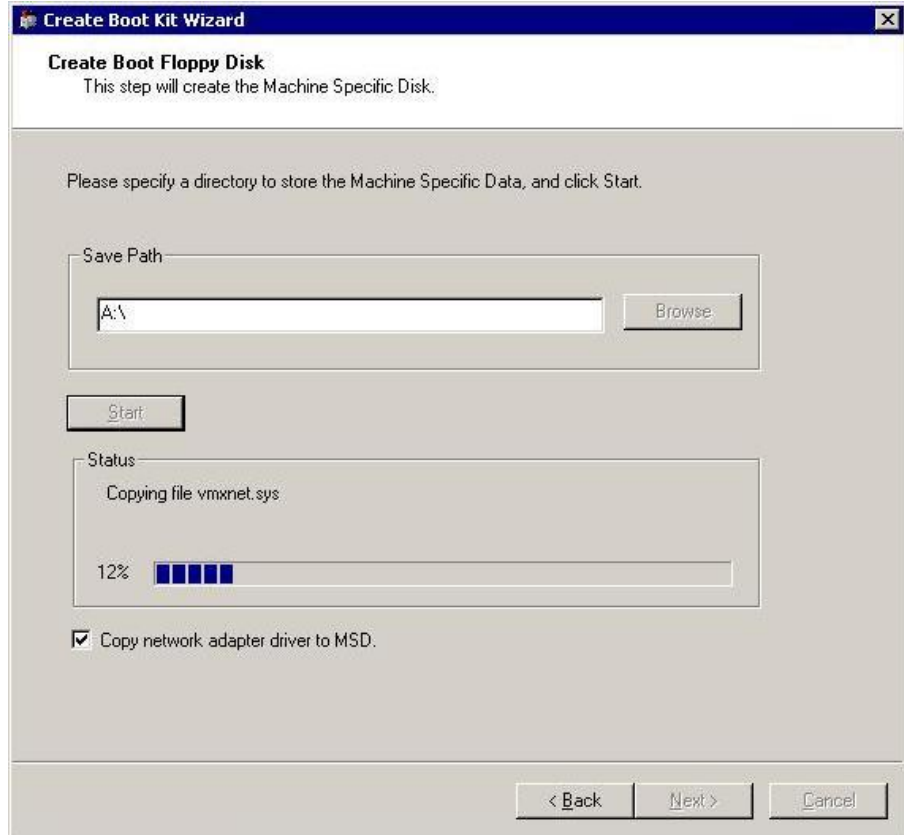
10. Click Next, and then click Finish.

    The newly created disk is a Arcserve Backup machine-specific disaster recovery disk. It is also the Windows ASR disk during the first phase of disaster recovery in ASR mode. You can use this disk to recover the local or remote computer in the event of a disaster.
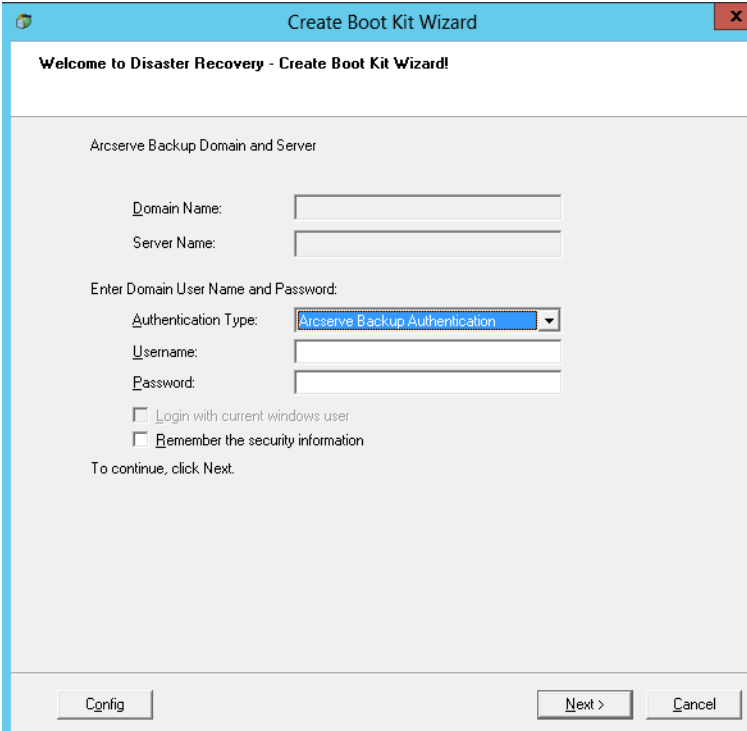
Reimage Bootable CD Using Boot Kit Wizard

You can integrate the machine specific disks, Arcserve Backup Disaster Recovery applications with Windows operating system and drivers such as the network adapters and SCSI into a single bootable media image. You can avoid using CDs and floppy disks. Reimaging CD is also known as remastering CD. You can reimage CD in Windows XP and Windows Server 2003 using the following process:

To reimage Bootable CD using the Boot Kit Wizard

1. From the Quick Start menu in the Home Page, select Utilities and then click Create Boot Kit Wizard.

    The Create Boot Kit Wizard dialog opens.

2. Enter the domain user name and password after confirming the domain name and server name.

Disaster Recovery Methods on Windows Server 2003 and Windows XP

3. Click Next.

   The Select Client Server dialog opens. The dialog has the list computers and their configurations saved on the Arcserve Backup server. This pane is empty when the Arcserve server does not back up a computer.

4. Select the computer name and click Next.

   Create Boot Kit Wizard with options opens.

5. Select the Arcserve Backup Bootable CD/DVD Image option and click Next.
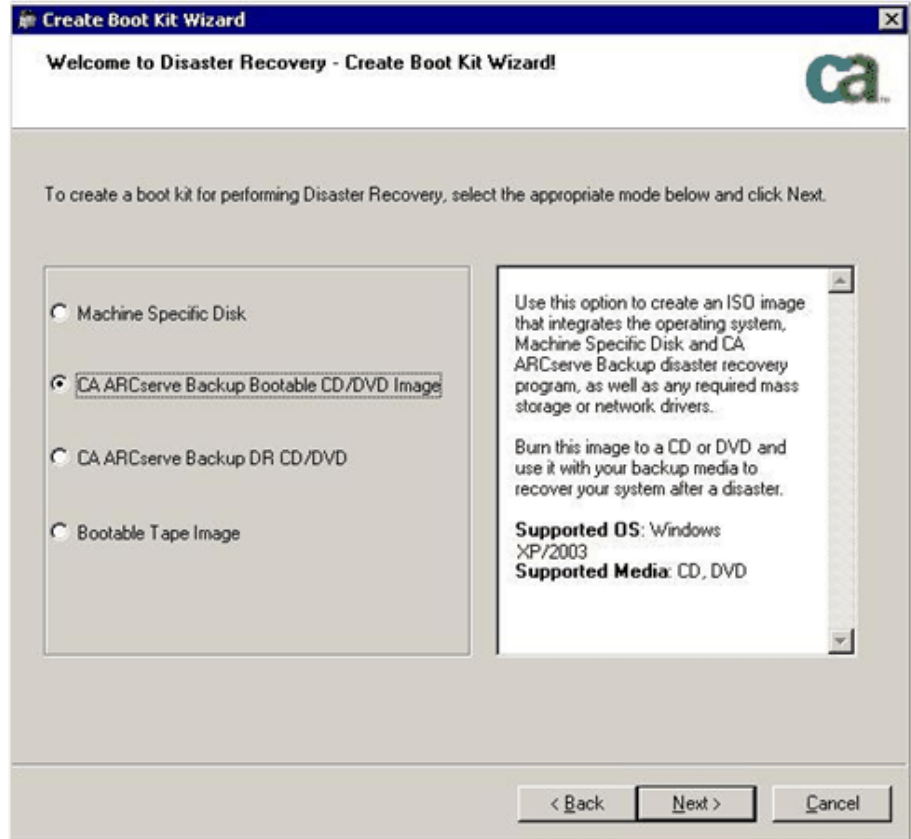
The license agreement dialog opens.

6. Click Next.

7. Specify the location for creating the Image, and click Next.

The Customize Bootable CD/DVD Image dialog opens.
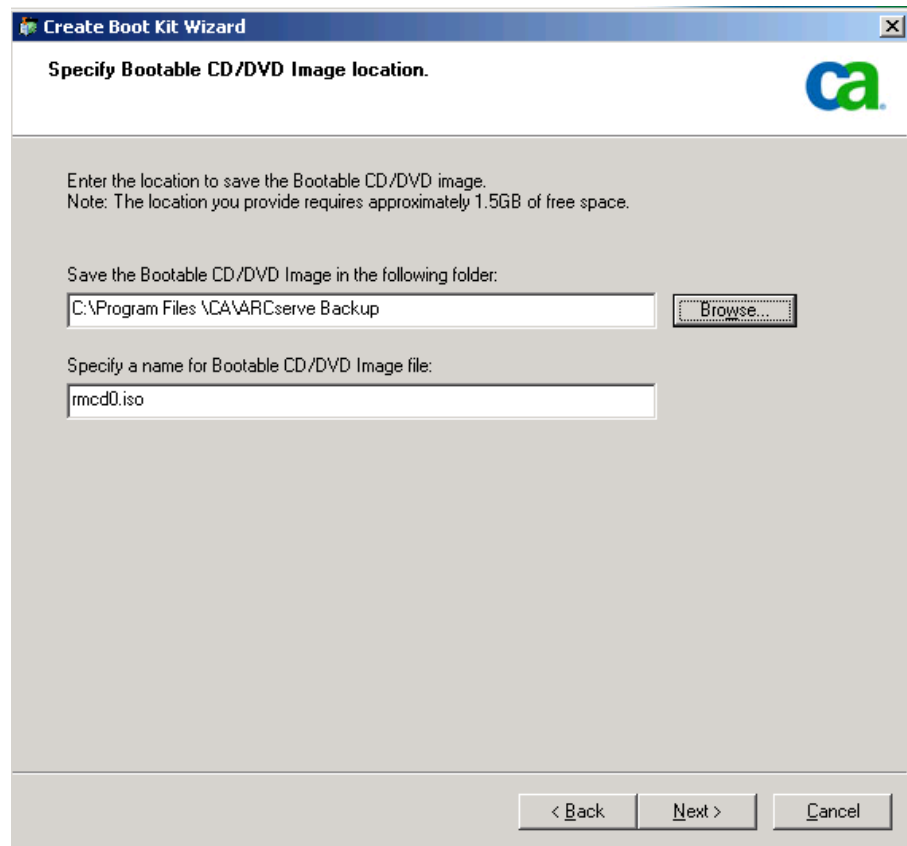
8. Select the necessary options, and click Next.

Customize Bootable CD Image dialog appears.
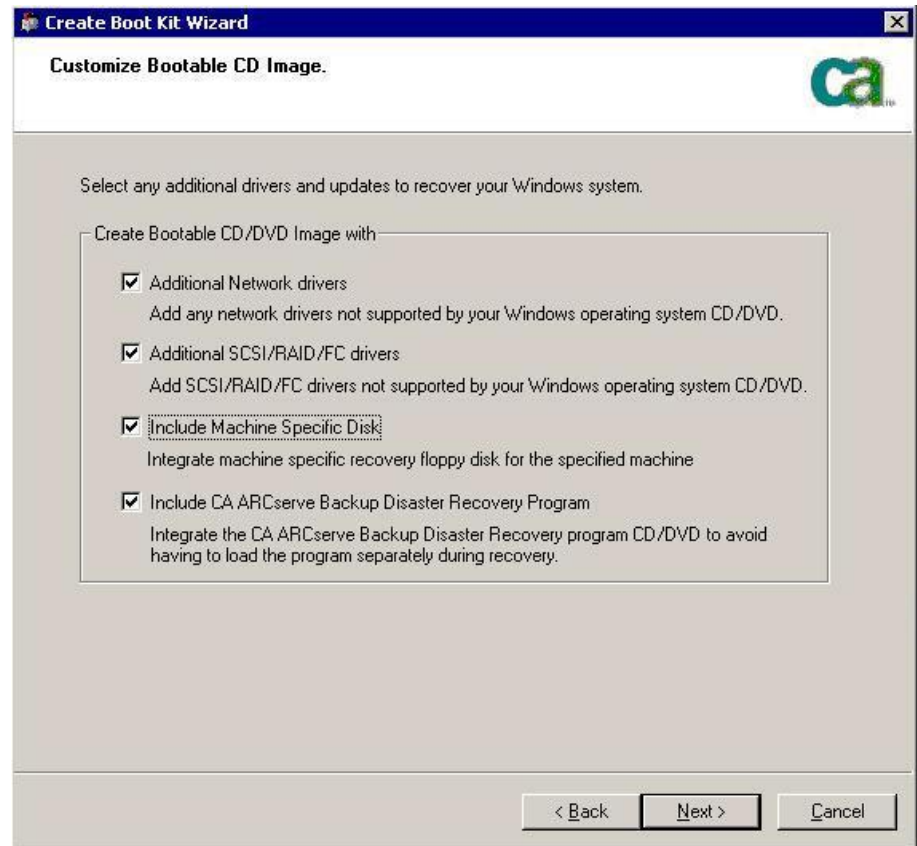
Select the necessary drivers and updates to create the image. The additional driver options include:

■ **Additional Network drivers**: You can select network drivers and integrate them into the re-imaged CD. The integrated network drivers will then be automatically installed during the disaster recovery process.

■ **Additional SCSI/RAID/FC drivers**: You can select the SCSI/RAID/FC drivers and integrate them into the re-imaged CD. The integrated drivers will be automatically installed during disaster recovery.

■ **Include Machine Specific Disk**: When you select this option the disaster recovery emergency data will be automatically integrated into the re-imaged CD. During disaster recovery. The machine specific disk need not be inserted.

■ **Include Arcserve Backup Disaster Recovery Program**: The disaster recovery programs will be automatically integrated into the re-imaged CD and you need not insert the Arcserve Installation DVD during the recovery process.

When creating Windows XP (64-bit) and Windows Server 2003 integrated CD, as the 64-bit client agent has to copy from the Arcserve Backup installation media, you must select the Machine Specific Disk, device drivers, the Arcserve Backup Disaster Recovery Integrated option, and the client computer and then integrate. The integrated MSD option is disabled in Windows XP (32-bit).

Note: While creating the 64-bit Windows Bootable CD, if you select Arcserve Backup Disaster Recovery Integrated option, you will be prompted to insert Arcserve Backup installation media or specify the path to install media. However, if you are using the 32-bit bootable CD this screen does not appear.

9. Click Next to specify the path of the <Win> installation media source files in the dialog that appears.
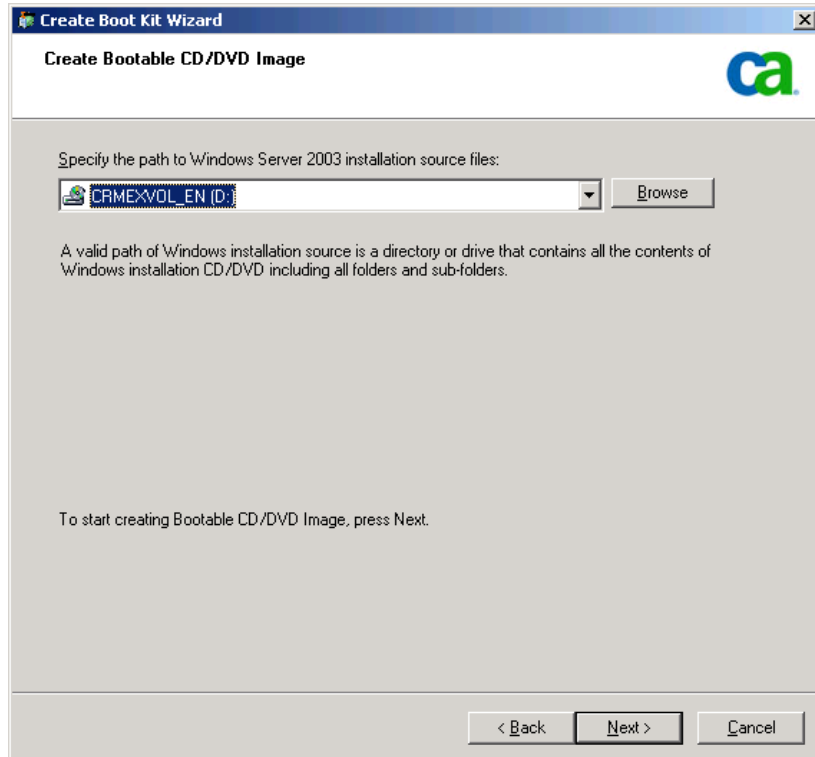
10. Click Next.

   The Summary dialog opens.
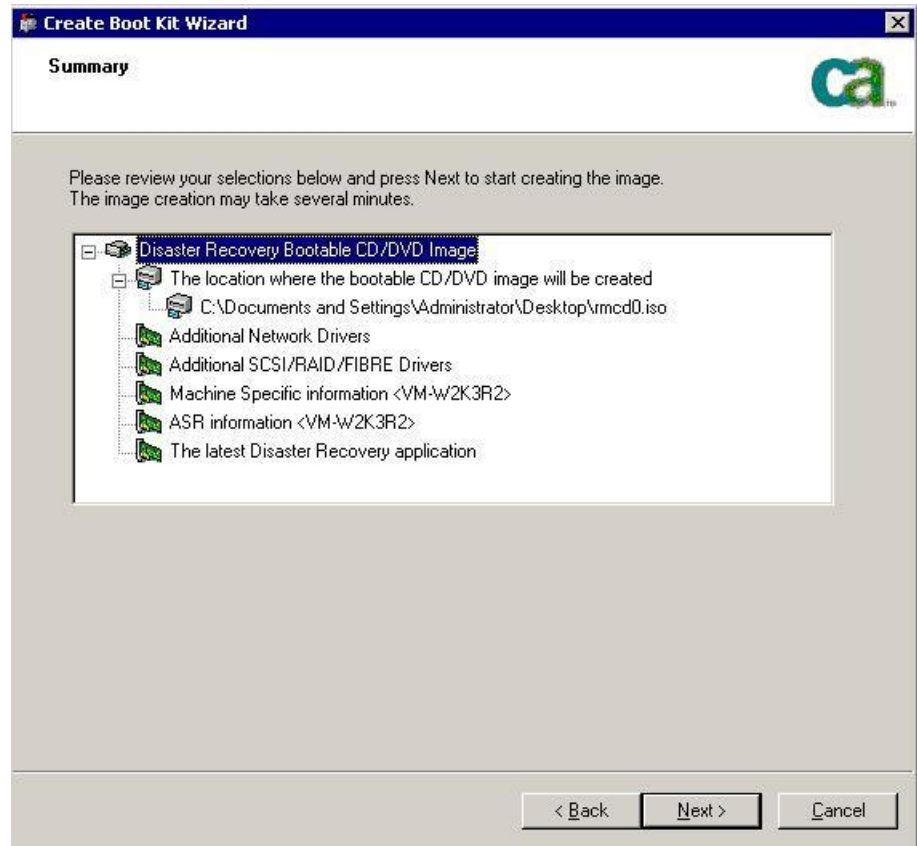
11. Click Next to start the bootable CD/DVD imaging process.

   Note: If the remastering is for a 64-bit operating system, provide the Arcserve Backup installation media to copy the client agent files.

   When the reimaging process completes, you can burn the ISO image to a bootable media.
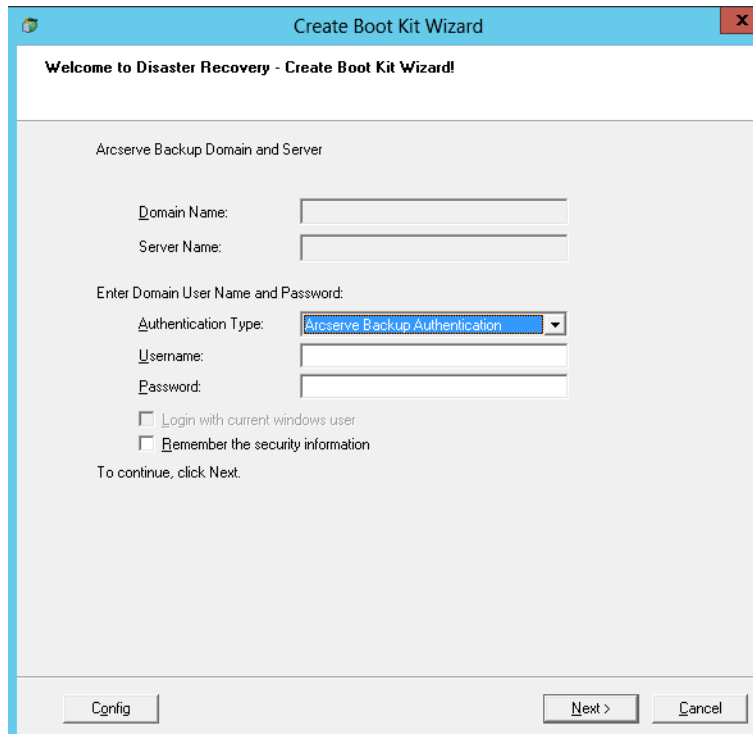
Create Arcserve Backup Disaster Recovery CD/DVD

You can create Arcserve Backup disaster recovery media using the Disaster Recovery wizard. This option lets you integrate the disaster recovery applications into a CD/DVD, especially after you apply any patches to Arcserve Backup.

To create the disaster recovery CD/DVD using the Create Boot Kit Wizard

1. From the Quick Start menu in the Home Page, select Utilities and then click Create Boot Kit Wizard.

    The Create Boot Kit Wizard dialog opens.

2. Enter the domain user name and password after confirming the domain and server name.

3. Click Next.

    The Select Client Server dialog opens. The dialog has the list computers and their configurations saved on the Arcserve Backup server. This pane is empty when the ARCserve server does not back up a computer.
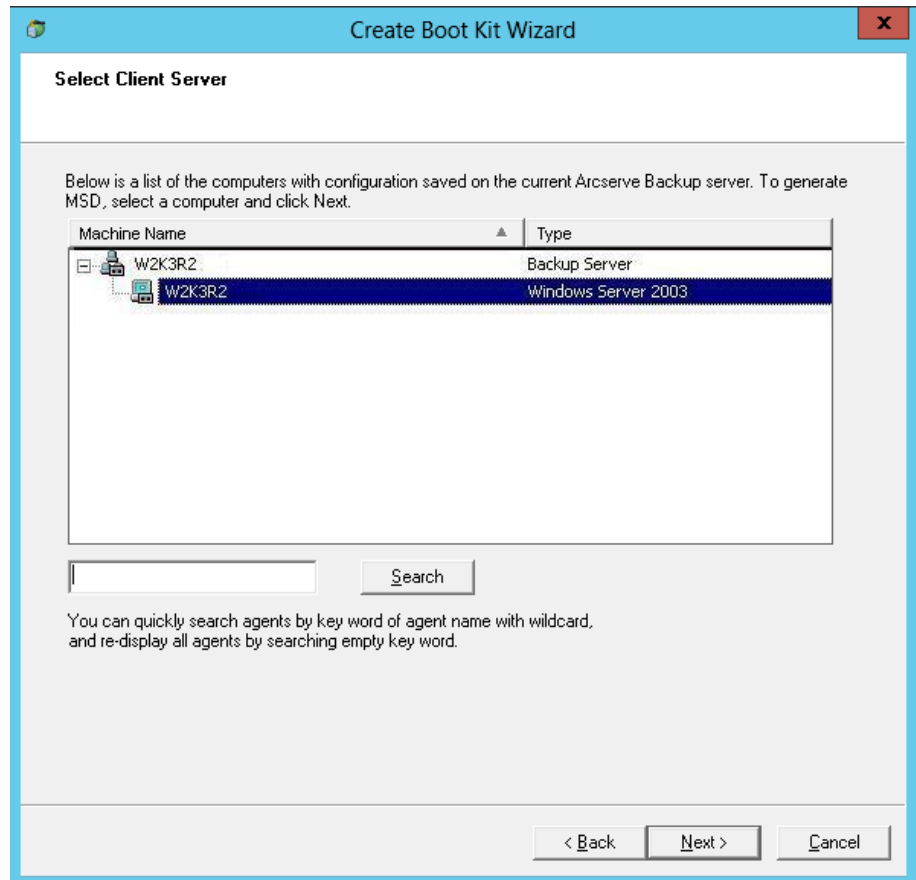
4. Select the computer name and click Next.

   Create Boot Kit Wizard with options opens.
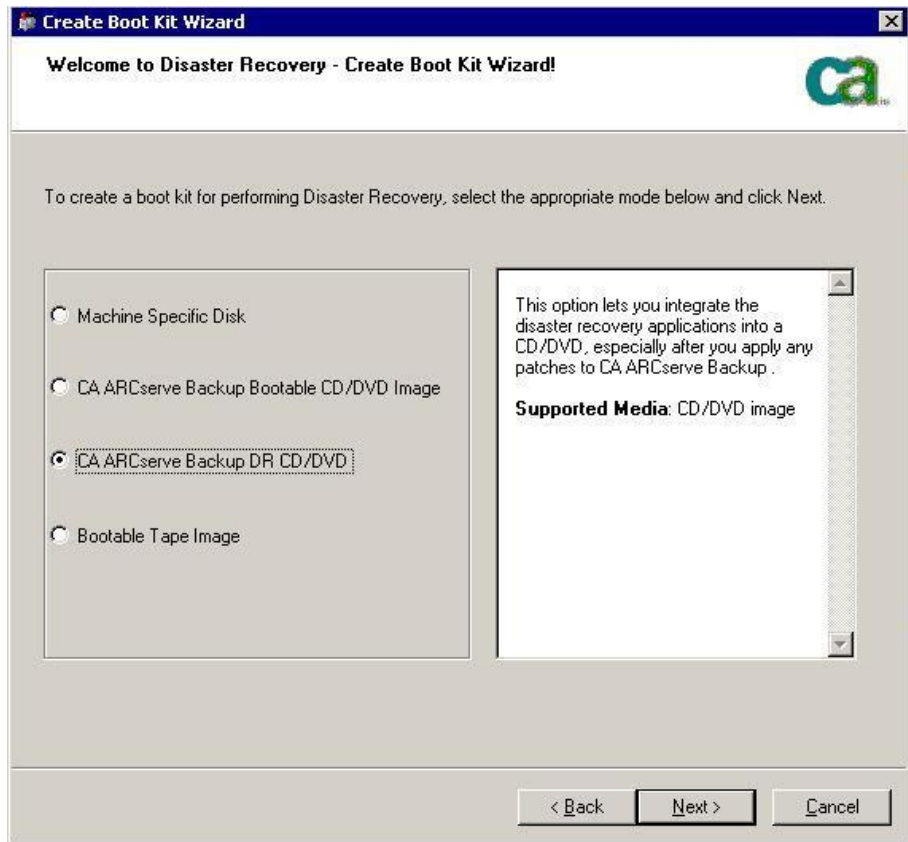
5. Select the Arcserve Backup DR CD/DVD option, and click Next.

   The Specify ARCserve DR Image location dialog opens.

6. Specify the location for creating the DR CD/DVD image and click Next.
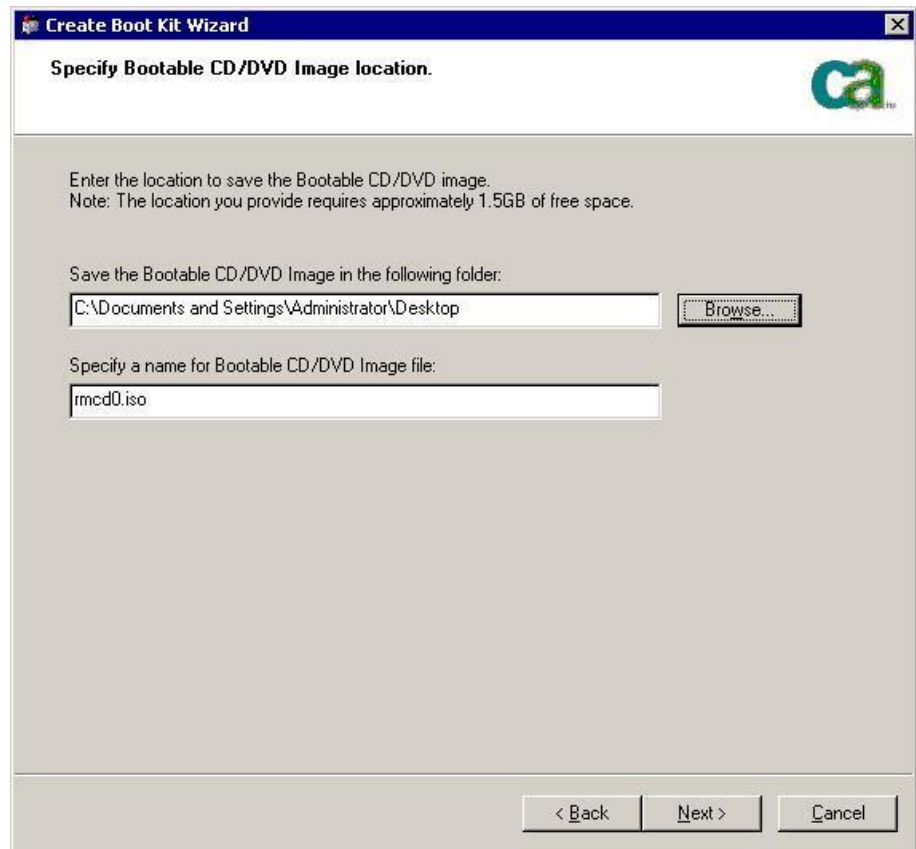
The Specify source location of ARCserve installation package dialog opens.

7. Click Next.

8. Specify the source location of ARCserve installation package and click Next to start creating ARCserve DR CD/DVD image.
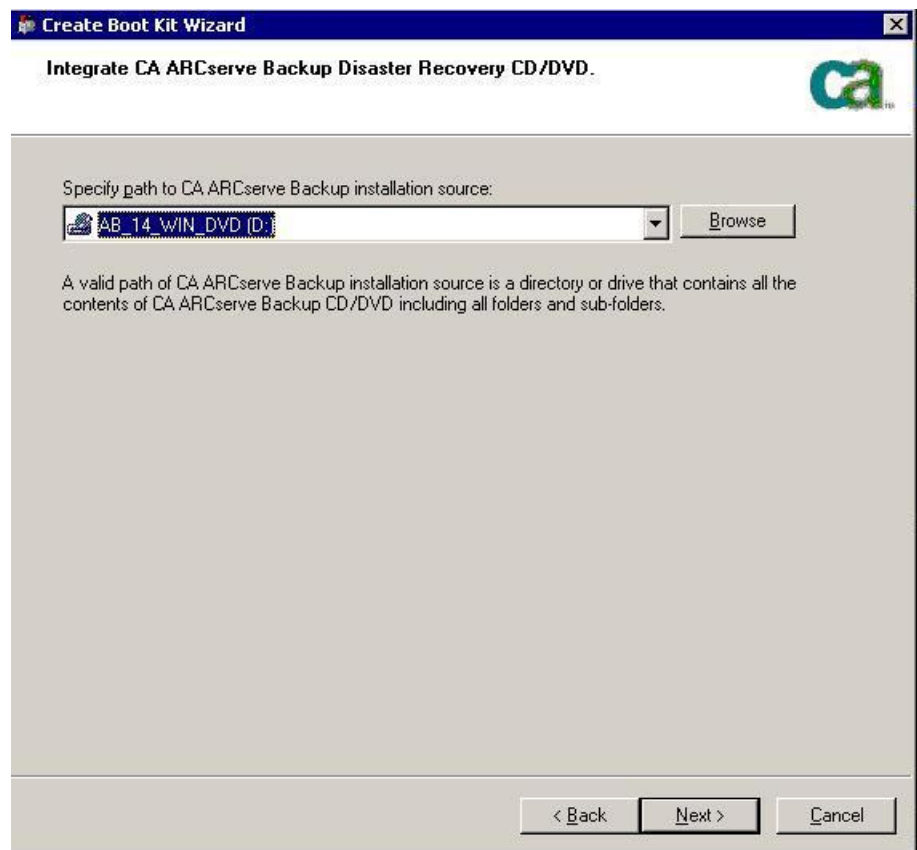
9. The creation process is complete.

    You can now burn the ISO image to a CD/DVD media.

Bootable Tape Method (OBDR) for Windows Server 2003
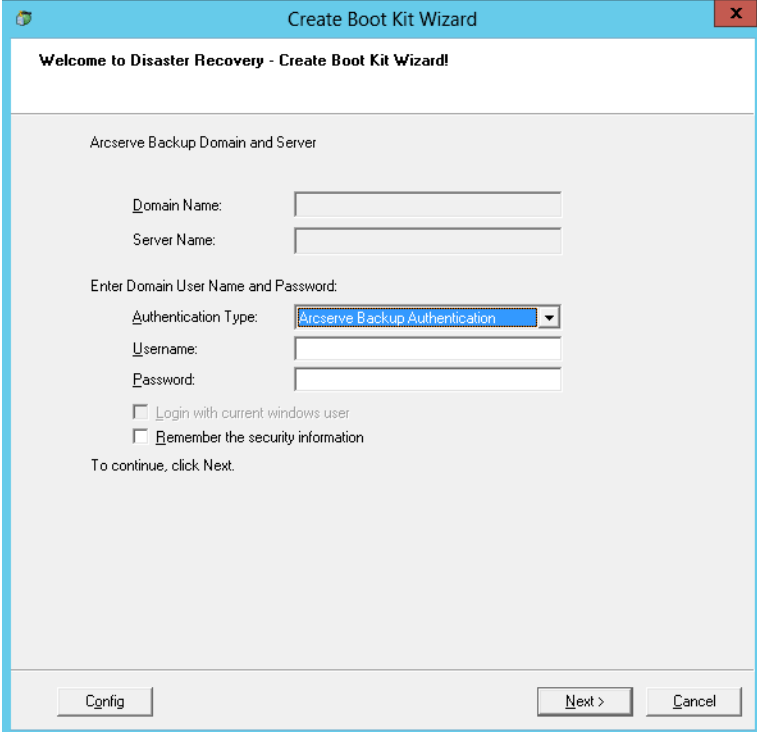
The bootable tape method for Windows Server 2003 allows you to protect the backup server without having to create a machine specific disk. Once the tape is formatted with the proper bootable image, the disaster recovery process can begin and finish completely from the tape drive with the media inside. The Windows Server 2003 CD and the Arcserve Backup CD/DVD are not required during the recovery process.

Note: Bootable tape method does not support Windows XP.

To prepare for a disaster using this method

1. From the Quick Start menu in the Home Page, select Utilities and then click Create Boot Kit Wizard.

    The Create Boot Kit Wizard dialog opens.

2. Enter the domain user name and password after confirming the domain name and server name.

3. Click Next.

    The Select Client Server dialog opens. The dialog has the list of computers and their configurations saved on the Arcserve Backup server. This pane is empty when the Arcserve server does not back up a computer.
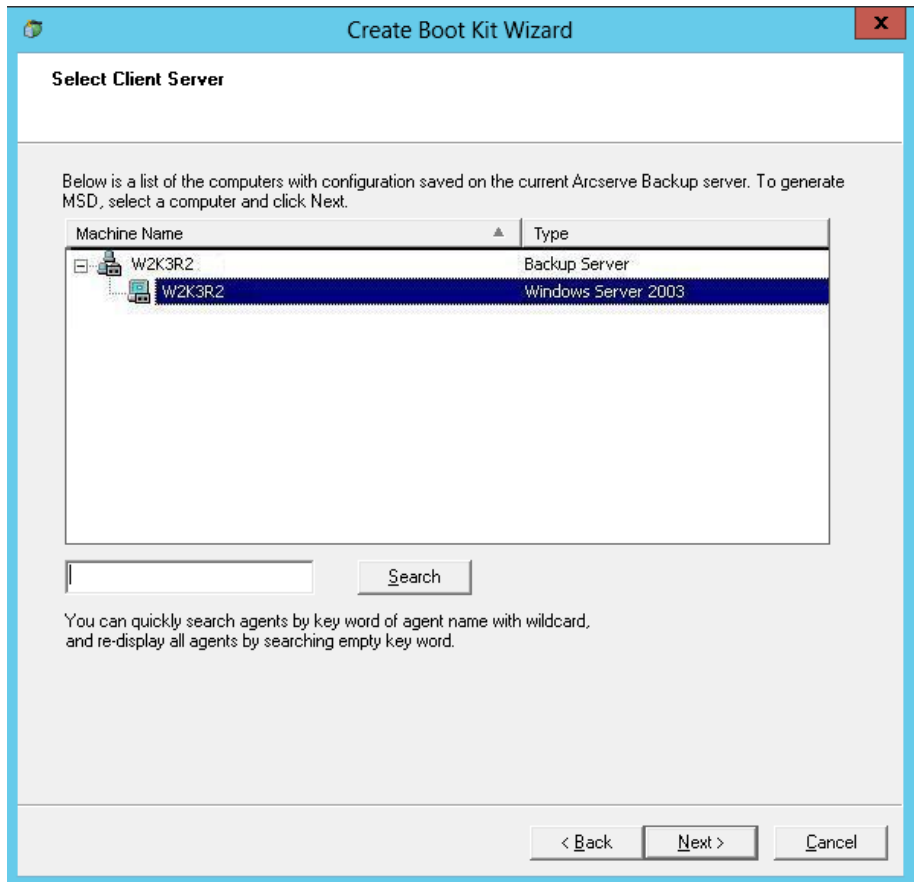
4. Select the computer name and click Next.

   Create Boot Kit Wizard with options opens.

5. Select Create Arcserve Bootable Tape Image, and click Next.
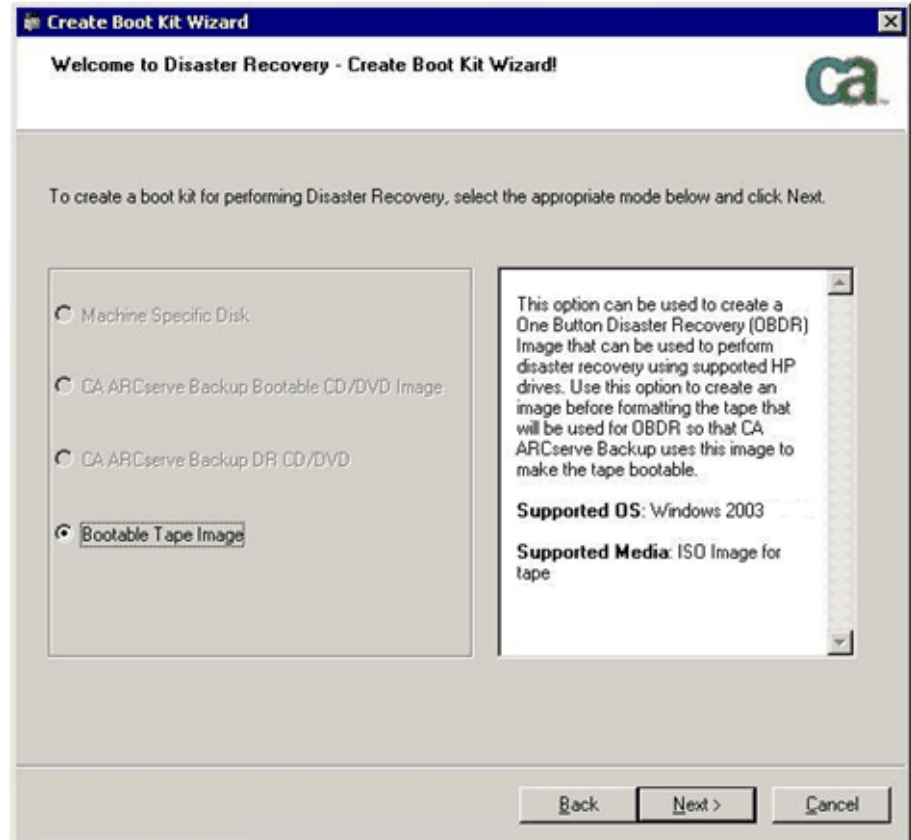
Note: This option is not enabled if a bootable tape drive is not detected.

6. Specify the path for the Windows installation media, and then click Next.

   Note: The Windows 2003 CD you use to create the bootable image must be the same version as that installed on the local system.

7. When the bootable image is created, click Finish.

8. Format the tape media using the Device Manager or Device Wizard to write the image to the tape.

9. Perform a full backup of the local Arcserve Backup server using the tape you formatted.

   Note: If any configuration has changed (for example, network card or SCSI card), you must create a new boot image and run another full backup.

Disaster Recovery on Windows Server 2003 and Windows XP

This section describes how you can recover from a disaster on Windows XP and Windows Server 2003 machines.

Bootable CD Method Disaster Recovery Requirements

To recover from a disaster using the Bootable CD method, you need the following:

- A Arcserve Backup machine-specific recovery disk for the computer that failed.

- If Windows XP Professional was installed on the original system, a Windows XP CD is needed. If Windows Server 2003 was installed, the Windows 2003 CD of the correct edition (for example, Web, Standard, or Enterprise Edition) is needed.

- The Arcserve Backup CD/DVD.

Important! During recovery, the disaster recovery process automatically partitions your hard disk into the original configuration. You can only use the machine-specific recovery disk to perform a disaster recovery on this computer.

More Information:

Create Machine Specific Disks for Disaster Recovery (see page 56)

Start the Disaster Recovery Process using the Bootable CD Method

You can start the disaster recovery process using the Bootable CD method in Windows XP and Windows Server 2003.

To perform disaster recovery on Windows XP, or Windows Server 2003

1. Start the computer you want to recover, using the Windows XP Professional or Windows Server 2003 CD.

2. Press any key to boot from the CD.

    Note: To install additional SCSI drivers that are not supported on the Windows CD, press F6.
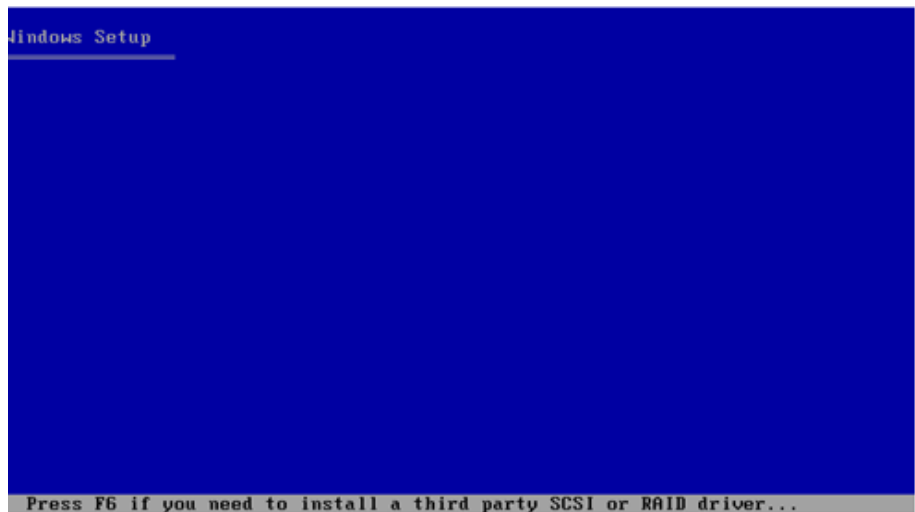
    A message appears at the bottom of the screen prompting you to press F2 to start Automated System Recovery.
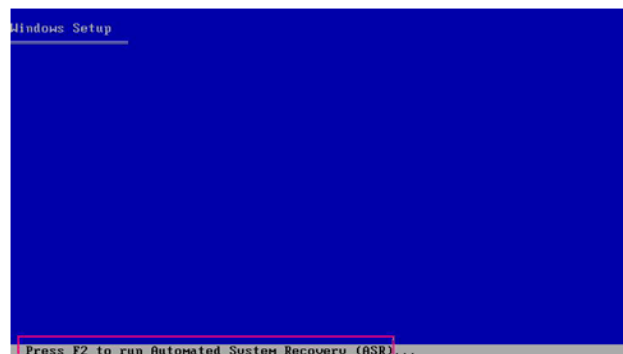
3. Press F2.

    Important! Press F2 to avoid normal Windows installation procedure.

4. When prompted to insert the Windows Automated System Recovery (ASR) Disk, insert the disk labeled Arcserve Backup Machine Specific Disk created for this server, and press Enter.

    If you had previously pressed F6, then you must insert device driver floppy disks.

    The ASR process evaluates the available disk configuration. If ASR requires you to recreate disk partitions, a recovery process dialog opens.

5. Press C to recreate your disk partitions, or F3 to quit.

    ```
    Windows Server 2003, Enterprise Edition Setup

        To restore the configuration of your system, Setup must delete
        and recreate all the partitions on the disks listed below.

        CAUTION:   All data present on these disks will be lost.

        Do you want to continue recreating the partitions?

            •   To continue, press C.  Partitions on all the disks listed
                below will be deleted.

            •   To quit Setup, press F3.  No changes will be made to any
                of the disks on the system.

        [102399 MB Disk 0 at Id 0 on bus 0 on symmpi [MBR]

    C=Continue Setup   F3=Quit
    ```

    This dialog does not appear if you are not recreating disk partitions.

6. Insert the device driver floppy disk if you have installed additional SCSI, FC, or RAID drivers.

    Based on the configuration of the computer you are recovering, you may have to insert the Windows Automated System Recovery disk several times. This disk is identical to the disk labeled Arcserve Backup Machine Specific Disk.

7. Press Enter again.

    The required files are copied to the Windows installation folders.

    Note: The Machine Specific Disk is also called as the Machine Specific Recovery Disk.

8. Remove the Arcserve Backup machine specific disk and reboot the computer. When you reboot, the ASR process continues.

   This process installs the device drivers and network protocols and configures the computer to run the disaster recovery process. It also restores and formats the volumes present on your computer automatically.

   Important! If you press Enter, Esc, or Alt-F4 when the Automated System Recovery is formatting the volumes on your Windows XP or Windows 2003 systems, the Automated System Recovery process is interrupted and the formatting fails. Consequently, the data on these volumes will not be restored.

9. Insert the Arcserve Backup CD/DVD, the machine specific disk, and then click OK.

   The Disaster Recovery wizard opens and the recovery process begins.

Complete the Disaster Recovery Process using the Bootable CD Method in Express Mode

You can complete the disaster recovery process on the Windows XP and Windows 2003 systems. This process begins when the Disaster Recovery wizard appears and the recovery process starts.

To complete the disaster recovery process

1. Start the disaster recovery process.

   Choose Mode dialog opens.

2. Select Express Mode to recover the system by using the computer default settings stored during the backup time.
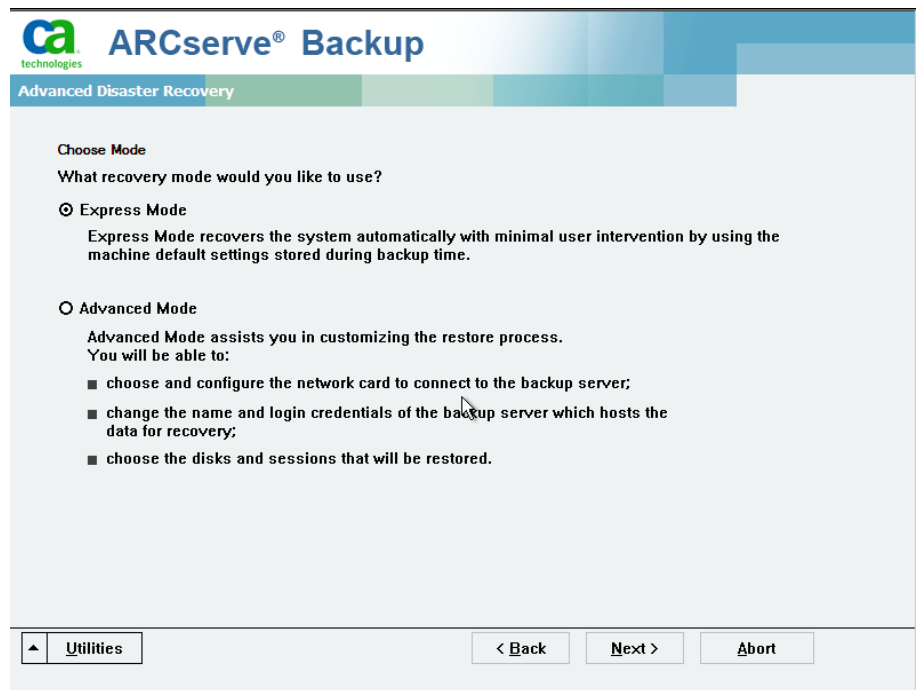
3. Click Next.

    The Enter caroot Password dialog opens.

    As the disaster recovery session has to be restored during this period, you will be prompted to provide the caroot password. The reason for which you must provide the password could be one of the following:

    - At least one session was encrypted by a key or protected by a password.

    - The session password was stored in the database according to the global option setting.

    - The caroot password is not empty.

    Note: This password is required to work with the saved session password or encryption key to restore the encrypted or password-protected sessions. Enter the correct caroot password, if necessary, to avoid manual decryption of each session.

4. Enter the password and click OK.

5. Click Next to start the restore process.

    The Disaster Recovery process is complete.

    Note: You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to Reboot.

When your computer restarts, it is restored to the state it was in at the time of the last full backup.

Important! If the Arcserve Backup database is installed on this computer and this computer is not the Arcserve Backup primary server, you must run the Arcserve Database Recovery Wizard at this time. For more information about the Arcserve Database Recovery Wizard, see the topic Recover the Arcserve Backup Database Using Arcserve Database Recovery Wizard in the *Arcserve Backup Administration Guide*.

Note: To run the Install and Reboot options on the Disaster Recovery wizard while using USB backup devices dialogs, use the following keyboard shortcuts:

- Install—Shift + i

- Reboot—Shift + r

Complete the Disaster Recovery Process using the Bootable CD Method in Advanced Mode

You can complete the disaster recovery process on the Windows XP and Windows 2003 systems. This process begins when the Disaster Recovery wizard appears and the recovery process starts.

To complete the disaster recovery process

1. Start the disaster recovery process.

   Choose Mode dialog opens.

2. Select the Advanced Mode to recover the system using the customized process. You can configure the network card, change the login credentials and also select the sessions.

3. Click Next.

   The Enter caroot Password dialog opens.

   The reason for which you must provide the password could be one of the following:

   ■ At least one session was encrypted by a key or protected by a password.

   ■ The session password was stored in the database according to the global option setting.

   ■ The caroot password is not empty.

   Note: This password is required to work with the saved session password or encryption key to restore the encrypted or password protected sessions. Enter the correct caroot password, if necessary, to avoid manual decryption of each session.

4. Enter the password and click OK.

   The Network connections dialog opens, and is followed by the Session dialog.

5. Select the session that you want to restore, and click Next.

You can enter the password for each session depending on the status of each key at the end of each row in the Session Assign dialog. Types of keys include:

■ When the session has a key option, it means that the session was encrypted by a key, but the key was not saved in the database. You must provide the encryption key to restore these sessions.

■ When the session has a key option with a tick mark, it means that the session was encrypted by a key or protected by a password, and the encryption key or session password was saved in the database. No encryption key or session password is required to restore these sessions.

■ When the session has a key option with a question mark, it means that the session password status is unknown. You can enter the session password, if necessary.

The Summary dialog opens.

6. Verify the Summary list.

7. Click Start Disaster Recovery to start the process.

   The data is copied from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

   Note: You can run most of the 32-bit Windows programs, such as regedit.exe, from the DOS prompt window. Click Utilities, and select Run to open a Windows command line console window.

   The Disaster Recovery process is complete.

   Note: You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to reboot.

When your computer restarts, it is restored to the state it was in at the time of the last full backup.

Important! If the Arcserve Backup database is installed on this computer and this computer is not the Arcserve Backup primary server, you must run the Arcserve Database Recovery Wizard at this time. For more information about the Arcserve Database Recovery Wizard, see the topic Recover the Arcserve Backup Database Using Arcserve Database Recovery Wizard in the *Arcserve Backup Administration Guide*.

Note: To run the Install and Reboot options on the Disaster Recovery wizard while using USB backup devices dialogs, use the following keyboard shortcuts:

- Install—Shift + i
- Reboot—Shift + r

Bootable CD Method Disaster Recovery Using the Reimaged CD Requirements

To recover from a disaster using the Reimaging CD, you need the following:

- Reimaged CD

Important! During the disaster recovery process, your hard disk is automatically partitioned per the original configuration.

More information:

Reimage Bootable CD Using Boot Kit Wizard (see page 63)

Start the Disaster Recovery Process using the Reimaged CD

You can perform disaster recovery using the reimaged or the remastered CD on a Windows XP or Windows 2003 computer..

To perform disaster recovery using the reimaged CD

1. Start the computer you want to recover, using the reimaged CD.

2. Press any key to boot from the reimaged CD.

   A message appears at the bottom of the screen prompting you to press F2 to start Automated System Recovery.
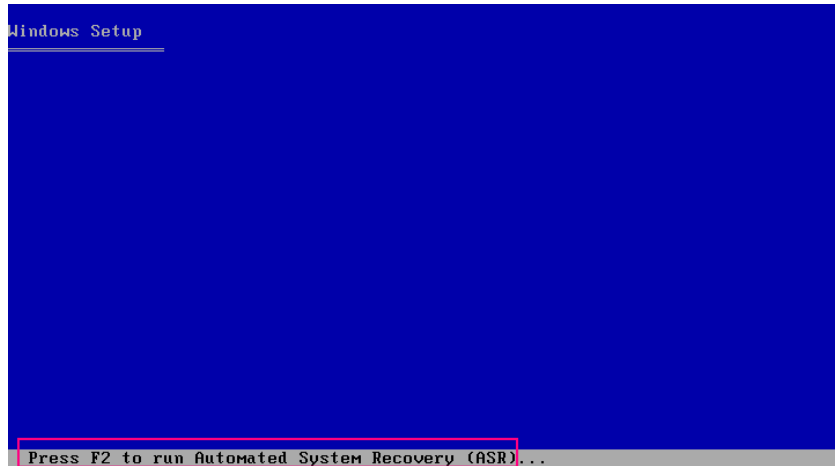
3. Press F2.

   For <win> XP, insert the machine specific disk after you press F2.

   For <win> Server 2003, press F2 and continue.

   Important! Press F2 to avoid normal Windows installation.

   The ASR process evaluates the available disk configuration. If ASR requires you to recreate disk partitions, a recovery process dialog opens.

4. Press C to recreate your disk partitions, or F3 to quit.

   This dialog does not appear if you are not recreating disk partitions.

   The files are copied to the Windows installation folders.

5. Remove any floppy disks from the system, except the reimaged CD.

   The computer will reboot automatically.

6. When prompted to insert Windows installation media, insert the reimaged CD.

   The Windows ASR process continues.

Important! If you press Enter, Esc, or Alt-F4 when the Automated System Recovery is formatting the volumes on your Windows XP or Windows 2003 systems, the Automated System Recovery process is interrupted and the formatting fails. Consequently, the data on these volumes will not be restored.

The Disaster Recovery wizard appears, and the recovery process begins.

Complete Disaster Recovery using the Reimaged CD in Express Mode

You can complete the disaster recovery process on Windows XP and Windows Server 2003 computer using the reimaged CD.

To complete the disaster recovery process

1. Start the disaster recovery process using the reimage CD.

    The Choose Mode dialog opens.

2. Select Express Mode to recover the system by using the machine default settings stored during backup.

3. Click Next.

    The Enter caroot Password dialog opens.

    The reason for which you must provide the password could be one of the following:

    ■   At least one session was encrypted by a key or protected by a password.

    ■   The session password was stored in the database according to the global option setting.

    ■   The caroot password is not empty.

    Note: This password is required to work with the saved session password or encryption key to restore the encrypted or password protected sessions. Enter the correct caroot password, if necessary, to avoid manual decryption of each session.

4. Enter the password and click OK.

5. Click Next to start the restore process.

    The Summary dialog opens.
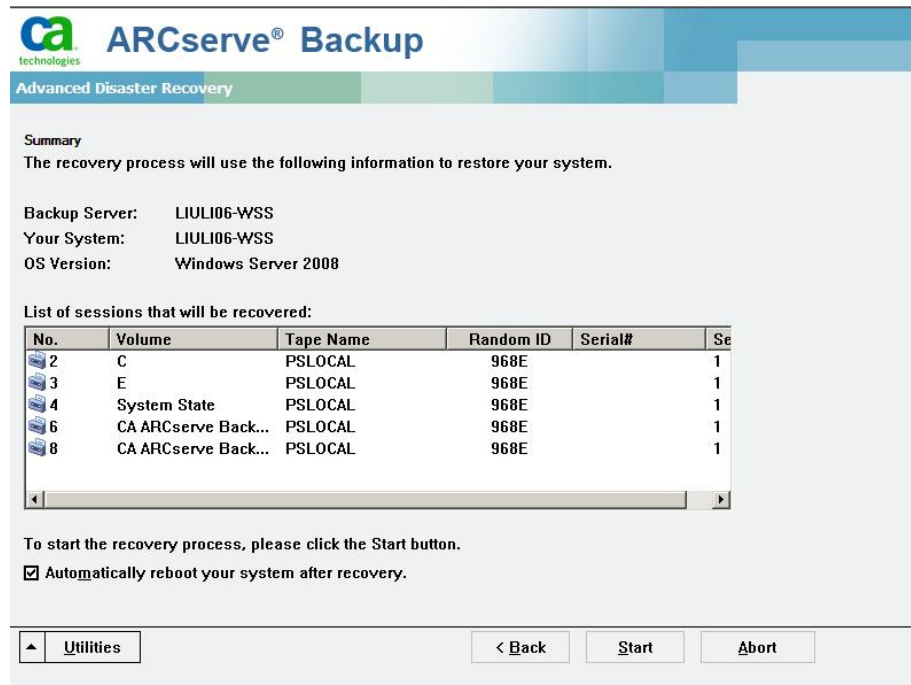
6. Verify the Summary list.

7. Click Start Disaster Recovery to start the process.

   The data is copied from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

   Note: Click Utilities, and select Run to open a Windows command line console window. You can run most of the 32-bit Windows programs, such as regedit.exe, from the DOS prompt window.

   The Disaster Recovery process is complete.

   Note: You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to reboot.

When your computer restarts, it is restored to the state it was in at the time of the last full backup.

Complete Disaster Recovery using the Reimaged CD in Advanced Mode

You can complete the disaster recovery process on Windows XP and Windows Server 2003 computer using the reimaged CD.

To complete the disaster recovery process

1. Start the disaster recovery process using the reimage CD.

    The Choose Mode dialog opens.

2. Select the Advanced Mode to recover the system using the customized process. You can configure the network card, change the login credentials, and also select the sessions.

3. Click Next.

    The Enter caroot Password dialog opens.

    The reason for which you must provide the password could be one of the following:

    ■   At least one session was encrypted by a key or protected by a password.

    ■   The session password was stored in the database according to the global option setting.

    ■   The caroot password is not empty.

    Note: This password is required to work with the saved session password or encryption key to restore the encrypted or password protected sessions. Enter the correct caroot password, if necessary, to avoid manual decryption of each session.

4. Enter the password, and click OK.

    The Network connections dialog opens followed by the Session dialog.

5. Select the session that you want to restore, and click Next.

You can enter the password for each session depending on the status of each key at the end of each row in the Session Assign dialog. Types of keys include:

■ When the session has a key option, it means that the session was encrypted by a key, but the key was not saved in the database. You must provide the encryption key to restore these sessions.

■ When the session has a key option with a tick mark, it means that the session was encrypted by a key or protected by a password, and the encryption key or session password was saved in the database. No encryption key or session password is required to restore these sessions.

■ When the session has a key option with a question mark, it means that the session password status is unknown. You can enter the session password, if necessary.

The Summary dialog opens.

6. Verify the Summary list.

7. Click Start Disaster Recovery to start the process.

   The data is copied from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

   Note: Click Utilities, and select Run to open a Windows command line console window. You can run most of the 32-bit Windows programs, such as regedit.exe, from the DOS prompt window.

   The Disaster Recovery process is complete.

   Note:You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to reboot.

When your computer restarts, it is restored to the state it was in at the time of the last full backup.

Bootable Tape Method Disaster Recovery Requirements for Windows Server 2003

To recover 32-bit Windows Server 2003 from a disaster using the Bootable Tape method, you need the following:

- The tape drive locally attached to the machine must be a bootable tape drive and must support OBDR.

- The tape media used in the tape drive must contain the proper bootable image.

  Note: You must have at least one full local machine backup of the system on the tape media.

Start the Bootable Tape Method Disaster Recovery Process <win> 2003

You can start the recovery process on a Windows Server 2003 computer using the Bootable Tape method using the following procedure.

To recover from a disaster using bootable tape method

1. Remove all media from the disk and CD drives and shut down the server.

2. Start the tape drive in boot mode.

3. Insert the bootable tape backup media into the tape drive.

4. Start the failed server.

   As the failed server starts, it performs startup diagnostics and locates the tape drive as its boot device.

5. Confirm if you really want to start the disaster recovery process. Enter Y for Yes to proceed.

   The system boots from the tape drive and enters the Windows setup mode.

6. Press F6 to install any SCSI drivers not supported by the Windows Server 2003 CD.


```
Windows Setup
```

```
Press F6 if you need to install a third party SCSI or RAID driver...
```

7. Press F2 to begin the Windows ASR process.


```
Windows Setup
```

```
Press F2 to run Automated System Recovery (ASR)...
```
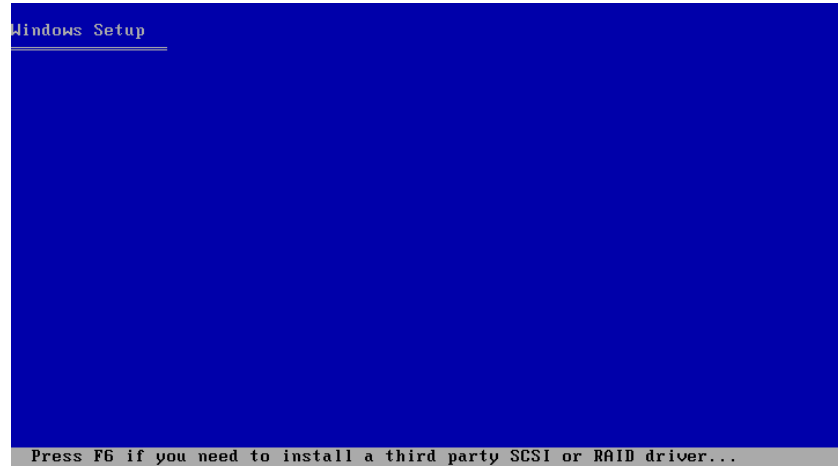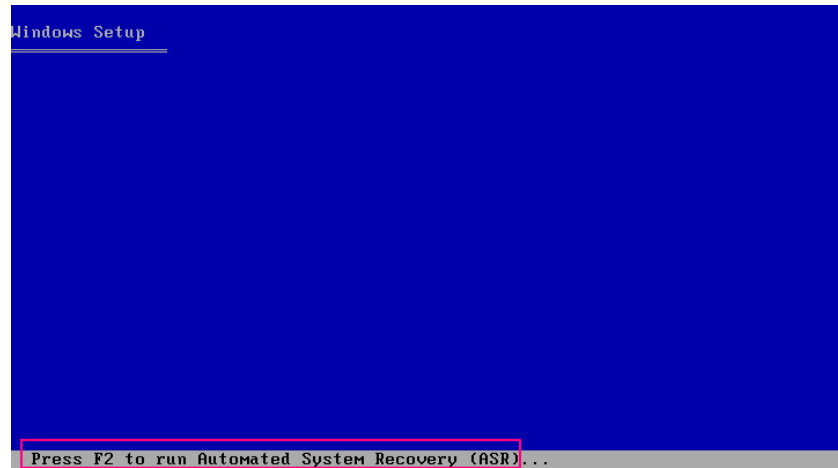
   For Windows 2003, the floppy disk is not required.

   The recovery process recreates the boot and system partitions and copies the setup files to the partitions. If the boot and system partitions are not the same partition, the disaster recovery process may require a reboot. If so, restart the disaster recovery process from the beginning of this procedure.

8. After the necessary Windows setup files have been copied to the system partition, reboot the server.

   The tape drive is reset to normal mode and the system is booted from the hard disk. After the system has finished booting, the ASR process initializes the environment and the Disaster Recovery wizard appears.

Complete the Bootable Tape Method Disaster Recovery Process in <win> Server 2003 in Express Mode

You must complete the Disaster recovery process on the Windows Server 2003 using the following procedure.

To complete the disaster recovery process

1. In the disaster recovery wizard, select Express Mode and click Next.

   Express Mode uses all the default settings as recorded on the backup tape to restore the system with very minimal user interaction.
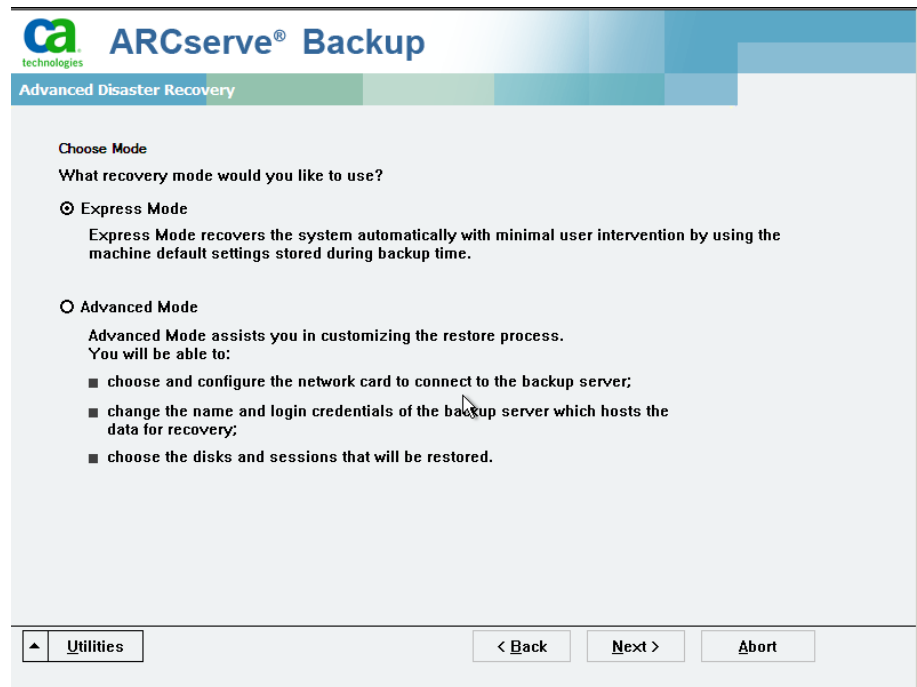
2. Select the Express mode, and click Next.

    The Enter caroot Password dialog opens.

    As the disaster recovery session has to be restored during this period, you will be prompted to provide the caroot password. This could be for one of the following reasons:

    ■ At least one session was encrypted by a key or protected by a password.

    ■ When you set to Save Current Session/Encryption Password to the Arcserve Backup database in the global option during backup.

    ■ The caroot password is not empty.

    Note: This password is required to work with the saved session password or the encryption key to restore encrypted or password protected sessions. Enter the correct caroot password, if necessary, to avoid manual decryption of each session.

3. Enter the password, and click OK to start the restore process.

    The Disaster Recovery process is complete.

    Note: You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to reboot.

    When your computer restarts, it is restored to the state it was in at the time of the last full backup.

Complete the Bootable Tape Method Disaster Recovery Process in <win> Server 2003 in Advanced Mode

You must complete the Disaster recovery process on Windows Server 2003 using the following procedure.

To complete the disaster recovery process

1. In the disaster recovery wizard, select Advanced Mode and click Next.

   Advanced Mode stores specific custom restore parameters to adapt to any change in the environment.
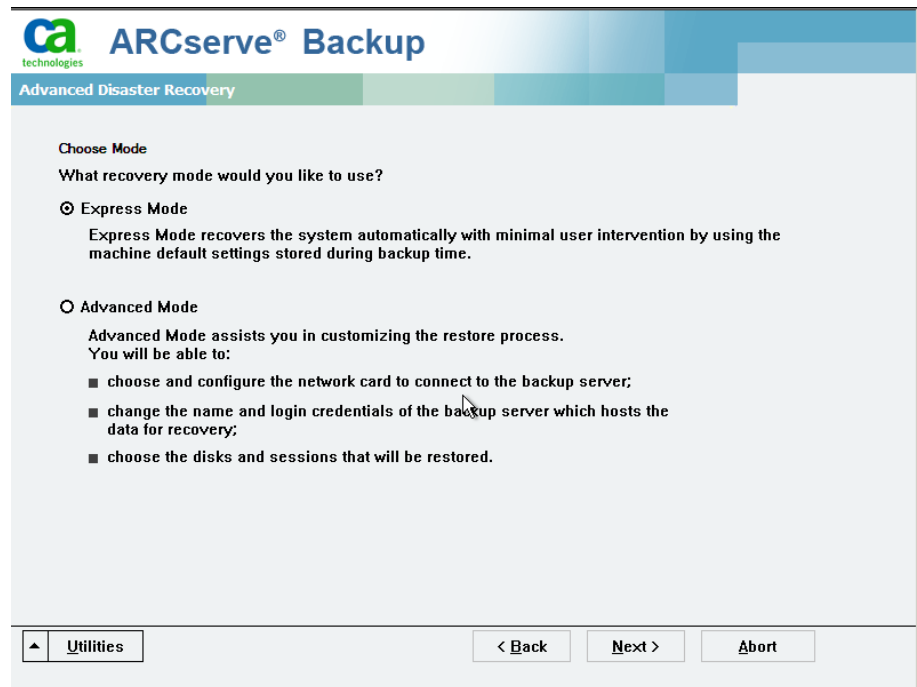
The Enter caroot Password dialog opens.

2.   Enter the password, and click OK.

The Network connections dialog appears followed by the Session dialog.

3.   Select the session that you want to restore, and click Next.
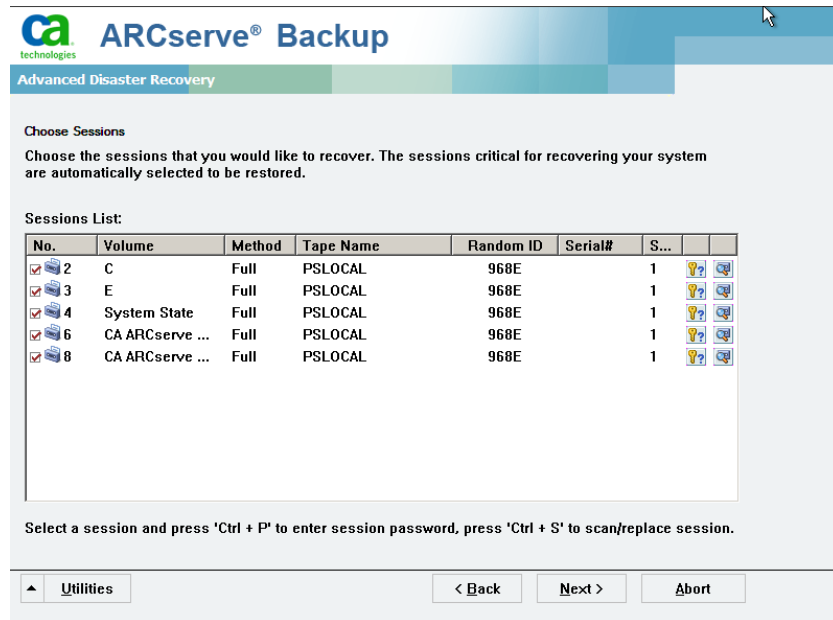
You can enter the password for each session depending on the status of each key at the end of each row in the Session Assign dialog. Types of keys include:

■ When the session has a key option, it means that the session was encrypted by a key, but the key was not saved in the database. You must provide the encryption key to restore these sessions.

■ When the session has a key option with a tick mark, then the session was encrypted by key or protected by password and the encryption key or session password was saved in the database. No encryption key/session password is required to restore these sessions.

■ When the session has a key option with a question mark, it means that the session password status is unknown. You can enter the session password, if necessary.

The Summary dialog opens.
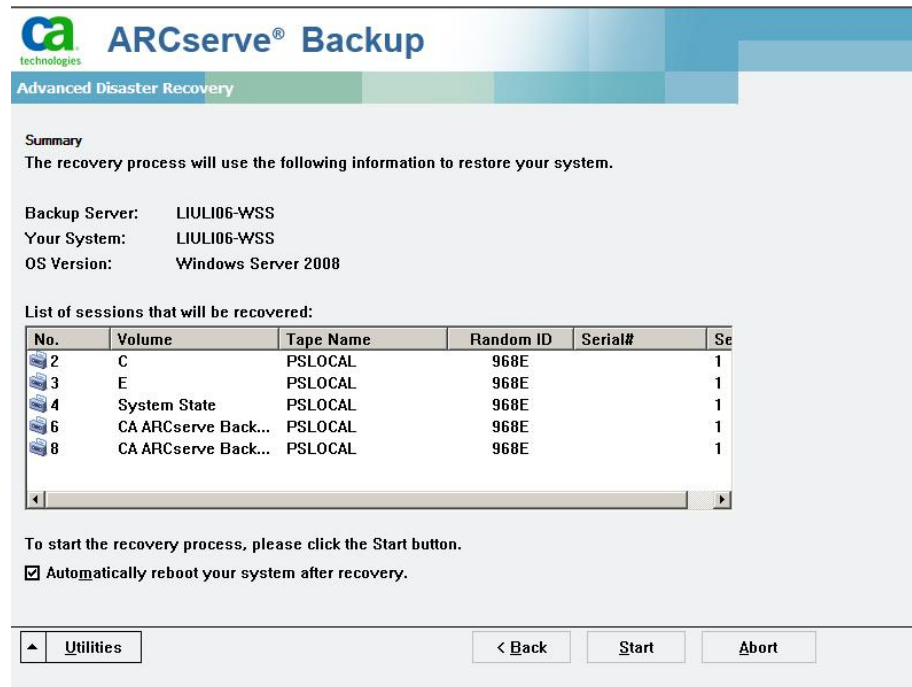
4. Verify the Summary list.

5. Click Start Disaster Recovery to start the process.

    The data is copied from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

    Note: You can run most of the 32-bit Windows programs, such as regedit.exe, from the DOS prompt window. Click Utilities, and select Run to open a Windows command line console window.

    The Disaster Recovery process is complete.

    Note: You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to reboot.

    When your computer restarts, it is restored to the state it was in at the time of the last full backup.

Disaster Recovery Using Locally-attached USB Backup Devices

The Arcserve Backup Disaster Recovery option supports the use of USB backup devices in disaster recovery operations.

Note: You must connect and turn on your USB devices to use them for disaster recovery.

For remote disaster recovery, if you have USB devices attached to your backup server, use the typical disaster recovery procedure to recover your data.

For a local disaster recovery, if you are using USB devices during your backup operation, the Disaster Recovery wizard displays a dialog prompting you to install third-party drivers for these devices.
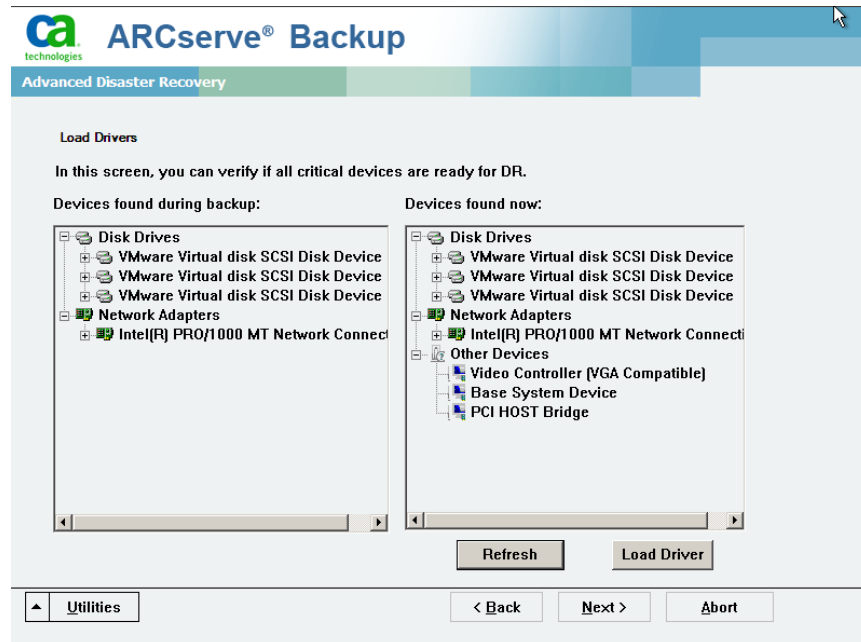
The dialog displays the following information:

Original Device List

Displays all USB backup devices discovered when the full machine backup was taken, based on the information stored on the machine specific disk.

Current Device List

Displays all USB devices discovered on the currently running system and provides the following information for each device:

– Device: Provides a description of the discovered device

– Service: Identifies the system service associated with the device

– Active: Provides the status of the service associated with the device

A value of Yes in the Active field indicates that a driver is installed for a device. If the Service field for a device is blank or the value in the Active field is No, you may have to install the third-party driver for the device to use it properly.

Note: The list identifies all discovered devices, not only those used for backup and restore purposes. You do not have to install drivers for devices that are not used during restore operations.

Install

Opens a dialog that lets you find a device driver and install it on the currently running system. The driver can be either an executable (EXE) supplied by a hardware vendor or an INF file:

– For drivers in EXE files, the wizard launches the executable. Follow the on-screen instructions to install the driver.

– For drivers in INF files, the wizard verifies that all dependency files (SYS, DLL, CAT, etc) coexist at the same location as the INF file. If not, the wizard displays a list of the missing files. If all the files are found, or if you proceed with the installation despite a missing file, the wizard installs the driver using its built-in PnP mechanism.

Note: You cannot specify the device on which the driver installs. Also, you can use the keyboard shortcut Shift+<i>for the install button on the wizard.

Refresh

Refreshes the Current Device List after installing a driver. You can use the keyboard shortcut Shift+ r for the Refresh button on the Disaster Recovery wizard.

Note: It can take some time before the installed driver begins to work with the device.

Install USB Devices After Backup

You can install USB drivers only if these devices were configured when the full machine backup was taken. If you did not set up these devices during backup, but you want to use them during disaster recovery, you must manually create a file called drusb.ini on the machine-specific disk, and add the following content:

```
[Devices]
0=None
[MetaData]
DeviceCount=1
```

Disaster Recovery in Windows Server 2003 and Windows XP Using Bootable CD method (64-bit)

This section describes how you can use the Bootable CD method to protect local and remote Windows Systems and recover from disaster. For more information on supported platforms, see Disaster Recovery Option Support (see page 13).

Note: Windows XP does not support local disaster recovery.

The disaster recovery process for Windows 64-bit uses the Client Agent to restore the actual data.

Disaster Recovery Requirements in Windows XP and Windows Server 2003

To recover from a disaster using the Bootable CD method, you need the following:

■ A Arcserve Backup machine-specific recovery disk for the computer that failed. This is the disk you created following the instructions in section Create Machine-Specific Recovery Disks (see page 56).

■ If Windows XP Professional (64-bit) was installed on the original system, a Microsoft Windows XP CD is needed. If Windows Server 2003 (64-bit) was installed, the Windows Server 2003 installation media of the correct edition (for example, Web, Standard, or Enterprise Edition) is needed.

■ The Arcserve Backup installation media

Important! During recovery, the disaster recovery process automatically partitions your hard disk per the original configuration. You can only use the machine-specific recovery disk to perform a disaster recovery on this computer.

Perform Disaster Recovery on Windows XP and Windows Server 2003

You can perform advanced disaster recovery on 64-bit Windows XP and Windows Server 2003 using the Client Agent.

To perform disaster recovery

1. Start the computer that you want to recover, using the Windows XP Professional or Windows Server 2003 64-bit CD.

   A prompt opens.

2. Press any key to boot from the CD.

   A message appears at the bottom of the screen prompting you to press F2 to start Automated System Recovery.
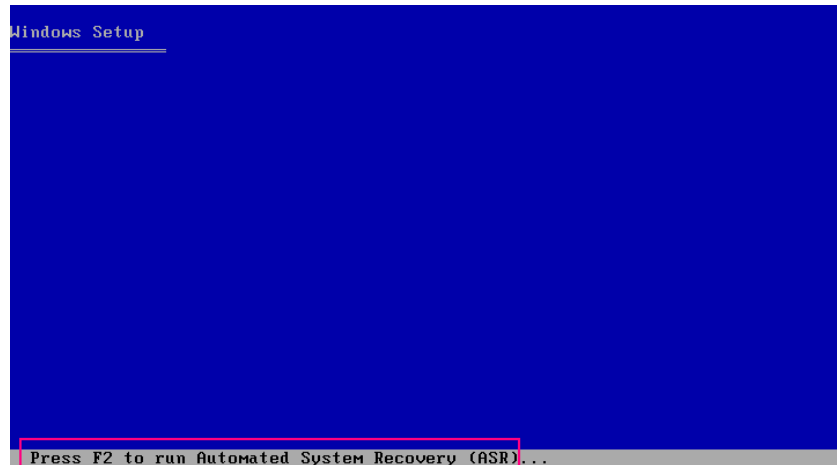
3. Press F2.

   The Windows Automated System Recovery GUI opens.

   Important! You must press F2; otherwise, the normal Windows installation procedure starts.

   The system and boot partitions are formatted, and the necessary files are copied to the hard drive.

4. Reboot the machine when the files are copied.

   The device drivers and network protocols are installed. The operating system formats the volumes screen.

   Important! Do not press Enter, Esc, or Alt-F4 and interrupt while the volumes on your Windows XP, or Windows 2003 are formatted; doing so terminates the formatting process, and the data on these volumes will not be restored.

   DRLAUNCH is initiated automatically. It copies the supplied media files and starts the 64-bit Advanced Disaster Recovery Wizard.

   ADR GUI ADRMAIN.exe starts executing, and reads the DR information.

5. Select the Express mode, or the Advanced mode in the Choose Mode dialog that opens.

   ■ In Express mode you recover the system using the machine default settings stored during backup.

   ■ In Advanced mode, you give the network configuration details for remote disaster recovery. Network configuration is also required for local disaster recovery for SAN member server and local disaster recovery using remote FSD.

   For Express Mode:

   a. Select the Express mode, and click Next.
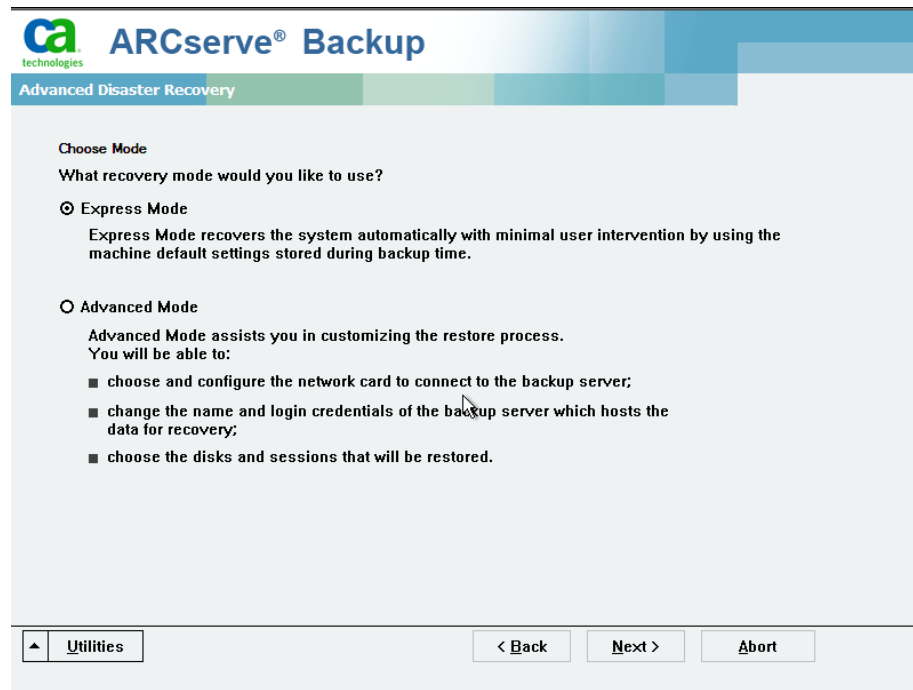
The Enter caroot Password dialog opens.

As the disaster recovery session has to be restored during this period, you will be prompted to provide the caroot password because

- At least one session was encrypted by key or protected by password.

- The password was saved to database in global option during backup.

- The caroot password is not empty.

Note: This password is required to work with saved session password or encryption key to restore encrypted or password protected sessions. Enter the correct caroot password, if necessary, to avoid decryption of each session manually.

b. Enter the password and click OK.

c. Click Start to begin the disaster recovery process.
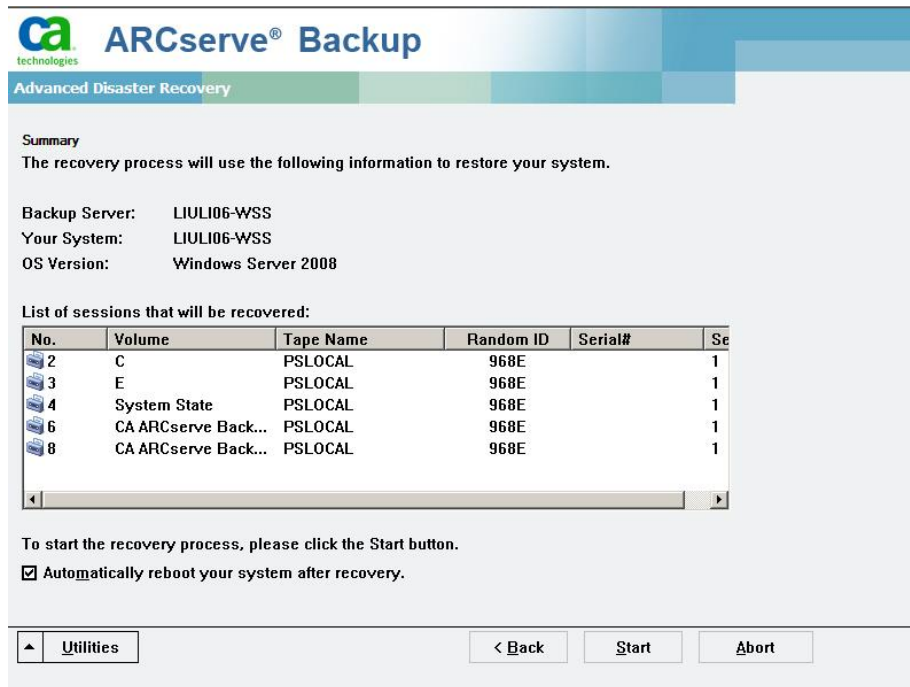
For Advanced Mode:

a. Select the Advanced mode on the Select Mode dialog, and click Next.
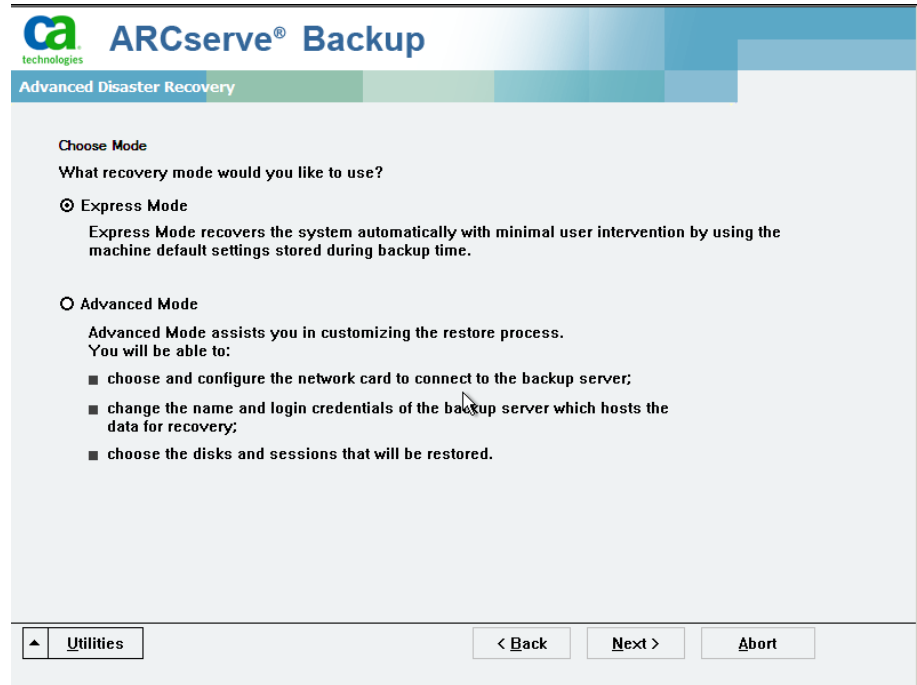
The Enter caroot Password dialog opens.

b.   Enter the password, and click OK.

The Network connections dialog opens followed by the Session dialog.

c.   Select the session that you want to restore, and click Next.

You can enter the password for each session depending on the status of each key at the end of each row in the Session Assign dialog. Types of keys include:

■   When the session has a key option, it means that the session was encrypted by a key, but the key was not saved in the database. You must provide the encryption key to restore these sessions.

■   When the session has a key option with a tick mark, it means that the session was encrypted by a key or protected by a password and the encryption key or the session password was saved in the database. No encryption key or session password is required to restore these sessions.

■   When the session has a key option with a question mark, then the session password status is unknown. You can enter the session password, if necessary.

The Summary dialog opens.

d. Verify the Summary list.

e. Click Start to begin the disaster recovery process.

The data is copied from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

Note: You can run most of the 32-bit Windows programs, such as regedit.exe, from the DOS prompt window. Click Utilities, and select Run to open a Windows command line console window.

The Disaster Recovery process is complete.

Note: You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to reboot.

When your computer restarts, it is restored to the state it was in at the time of the last full backup.

Important! If the Arcserve Backup database is installed on this computer and this computer is not the Arcserve Backup primary server, you must run the Arcserve Database Recovery Wizard at this time. For more information about the Arcserve Database Recovery Wizard, see the topic Recover the Arcserve Backup Database Using Arcserve Database Recovery Wizard in the *Arcserve Backup Administration Guide*.

Note: To run the Install and Reboot options on the Disaster Recovery wizard while using USB backup devices dialogs, use the following keyboard shortcuts:

- Install—Shift + i

- Reboot—Shift + r

Disaster Recovery in Windows Server 2008 and Windows 7

Disaster recovery in Windows Server 2008 is based on the Windows Server 2008 Recovery Environment. Only the Bootable CD method is supported for Windows Server 2008. The Windows Server 2008 platforms that are supported include:

- Windows Server 2008 (x86-bit)

- Windows Server 2008 (x64-bit)

- Windows Server 2008 (IA 64-bit)

- Windows Server 2008 R2

Note: For more information about <win> Server 2008, see http://www.microsoft.com/.

Windows 7 supports only remote disaster recovery:

- Windows 7 (x86-bit)

- Windows 7 (x64-bit)

Disaster Recovery Requirements for Windows Server 2008 and Windows 7

You can perform disaster recovery on <win> Server 2008 and Windows 7 using a machine-specific recovery disk and Windows Server 2008 or Windows 7 installation media. To perform an advanced disaster recovery in Windows Server 2008 or Windows 7 you need the following:

- Arcserve Backup machine-specific recovery disk or a USB flash media

  Note: A Windows Server 2008 or Windows 7 machine-specific disk can be stored on a floppy disk and USB flash media.

- The Windows Server 2008 or Windows 7 installation media of the correct edition (for example, Web, Standard, or Enterprise Edition)

- Arcserve Backup Disaster Recovery CD

More information:

Create Machine Specific Disks for Disaster Recovery (see page 56)

Recover Windows Server 2008 and Windows 7 from a Disaster

You can perform disaster recovery on Windows Server 2008 and Windows 7 systems using the Bootable CD method.

Follow these steps:

1. Start the system and insert the Windows Server 2008 installation media in the optical drive. Verify that the BIOS is configured to boot from this optical drive. Insert the machine specific recovery disk in the floppy drive or USB port, and turn on the system.

   Note: You can also use the USB flash media for recovery. If there is more than one raw disk present in the system, you will be prompted to reboot the system. Click OK to reboot and follow step 1.

2. Insert the Arcserve Backup Disaster Recovery media, and then click Next to open the Advanced Disaster Recovery dialog and start the recovery process.

3. Specify the language and keyboard settings and click Next.

4. Specify the path for machine specific disk, and then click Next to open the Choose Mode dialog. You can specify either a local path, or a network location.

   Note: In <win> Server 2008 disaster recovery, multiple instances of machine specific disks are stored on the storage media.

5. Select from the following modes that appear on the Choose Mode dialog:

   Express Mode

   Recovers the system by using the machine default settings stored during backup.

   Advanced Mode

   Recovers the system using the customized process. You can configure the network card, change the login credentials and also select the sessions.

   For Express Mode:

   a. Select the Express mode, and click Next.
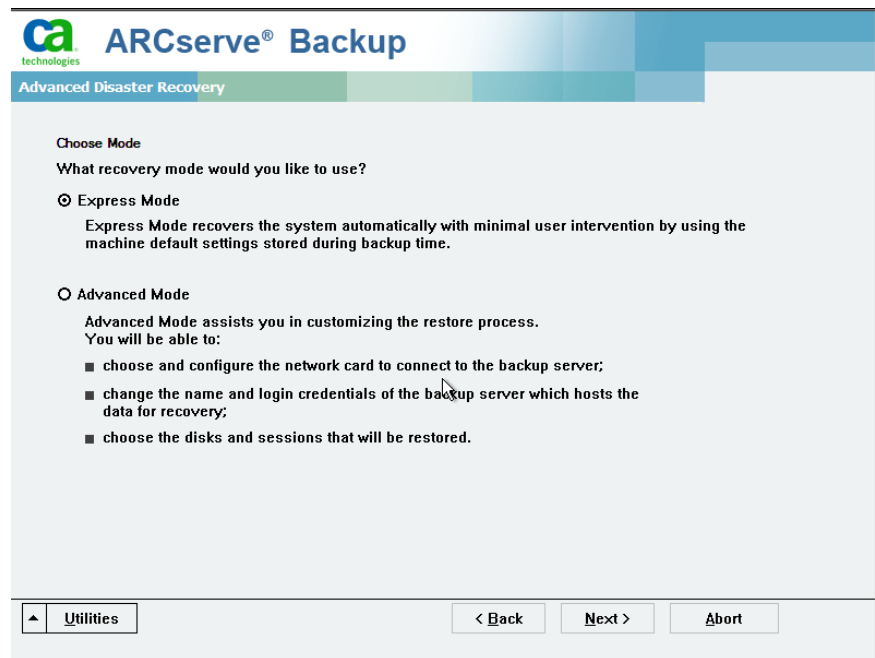
The Enter caroot Password dialog opens.

As the disaster recovery session has to be restored during this period, you will be prompted to provide the caroot password. This could be for the following reasons:

■   At least one session was encrypted by a key or protected by a password.

■   When you set to Save Current Session/Encryption Password to the Arcserve Backup database in the global option during backup.

■   The caroot password is not empty.

Note: This password is required to work with the saved session password or the encryption key to restore encrypted or password protected sessions. Enter the correct caroot password, if necessary, to avoid manual decryption of each session.

b.   Enter the password, and click OK.

Important! Windows formats the disk after you click OK.

c.   Click Next to start the restore process.

For Advanced Mode:

a. Select the Advanced mode on the Select Mode dialog, and click Next.
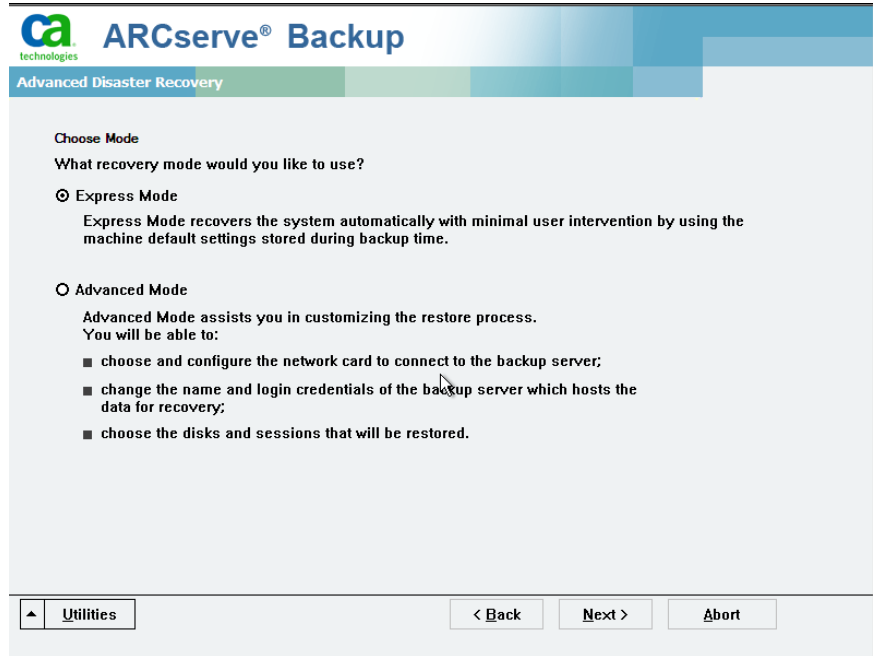
The Enter caroot Password dialog opens.

b. Enter the password, and click OK.

The Load Drivers dialog opens.
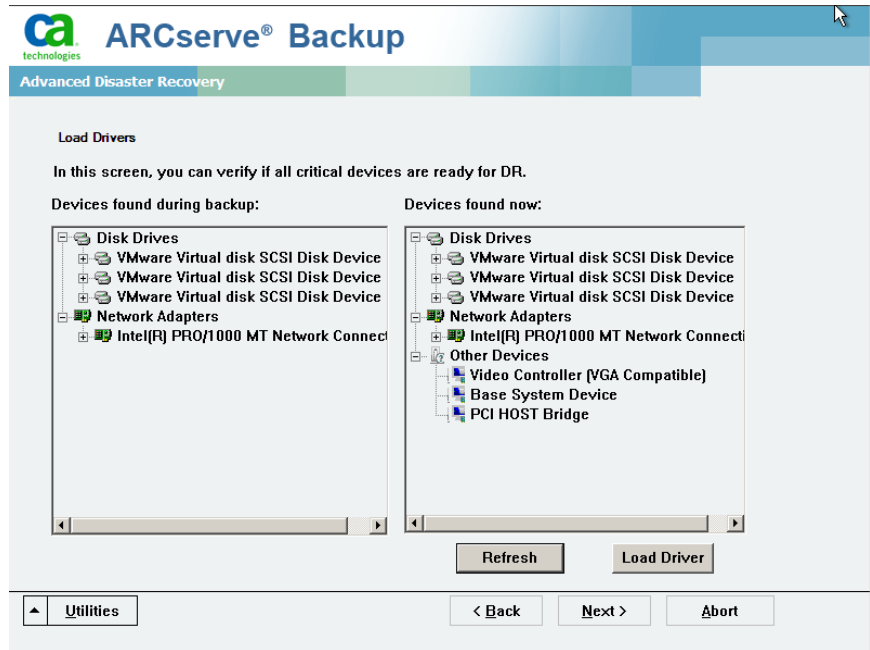
c. Verify the devices and click Next on Load Drivers dialog.

Important! Windows formats the disk after you click Next.

The Network connections dialog opens followed by the Session dialog.
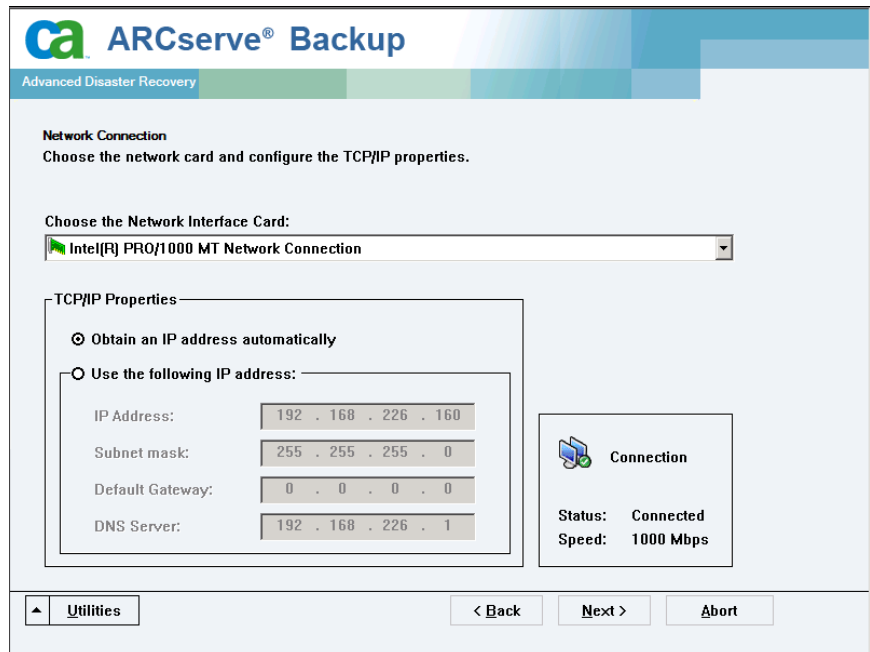
d. Select the session that you want to restore, click Next.

You can enter the password for each session depending on the status of each key at the end of each row in the Session Assign dialog. Types of keys include:

■ When the session has a key option, it means that the session was encrypted by a key, but the key was not saved in the database. You must provide the encryption key to restore these sessions.

■ When the session has a key option with a tick mark, then the session was encrypted by a key or protected by a password and the encryption key or the session password was saved in the database. No encryption key or session password is required to restore these sessions.

■ When the session has a key option with a question mark, then the session password status is unknown. You can enter the session password, if necessary.

The Summary dialog opens.

e. Verify the Summary list.
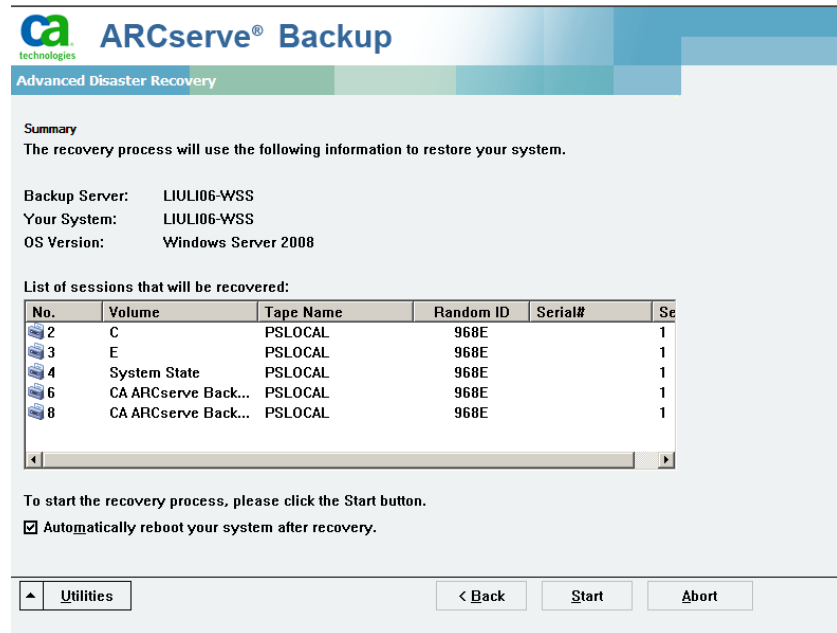
f. Click Start Disaster Recovery to start the process.

The data is copied from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

Note: You can run most of the 32-bit Windows programs, such as regedit.exe, from the DOS prompt window. Click Utilities, and select Run to open a Windows command line console window.

The Disaster Recovery process is complete.

Note: You can use the keyboard shortcut Shift+ r on the Disaster Recovery wizard to reboot.

When the computer restarts, it is restored to the state it was in at the time of the last full backup.

Important! When the Arcserve Backup database is installed on this computer and this computer is not the Arcserve Backup primary server, you must run the Arcserve Database Recovery Wizard at this time. For more information about the Arcserve Database Recovery Wizard, see the topic Recover the Arcserve Backup Database Using Arcserve Database Recovery Wizard in the *Arcserve Backup Administration Guide*.

Note: To run the Install and Reboot options on the Disaster Recovery wizard while using USB backup devices dialogs, use the following keyboard shortcuts:

■ Install—Shift + i

■ Reboot—Shift + r

Chapter 5: Disaster Recovery Scenarios

This section contains the following topics:

Disaster Recovery Scenarios on Windows 2003

The scenarios specified in this section provides system-specific information and procedures to recover a typical Windows 2003 system. The procedure you use to recover a Windows 2003 system is similar to the procedure you use to recover a Windows XP system.

Scenario 1: Primary SAN Disaster Recovery for an HP ProLiant ML330 G3

The Server Specifications (see page 121) scenario uses the ASR-based (Automated System Recovery) disaster recovery process to recover a Arcserve Backup Windows 2003 server.

Server Specifications

In this scenario, the server conforms to the following specifications:

- System: HP ProLiant ML330 G3 with one Xeon 2.8 GHz CPU and 1 GB RAM connected to a StorageTek L20 DLT800 Tape Library through an Emulex LP9000 HBA

- Network Adapter: HP NC7760 Gigabit Server Adapter

- Fiber Environment

  - Emulex LightPulse 9000 PCI Fibre Channel HBA

  - gadzoox Networks slingshot 4218 switch

  - Crossroads 4250 FC Bridge

- Storage

  - Three disks of 36.4 GB connected to a Smart Array 642 Controller

  - First volume configured as RAID level 5 (32.22 GB)

  - Second volume configured as RAID level 5 (35.6 GB)

- Partitions

  - Drive C - 10 GB - disk 0 - system and boot volume (NTFS)

  - Drive E - 22.22 GB - disk 0 - Windows primary (NTFS)

  - Drive F - 20 GB - disk 1 - Windows primary (NTFS)

- Software Environment

  - Microsoft Windows 2003 Enterprise Edition Server

  - Arcserve Backup

  - Arcserve Backup Disaster Recovery Option

  - Arcserve Backup Tape Library Option

  - Arcserve Backup SAN Option

Prepare for Disaster During Primary Server Setup

Planning for a successful disaster recovery begins when you set up your primary server. Perform the following procedure when you install Arcserve Backup and the Disaster Recovery Option on your primary server (HP ProLiant ML330 G3):

1. Note the hardware RAID configuration on your system. In this scenario we have:

   - Three disks of 36.4 GB each, connected to an HP Smart Array 642 Controller

   - First volume configured as RAID level 5 (32.22 GB)

   - Second volume configured as RAID level 5 (35.6 GB)

   This scenario does not use an EISA partition.

   Note: The option does not recreate the hardware RAID volumes. You must recreate the hardware RAID configuration manually during disaster recovery.

2. Add the CD provided by the hardware vendor (used to create the RAID volumes) to the disaster recovery kit for this primary server. In this scenario, it is the HP SmartStart CD release 6.40.

3. Save the extra hardware drivers you installed (by pressing F6) when you set up your ML330 G3 Windows 2003 server. Add these disks to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery. In this scenario, we save the Emulex LP9000 PCI Fibre Channel HBA driver and the HP Smart Array 642 Controller driver to disk.

   Note: If you do not know the devices installed on the Windows primary server, look in the Device Manager. If your system is no longer up and running, open the CardDesc.txt file on the machine-specific recovery disk to view a summary of the devices and drivers.

4. Start Arcserve Backup and perform a full backup.

Disaster Recovery Prerequisites

To begin disaster recovery, you must have all of the following items:

- Arcserve Backup machine-specific recovery disk. For more information, see section "Disaster Recovery Methods on Windows Server 2003 and Windows XP (see page 55)".

- A full backup of the ML330 G3 primary server

- Windows 2003 Server distribution CD

- HP SmartStart CD release 6.40

- The original hardware RAID configuration

- Arcserve Backup for Windows distribution CD

- Emulex LP9000 PCI Fibre Channel HBA driver disk

- HP Smart Array 642 Controller driver disk

Recover from Disaster

You can recover your server after a disaster using the following procedure.

To recover your Windows 2003 system after a disaster

1. Boot the primary server (HP ProLiant ML330 G3) using the HP SmartStart CD release 6.40.

2. Follow the HP guidelines to recreate the hardware RAID configuration.

3. Boot the primary server using the Windows 2003 Server distribution CD and follow the on-screen ASR instructions. For more information about Disaster Recovery, see section "Disaster Recovery Methods on Windows Server 2003 and Windows XP (see page 55)."

4. Press F6 to enable the addition of the SCSI or RAID drivers required, using the device driver floppy disks

5. Press F2 to begin the Windows ASR process

6. When prompted to insert the Windows ASR Disk, insert the Arcserve Backup machine-specific recovery disk created for the ML330 G3 server and press Enter.

7. The option loads a temporary Windows operating system, including the necessary SCSI and RAID drivers you enabled by pressing the F6 key in a previous step. The ASR process may prompt you to insert the disks to install the hardware drivers.

   In this scenario, we insert the disks and load the drivers for the HP Smart Array 642 Controller and the Emulex LP9000 PCI Fibre Channel HBA.

8. After Windows has loaded the drivers, insert the machine-specific recovery disk again. The option reads the original system disk configuration from the machine-specific recovery disk.

9. The ASR process evaluates the available disk configuration. If ASR requires you to recreate disk partitions, a recovery process screen appears. Press C to recreate your disk partitions or press F3 to quit. If you are not recreating disk partitions, this screen does not appear.

   The Windows ASR disaster recovery bluescreen mode finishes and the computer reboots.

10. The Windows Install screen appears. The option performs installation tasks for the ASR process. When these tasks are complete, the Disaster Recovery Wizard appears. Follow the instructions in the Disaster Recovery Wizard.

    The Disaster Recovery Wizard installs the Arcserve Backup files and services and connects to the Arcserve Backup backup server over the network.

11. When prompted, start the data restore operation.

12. At the end of the data restore process, boot back to your original system.

Scenario 2: Primary SAN Advanced Disaster Recovery for an HP ProLiant ML330 G3

The Server Specifications (see page 125) scenario uses the ASR-based (Automated System Recovery) advanced disaster recovery process to recover a Arcserve Backup Windows 2003 server.

Server Specifications

In this scenario, the server conforms to the following specifications:

- System: HP ProLiant ML330 G3 with one Xeon 2.8 GHz CPU and 1 GB RAM connected to a StorageTek L20 DLT800 Tape Library through an Emulex LP9000 HBA

- Network Adapter: HP NC7760 Gigabit Server Adapter

- Fiber Environment

  - Emulex LightPulse 9000 PCI Fibre Channel HBA

  - gadzoox Networks slingshot 4218 switch

  - Crossroads 4250 FC Bridge

- Storage

  - Three disks of 36.4 GB connected to a Smart Array 642 Controller

  - First volume configured as RAID level 5 (32.22 GB)

  - Second volume configured as RAID level 5 (35.6 GB)

- Partitions

  - Drive C - 10 GB - disk 0 - system and boot volume (NTFS)

  - Drive E - 22.22 GB - disk 0 - Windows primary (NTFS)

  - Drive F - 20 GB - disk 1 - Windows primary (NTFS)

- Software Environment

  - Microsoft Windows 2003 Enterprise Edition Server

  - Arcserve Backup

  - Arcserve Backup Disaster Recovery Option

  - Arcserve Backup Tape Library Option

  - Arcserve Backup SAN Option

Prepare for Disaster During Primary Server Setup ADR W2003 S1

A successful disaster recovery begins when you set up your primary server. Perform the following procedure when you install Arcserve Backup and the Disaster Recovery Option on your primary server (HP ProLiant ML330 G3):

To prepare for disaster during primary server setup

1. Check the hardware RAID configuration on your system. In this scenario we have:

    ■   Three disks of 36.4 GB each, connected to an HP Smart Array 642 Controller

    ■   First volume configured as RAID level 5 (32.22 GB)

    ■   Second volume configured as RAID level 5 (35.6 GB)

    This scenario does not use an EISA partition.

    Note: The option does not recreate the hardware RAID volumes. You must recreate the hardware RAID configuration manually during disaster recovery.

2. Add the CD provided by the hardware vendor (used to create the RAID volumes) to the disaster recovery kit for this primary server. In this scenario, it is the HP SmartStart CD release 6.40.

3. Save the extra hardware drivers you installed (by pressing F6) when you set up your ML330 G3 <win> 2003 server. Add these disks to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery. In this scenario, we save the Emulex LP9000 PCI Fibre Channel HBA driver and the HP Smart Array 642 Controller driver to disk.

    Note: If you do not know the devices installed on the <win> primary server, look in the Device Manager. If your system is no longer up and running, open the CardDesc.txt file on the machine-specific recovery disk to view a summary of the devices and drivers.

    Start Arcserve Backup and perform a full backup.

Disaster Recovery Prerequisites

To begin disaster recovery, you must have all of the following items:

■   Arcserve Backup machine-specific recovery disk

■   A full backup of the ML330 G3 primary server

■   <win> 2003 Server distribution CD

■   HP SmartStart CD release 6.40

■   The original hardware RAID configuration

■   Arcserve Backup for <win> distribution CD

■   Emulex LP9000 PCI Fibre Channel HBA driver disk

■   HP Smart Array 642 Controller driver disk

Recover <win> 2003 from Disaster

You can recover the Windows 2003 server from a disaster using the following procedure

To recover your Windows 2003 system after a disaster

1. Boot the primary server (HP ProLiant ML330 G3) using the HP SmartStart CD release 6.40.

2. Follow the HP guidelines to recreate the hardware RAID configuration.

3. Boot the primary server using the Windows 2003 Server distribution CD and follow the on-screen ASR instructions.

4. Press F6 to enable the addition of the SCSI or RAID drivers required, using the device driver floppy disks.

5. Press F2 to begin the Windows ASR process

6. When prompted to insert the Windows ASR Disk, insert the Arcserve Backup machine-specific recovery disk created for the ML330 G3 server and press Enter.

7. The option loads a temporary Windows operating system, including the necessary SCSI and RAID drivers you enabled by pressing the F6 key in a previous step. The ASR process may prompt you to insert the disks to install the hardware drivers.

   In this scenario, we insert the disks and load the drivers for the HP Smart Array 642 Controller and the Emulex LP9000 PCI Fibre Channel HBA.

8. After Windows has loaded the drivers, insert the machine-specific recovery disk again. The option reads the original system disk configuration from the machine-specific recovery disk.

9. The ASR process evaluates the available disk configuration. If ASR requires you to recreate disk partitions, a recovery process screen appears. Press C to recreate your disk partitions or press F3 to quit. If you are not recreating disk partitions, this screen does not appear.

   The Windows ASR advanced disaster recovery bluescreen mode finishes and the computer reboots.

10. The Windows Install screen appears. The option performs installation tasks for the ASR process. When these tasks are complete, the Advanced Disaster Recovery Wizard appears. Follow the instructions in the Advanced Disaster Recovery Wizard.

    The Advanced Disaster Recovery Wizard installs the Arcserve Backup files and services and connects to the Arcserve Backup backup server over the network.

11. When prompted, start the data restore operation.

    At the end of the data restore process, boot back to your original system.

Disaster Recovery Scenario on Windows XP

The scenarios specified in this section provides system-specific information and procedures to recover a typical Windows XP system. The procedure used to recover a Windows XP system is similar to the procedure used to recover a Windows 2003 system.

Scenario 1: Remote Disaster Recovery for a Dell PowerEdge 1600SC

The scenarios specified in this section uses the Automated System Recovery (ASR)-based disaster recovery process to recover a Arcserve Backup Windows XP client.

Client Specifications

In this scenario, the client conforms to the following specifications:

- System: Dell PowerEdge 1600SC with a dual-processor Xeon 2.00 GHz CPU and 1.99 GHz and 1 GB RAM

- Network Adapter: Intel Pro based PCI Ethernet Adapter

- Storage

  - Three disks of 34.6 GB connected to a PERC 4/SC single channel U320 RAID controller

  - One logical disk configured as RAID level 0 (103.6 GB)

- Partitions

  - Drive C - 68.3 GB - disk0 - system and boot volume (NTFS)

  - Drive D - 32.8 GB - disk0 - data volume (NTFS)

- Software Environment

  - Microsoft Windows XP Professional, Service Pack 1a

  - Arcserve Backup Client Agent for Windows

Note: Although we have not done so in this scenario, you can also configure the client computer with an EISA partition.

Server Specifications

In this scenario, the server conforms to the following specifications:

- System: HP tc3100 server connected to a Quantum SDLT changer through an Emulex LP9000 adapter

- Software Environment

    - Arcserve Backup

    - Arcserve Backup Disaster Recovery Option

    - Arcserve Backup Agent for Open Files

    - Arcserve Backup Diagnostic Utility

Prepare for Disaster During Client Computer Setup

Planning for a successful disaster recovery begins when you set up your client computer. Perform the following procedure when you install the Client Agent for Windows on your client computer (Dell PowerEdge 1600SC):

1. Note the hardware RAID configuration and EISA partition (if one exists) on your system. In this scenario we have the following:

    - Three disks of 34.6 GB each, connected to a PERC 4/SC single channel U320 RAID controller

    - One logical disk configured as RAID level 0 (103.6 GB)

    Note: The option does not recreate the hardware RAID volumes. You must recreate the hardware RAID configuration manually during disaster recovery.

2. Add the CD provided by the hardware vendor (used to create the RAID volumes) to the disaster recovery kit for this primary server. In this scenario, we add the DELL Server Assistant version 7.5 Bootable CD.

3. Save the extra hardware drivers you installed (by pressing F6) when you set up your 1600SC Windows XP client. Add these disks to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery. In this scenario, we save the PERC 4/SC single channel U320 RAID controller.

    Note: If you do not know the devices installed on the Windows server, look in the Device Manager. If your system is no longer up and running, open the CardDesc.txt file on the machine-specific recovery disk to view a summary of the devices and drivers.

4. Add the Windows client computer (Dell PowerEdge 1600SC) to the Arcserve Backup server and perform a full backup.

Disaster Recovery Prerequisites

To begin disaster recovery, you must have all of the following items:

- Arcserve Backup machine-specific recovery disk. For more information see section "Disaster Recovery Methods on Windows Server 2003 and Windows XP (see page 55)".

- A full backup of the 1600SC client

- Windows XP distribution CD

- Dell Server Assistant version 7.5 Bootable CD

- The original hardware RAID configuration

- Arcserve Backup for Windows distribution CD

- The PERC 4/SC single channel U320 RAID controller driver disk

Recover from Disaster

To recover from a disaster, perform the following procedure. The first two steps form the Dell Server Assistant version 7.5 Bootable CD Setup process, and the remaining steps form the Windows XP ASR boot process:

To recover from a disaster

1. Boot the client computer (Dell PowerEdge 1600SC) using the Dell Server Assistant version 7.5 Bootable CD.

    Note: Follow the Dell guidelines to recreate the hardware RAID configuration.

2. Boot the client computer using the Windows XP distribution CD and follow the on-screen ASR instructions. For more information on Disaster Recovery, see section "Disaster Recovery Methods on Windows Server 2003 and Windows XP (see page 55)".

3. Press F6 to enable the addition of the SCSI or RAID drivers required, using the device driver floppy disks.

4. Press F2 to begin the Windows ASR process.

    You will be prompted to insert Windows ASR disk.

5. When prompted to insert the Windows ASR disk, insert the Arcserve Backup machine-specific disk and press Enter.

    The option loads a temporary Windows operating system, including the necessary SCSI and RAID drivers enabled by pressing the F6 key in a previous step.

6. The ASR process may prompt you for the disks to install the hardware drivers. In this scenario, we insert the disk and load the driver for the PERC 4/SC single channel U320 RAID controller.

7. After Windows loads the driver, insert the machine-specific disk again. The option reads the original system disk configuration from the machine-specific recovery disk.

8. The ASR process evaluates the available disk configuration.

    If ASR requires you to recreate disk partitions, a recovery process screen appears.

9. Press C to recreate your disk partitions or press F3 to quit. This screen does not appear if disk partitions are not being recreated.

    The Windows ASR disaster recovery bluescreen mode finishes and the computer reboots.

    Note: You may be prompted to insert the CADRIF disk. This is the machine-specific recovery disk.

    The Windows Install dialog appears.

10. You can perform the installation tasks for the ASR process.

    When these tasks are complete, the disaster recovery wizard appears.

11. Follow the instructions in the disaster recovery wizard.

    The wizard installs the Arcserve Backup files and services and connects to the Arcserve Backup backup server over the network.

12. When prompted, start the data restore operation.

13. At the end of the data restore process, boot back to your original system.

Disaster Recovery Scenarios on Windows Server 2008

The scenarios specified in this section provides information and procedures to recover a typical system. The procedure you use to recover a Windows Server 2003 system, is similar to the procedure you use to recover a Windows Server 2008 system.

Scenario 1: Primary Server Disaster Recovery

The scenario specified in this section lets you recover a primary server in the SAN environment.

Prepare for Disaster During Primary Server Setup

Planning for a successful disaster recovery begins when you set up your primary server. Perform the following procedure when you install Arcserve Backup and the Disaster Recovery Option on your primary server.

To prepare for disaster during primary server setup

1. Add the Windows Server 2008 installation media to the disaster recovery kit for this primary server.

2. Save the additional hardware drivers you installed when you set up your primary server. Add these drivers to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery.

   Note: If you do not know the devices installed on the Windows primary server, look in the Device Manager. If your system is no longer up and running, open the CardDesc.txt file on the machine-specific recovery disk to view a summary of the devices and drivers.

3. Start Arcserve Backup and perform a full backup.

Disaster Recovery Prerequisites

To begin disaster recovery, you must have all of the following items:

- Arcserve Backup machine specific recovery disk

- A full backup of the primary server

- Windows Server 2008 installation media

- Arcserve Backup Disaster Recovery CD

- Driver disk

Recover Primary Server

You can recover a primary server from a disaster using the following procedure:

To recover your system after a disaster

1. Insert the machine specific recovery disk into the machine.

2. Boot the primary server using the Windows Server 2008 installation media.

3. Insert the Arcserve Backup Disaster Recovery media, when prompted and click Next.

   Note: You must specify the machine specific disk data for restore as multiple machine specific disk data is stored in the disk storage media.

4. On the driver page, load the drivers.

5. Click Next to view the Network configuration screen.

   In Advanced mode, give the network configuration details for the remote Disaster Recovery. Network configuration is also required for the local Disaster Recovery for SAN member server and local Disaster Recovery using remote file system devices.

6. Configure the remote file system devices page. Enter the authentication details, if necessary.

   The session list opens.

7. You can make changes to this list and click Next.

   The Summary page appears listing the sessions that you want to restore. Click Next and follow the instructions.

8. The restore process begins.

   Reboot the machine after the restore process is complete.

Appendix A: Troubleshooting

This appendix provides troubleshooting information that you may need while using the Disaster Recovery Option. To help you find the answers to your questions quickly, the information in this appendix is divided into the following categories and, where appropriate, each category is further divided into questions and answers for specific operating systems:

■ General usability

■ Hardware

■ Operating systems

■ Utilities

This section contains the following topics:

General Usability

This section provides answers to frequently asked questions about using the option to perform disaster recovery.

All Windows Platforms

The information in this section applies to all supported Windows platforms.

Error Messages Appear in the Windows Event Log that Relate to the Arcserve Database-DRW

Valid on Windows Server 2003 and Windows Server 2008

Symptom

When you recover an Arcserve server that is running Windows Server 2003 from a disaster using the bootable CD method, the operating system records many error messages to the Windows Event Log that relate to the Arcserve database. The details of the error messages that are most like to appear are as follows:

- **Error codes:** 8355, 17204, and 17207

- **Instance:** MSSQL$ARCSERVE_DB

Solution

The process of recovering the Arcserve database causes these events occur. You can ignore the error messages.

Full System Backup

Symptom

What constitutes a full system backup for disaster recovery purposes?

Solution

If a computer is designated for a full backup, the selection box for the computer is solid green. This applies to both a local backup and a remote backup using Arcserve Backup for Windows.

System Configurations to Avoid Disaster Recovery

Symptom

What system configurations should I avoid for disaster recovery?

Solution

You should avoid the following configurations:

Windows 2003 and Windows XP:

You should avoid making the boot disk of the system a dynamic disk.

Windows XP and Windows 2003:

You should avoid creating FAT partitions over 2 GB. These partitions are not restored by ASR.

Restore of Incremental and Differential Backups

Valid on Windows 2003 and Windows XP

Symptom

Every time I perform an incremental/differential backup, should I store the sessions in the same media as the full backup?

Solution

The full and incremental / differential sessions can reside on different media or same media. You can create a machine specific disk (MSD) after all backups are run or after every incremental /differential backup.

Perform the disaster recovery process, as you would do normally. The Disaster Recovery Option will not automatically scan any additional sessions created after creation of this MSD. The MSD would have information about all backups (full and incremental / differential) that were performed before MSD was created. The Disaster Recovery Option would now automatically restore all the full sessions and incremental /differential sessions recorded in this MSD.

Perform Incremental and Differential Backups

Symptom

After performing full backup of the server, I schedule incremental and differential backups of the full server. Is this backup information recorded in the machine- specific recovery disks (MSDs)? Can I recover these incremental and differential backup sessions during disaster recovery?

Solution

Windows 2003

Yes. The incremental and differential backup sessions of full node backups are recorded in the MSDs along with the full backups. During disaster recovery, you can select the sessions you want to restore.

Local DR using Remote FSD

Valid on Windows XP, Windows 2003, and Windows 2008

Symptom

I have backed up the Arcserve Backup server to a remote file system device. During disaster recovery, can I access the remote file system device and restore the backup data from it?

Solution

Yes. The file system device configuration is recorded in machine specific disk and you can restore the backup data while performing disaster recovery. Disaster Recovery Option retrieves this and handles the connection automatically.

If there is any change in the authentication information of the server on which the file system device is located, disaster recovery prompt you to enter the new account and password for authentication.

Additional Drivers

Symptom

Should I add extra drivers during the disaster recovery procedure? Why doesn't the disaster recovery process detect my SCSI, Fiber, and RAID adapters?

Solution

Mid to high-range servers typically require drivers for RAID and SCSI adapters. The option uses these drivers to access the disks and storage devices in the system. Without these drivers, the option may not function properly.

If you are using a system that requires proprietary drivers for the SCSI, fiber, and RAID cards, it is possible that the drivers are not on the operating system CD. In this case, it is possible that the disaster recovery process cannot detect or load the drivers.

If you have a copy of the proper SCSI, FIBRE, or RAID drivers on a disk, you can reboot using the disaster recovery disks, and add the drivers when prompted. You can add these drivers during the bluescreen mode of disaster recovery by pressing F6. You should update the drivers for adapters provided on the Windows installation CD, in the event the Windows CD versions were updated by the manufacturer. This is particularly important for fiber adapters.

Disaster Recovery from a Different Server

Symptom

Can I perform disaster recovery from a Arcserve Backup server other than the server from which the backup was performed?

Solution

Yes, as long as the media can be used by the new server and new server information is present on the machine-specific recovery disk.

Windows XP and Windows 2003:

You can perform disaster recovery from a different server using the Advanced Disaster Recovery wizard by entering the server details and the IP address, when prompted.

Remote Computer Backup Over a Network

Symptom

Can I use the option to back up remote computers over the Network?

Solution

The Disaster Recovery Option is only supported over the network when the Client Agent for Windows is installed on the remote Windows computer.

Ghost Application Duplicating System Configuration

Symptom

Can I use disaster recovery as a "ghost" application to duplicate my system configuration?

Solution

No. The option is a system restoration application, not a system configuration replication program. Do not use the option to replicate systems.

Remote Disaster Recovery Cannot Use Local Backups

Symptom

Can I use a local backup to perform a remote disaster recovery?

Solution

You cannot use local backups for remote disaster recovery, nor can you use remote backups for local disaster recovery.

Specific Session Restoration

Symptom

Can I restore specific sessions during the disaster recovery process?

Solution

Yes. You can do this by un-assigning sessions from volumes you do not want to restore. Using the disaster recovery process, you can choose specific sessions that you want to restore.

Note: The system may not boot after disaster recovery if you do not restore the operating system volumes or other volumes critical for booting the system.

Machine-Specific Disk Update

Symptom

How can I update the machine-specific recovery disk if my Arcserve Backup server fails?

Solution

You can update a machine-specific recovery disk if you configured an alternate location during installation or after installing the option and before performing a full backup.

To update a machine-specific recovery disk on a backup server, access the alternate location and copy the contents of the folder representing the server that you want to recover to a blank disk. This is your machine-specific recovery disk for the failed server. If the failed server contains Windows Server 2003, you must also copy the contents of the DRPATCH.XP folder to the new disk.

To achieve the highest level of disaster recovery support, you should set up an alternate location for disaster recovery during installation or immediately after installing the option.

EISA Partition Restoration

Symptom

Can the option restore the EISA (Utility) partition on my server?

Solution

No. The option does not back up EISA partitions. Therefore, the option cannot recover these partitions using the disaster recovery process. You must recreate these partitions manually. Use the CD or disks provided by the hardware vendor to recreate these partitions.

Alternate Location Reconfiguration

Symptom

How do I reconfigure or set up an alternate location after the option has been set up?

Solution

In the Create Boot Kit wizard, click the Config button at the bottom of the screen.

File Sharing Violations

Symptom

If I receive file-sharing violations during a backup operation, can I still use sessions from that tape for disaster recovery?

Solution

Yes, you can use these sessions for disaster recovery if you did not deselect anything from the drive for the backup.

Note: The backup operation does not back up open files. Therefore, these files cannot be restored during the disaster recovery process.

Major Hardware or Software Upgrades

Symptom

What should I do if I install a different operating system or NIC card, or change between hardware and software RAID?

Solution

When you perform a major system upgrade (hardware or software), you should delete the machine-specific directory for that system on both the Arcserve Backup home DR directory and alternate location. After completing these tasks, perform a full system backup.

Indicating Backup can be used for DR

Symptom

How can I know if I can recover the full node backup data using the licensed Disaster Recovery Option installed on my machine?

Solution

You can recover the full node backup data using Disaster Recovery Option if the following information is logged in the Activity log after the full node backup is finished:

Information   HOSTNAME   MM/DD/YYYY HH:MM:SS JobID
Successfully Generated Disaster Recovery Information for TEST05-W2K3-VM

Unable to Detect Second Sequence Tape, when Restoring from a Tape Drive

Symptom

I perform disaster recovery using a stand alone tape drive. After tape span, when I insert the next sequence tape into the drive and click OK on the mount tape pop-up dialog, Disaster Recovery Option still asks for the next sequence tape?

Solution

This error occurs because the driver of that tape drive that is installed in the operating system accepts the media change notice from hardware directly because of which Arcserve Backup fails to detect the media change event.

To detect the second sequence tape

1.   Eject the sequence 2 tape.

2.   Click OK on the Mount Tape popup dialog.

3.   Insert the sequence 2 tape.

4.   Click OK on the Mount Tape popup dialog again.

Manual Changes to Disk Configuration During Disaster Recovery

Symptom

Can I change partition information during disaster recovery?

Solution

No. If the disk configuration is changed manually during the disaster recovery, you may not be able to restore the system.

Raw Partition Restoration

Symptom

Can I back up and restore raw partitions using disaster recovery?

Solution

No. The option does not support restoration of raw partitions.

Use Locally Attached Disk

Symptom

Can I use a locally attached disk to perform a file system backup and a disaster recovery of the backup server?

Solution

Performing a disaster recovery of a backup server using a locally attached file system device is supported only if all of the following criteria are met:

- The backup server is running Windows 2003

- The disks containing the file system device do not contain the boot partition

- The disks containing the file system device do not contain the system (Windows) partition

- The disks containing the file system device are not corrupted or damaged

- The disks containing the file system device provide, unchanged, the following properties:

  - Partition layout

  - Volume information (for example, drive letter, file system, or label)

  - Disk signature

Note: We strongly recommend that you also maintain a tape backup that can be used if the backup on the file system device is damaged during a disaster. If you use a local disk as a backup device, run a test of the disaster recovery process before deploying it in a production environment.

Back Up English Client Machine from Non-English Server

Symptom

My Backup Server is installed on a non-English Windows platform and I use it to backup a client machine running on English Windows platform. When I try to perform disaster recovery on the English client machine, I am getting some error messages saying the backup tape media cannot be found and the DR wizard keeps asking me to mount the tape. I am very sure the tape is mounted. What can be wrong?

Solution

The problem is caused by difference in the ANSI code page used by the backup server and the client machine. If the tape being used has non-English text name, the recovery process may not able to locate the tape media correctly. In general, The Disaster Recovery Option does not completely support cross-language Windows environment. If you have to backup an English Windows client machine using an non-English backup server, make sure the backup media using used does not contain any non-English character in the name.

DNS Record

Symptom

What should I do if the Disaster Recovery machine is unable to connect to the Arcserve Backup server?

Solution

If you have not updated the Arcserve Backup server's Domain Name Server record, the Disaster Recovery machine cannot connect to the Arcserve Backup server. To avoid this problem, add the correct IP address in the hosts file.

Windows ASR cannot restore the disk partition layout for multi-path SAN disk

Valid on Windows Server 2003 platforms

Symptom

While performing restore operation, Windows ASR cannot restore the disk partition layout for multi-path SAN disk.

Solution

During disaster recovery, Windows ASR cannot map the disk and restore the partition correctly. You can only restore the disk partition layout for a single-path SAN disk.

ASDB Sessions Cannot be Restored

Symptom

Arcserve Database Recovery wizard fails to find a backup device and gives the error "Please mount the media <media name>", the media name is the media on which SQL server was backed up.

Solution

After disaster recovery, the Database Recovery Wizard will be automatically launched to help you recover ASDB. During this procedure, it may fail to find a backup device this happens because the backup device was not included during full machine backup. You can perform the following steps:

To restore an ASDB session

1. Recover ASDB from Arcserve Database Recovery Wizard using the Media1 on which full machine backup was taken.

2. You must restore master, msdb, model and user databases manually from Media1 using the Restore Manager.

3. Create a Media2 and point to the location where the SQL server session was backed up.

4. Merge the Media2.

5. Then, restore the user databases manually from Media2 to recover the SQL database to the latest point.

Note: For more information about the Arcserve Database Recovery Wizard, see the topic Recover the Arcserve Backup Database Using Arcserve Database Recovery Wizard in the *Arcserve Backup Administration Guide*.

Hardware

This section provides answers to frequently asked questions related to hardware.

Windows 2003 and Windows XP

The information in this section applies to Windows 2003 and Windows XP platforms.

Multiple Connections to the Same Device

Symptom

I have two or more fibre channel adapters on the server connecting to the same SAN network for fault tolerance purposes. When I try to recover the server using the disaster recovery process, the disaster recovery fails with tape engine errors. What should I do?

Solution

By default, the disaster recovery process treats all storage devices as separate and distinct devices. Having multiple connections to the same device would cause the disaster recovery process to initialize the same device on multiple occurrences causing the error. To alter this default behavior, you must add a signature file labeled **redconn** to the machine-specific recovery disk.

To create the signature file, perform the following steps

1. Use the Create Boot Kit Wizard to create a machine-specific recovery disk for the server with multiple fibre channel adapters.

2. Create a new file, called **redconn,** on the machine-specific recovery disk. The size of the file should be zero.

3. Perform disaster recovery for the server using the machine-specific recovery disk containing the signature file.

How to Add an OEM Network Adapter Driver to a RIS Installation

Valid on Windows Server 2003 and Windows XP

Symptom

Adding a network adapter that requires an OEM driver to a CD-ROM-based RIS image involves some of the steps as adding such a driver to a typical unattended installation. However, because the installation method begins by using Pre-Boot eXecution Environment (PXE) and then switches over to using the Server Message Block (SMB) protocol, the network adapter driver and its .inf file must be available during text-mode setup. If the driver and the .inf file are not available, you receive the following error message:

The network server does not support booting Windows 2003. Setup cannot continue. Press any key to exit.

When a PXE client that is running Client Installation Wizard (CIW) connects to an RIS server, the network adapter is using Universal Network Device Interface to communicate with the RIS server. When Windows Setup switches to SMB, the network adapter is detected, and the appropriate driver is loaded. Therefore, the driver must be available.

Solution

You can add the OEM network adapter to the RIS image.

Do the following:

Check with the OEM to determine whether the supplied network adapter driver is digitally signed. If the drivers from the manufacturer contain a catalog (.cat) file, they are properly signed. Drivers signed by Microsoft have been verified and tested to work with Windows. If your driver has not been signed but you still want to use it, make sure to add the following unattended-setup parameter to the .sif file that is located in the RemoteInstall\Setup\Language\Images\Dir_name\I386\Templates folder: [Unattended]

DriverSigningPolicy = Ignore

Note: If the OEM driver is an update of an included Windows XP driver (for example, if the drivers have the same name), the file must be signed or else Setup uses the included driver instead.

1. On the RIS server, copy the OEM-supplied *.inf* and *.sys* files for the network adapter to the **RemoteInstall\Setup\Language\Images\Dir_name\i386** folder. This allows Setup to use the driver during the text-mode portion of the installation.

2. At the same level as the i386 folder on the RIS image, create a oem folder. Use the following structure:

\$oem$\$1\Drivers\Nic

3. Copy the OEM-supplied driver files to this folder. Note the folder in which the .inf file looks for its drivers. Some manufacturers place the .inf file in a folder and copy the driver files from a subfolder. If this is the case, create the same folder structure below the one you created in this step.

4. Make the following changes to the *.sif* file that is used for this image installation:

   [Unattended]
   OemPreinstall = yes
   OemPnpDriversPath = \Drivers\Nic

5. Stop and then restart the Remote Installation service (BINLSVC) on the RIS server. To do this, type the following commands at the command prompt and press **Enter** after each command:

   net Stop binlsvc
   net Start binlsvc

   Note: You must stop and restart the Remote Installation Service because the Boot Information Negotiation Layer (BINL) needs to read all the new network adapter-related .inf files and create .pnf files in the image. This is a time-consuming task and is performed only when the Remote Installation Service starts.

If you have multiple network adapters that require OEM drivers, follow the preceding steps for each adapter. However, the PXE clients that have included network adapter drivers are unaffected by these changes and can use this image for installation.

Add an OEM SCSI/RAID/SCSI Driver When Setup Fails

Valid on Windows Server 2003 and Windows XP

Symptom

If your machine boots from a hard disk which connects to an OEM SCSI adapter, the setup will fail. So, to use RIS to set up computer nodes you must add the OEM SCSI adapter mode drivers to the RIS image.

Solution

This procedure is specifically for an Adaptec AAR-1420SA SATA HostRAID driver, but you can use it when other drivers are required.

To add an OEM SCSI/RAID/SCSI driver to a RIS image

1. Click Install RIS, as a section of the Cluster Deployment Tasks involves RIS.

    The Remote Installation Services Wizard appears on your server.

2. Click Manage Images and choose Add New Image.

    For client support, you typically check Respond to client computers requesting service.

3. Click Manage Images a second time and select Modify Image Configuration to add your image key.

    The mass storage drivers are only copied during the Text Mode portion of the compute node setup through RIS. You need to add an OEM\TEXTMODE folder to the image. Your folder structure should look like this:

    %RIS_IMAGE_FOLDER%\amd64 (this folder already exists)
    %RIS_IMAGE_FOLDER%\i386 (this folder already exists)
    %RIS_IMAGE_FOLDER%\OEM (create this folder)
    %RIS_IMAGE_FOLDER%\$OEM$TEXTMODE (create this subfolder)

    Note: %RIS_IMAGE_FOLDER% is the folder which holds the RIS image on the head node. This folder might be similar to this:

    D:\RemoteInstall\Setup\English\Images\WINDOWS

4. Copy the setup files from the driver disk to the TEXTMODE folder.

    In this example, there are four files:

    %RIS_IMAGE_FOLDER%\$OEM$TEXTMODE\txtsetup.oem
    %RIS_IMAGE_FOLDER%\$OEM$TEXTMODE\aar81xx.inf
    %RIS_IMAGE_FOLDER%\$OEM$TEXTMODE\aar81xx.sys
    %RIS_IMAGE_FOLDER%\$OEM$TEXTMODE\aar81xx.sys

    TXTSETUP.OEM, which was copied in the previous step, must be edited to reflect this new path for the drivers. In the [Disks] section, modify disk1 (or d1) to reflect the new path. In the example below, the original entry is commented out and a new entry added:

[Disks]

d1 = "Adaptec AAR-1420SA Serial ATA HostRAID Driver for Windows x64 Edition (EM64T/AMD64)",
\hraidsk1, \amd64

d1 = "Adaptec AAR-1420SA Serial ATA HostRAID Driver for Windows x64 Edition (EM64T/AMD64)", \, \

Note: When you run an unattended installation using a small computer system interface (SCSI) controller with a manufacturer's drives, you may receive the following error message: Illegal or missing file types specified in section Files.SCSI.name. This behavior might occur because the line in the Txtsetup.oem file under the [Files.SCSI.name] heading is not a supported file type for a SCSI.

For example, if you found an unsupported file type (such as a .dll), in the [Files.SCSI.name] section, you must remove the line.

5.   Edit the file RISTNDRD.SIF to indicate that a mass storage driver must be installed with the operating system and the location of the required files. This file is located in the %RIS_IMAGE_FOLDER%\amd64\Templates folder. Add the lines shown below the comment "# Add these lines." The name used in the [MassStorageDrivers] section should correspond to the name given in the [SCSI] section of TXTSETUP.OEM. After editing, save the file.

[data]
floppyless="1"
msdosinitiated="1"
OriSrc="\\%SERVERNAME%\RemInst\%INSTALLPATH%\%MACHINETYPE"
OriTyp="4"
LocalSourceOnCD=1
DisableAdminAccountOnDomainJoin=1
[SetupData]
OsLoadOptions="/noguiboot /fastdetect"
SetupSourceDevice="\Device\LanmanRedirector\%SERVERNAME%\RemInst\%INSTALLPATH%"
[Unattended]
OemPreinstall=yes
FileSystem=LeaveAlone
ExtendOEMPartition=0
TargetPath=\WINDOWS
OemSkipEula=yes
InstallFilesPath="\\%SERVERNAME%\RemInst\%INSTALLPATH%\%MACHINETYPE%"
LegacyNIC=1
UnattendMode=FullUnattended
WaitForReboot=no
#Add these lines
OemPnPDriversPath="\\%SERVERNAME%\RemInst\%INSTALLPATH%\OEM\textmode"
DUDisable=no
DriverSigningPolicy=ignore
[MassStorageDrivers]
"Adaptec HOSTRAID driver for Windows XP/2003 x64 Edition"="OEM"
[OEMBootFiles]
aar81xx.cat
aar81xx.inf
aar81xx.sys

txtsetup.oem

6. Stop and restart the RIS service on the head node by typing the following at a command prompt:

net stop binlsvc

net start binlsvc

Windows Server 2008 Cannot Communicate While Recovering from a Disaster

Valid on Windows Server 2008 systems.

Symptom

When you recover Windows Server 2008 systems from a disaster using a machine specific disk (MSD), Windows installation media, or both, that contain integrated network interface card (NIC) drivers, the NIC becomes unavailable to the disaster recovery process. As a result, the disaster recovery fails and Arcserve Backup displays a message "Cannot connect to remote media."

Solution

This behavior occurs when you perform disaster recovery using Windows installation media, an MSD, or both, that contain NIC drivers that require you to restart the computer to install the NIC drivers.

To remedy this problem, do the following:

1. Rename the NIC driver's INF file (from *.inf to *.inf.bak) on the MSD and restart the disaster recovery.

2. If the disaster recovery fails, go to the vendor's web site and download drivers for the NIC that do not require you to restart the computer to install the drivers.

3. After you download the NIC drivers, copy the drivers to a floppy disk or USB thumb drive and attach the media to the computer. Then you can load the drivers manually by clicking the Load driver button on the Load driver page.

Operating Systems

This section provides answers to frequently asked questions related to operating systems.

All Windows Platforms

The information in this section applies to all supported Windows platforms.

Operating System Changes During Disaster Recovery

Valid on all Windows platforms

Symptom

My original system has a Windows 2003 Server Edition operating system. Can I perform disaster recovery using the Windows 2003 Enterprise Server Edition CD?

Solution

No. You should not use a different version of the operating system's CD to perform the disaster recovery process.

Temporary Operating System Partitions

Symptom

What partition should I choose to install the temporary operating system?

Solution

Choose the appropriate partition for your operating system, as follows:

Windows XP and Windows 2003:

For ASR disaster recovery, choose the partition on which the operating system was originally installed.

Command Prompt Access During Disaster Recovery Mode

Symptom

How can I open a command prompt window during the disaster recovery mode?

Solution

Windows XP and Windows 2003:

To open a command prompt in the Advanced Disaster Recovery GUI, click Utilities, and select Run.

Hardware Changes

Symptom

After my server failed, I replaced the hard disk and some outdated hardware. Now, when I run the disaster recovery restoration process, it appears to write everything back to disk, but when I reboot the server I get a bluescreen failure. Why?

Solution

The option is not designed to recover a system on which the hardware has been changed. When you restore a system, it restores all of the previous systems drivers. The option attempts to load the drivers for the old hardware, and, if the driver is incompatible with the new hardware, the operating system fails.

Some hardware changes are permitted, such as audio, video card, and so on. Changes of SCSI/RAID and network cards require special attention.

Cannot Connect to Server Message

Symptom

My remote disaster recovery fails with the message "failed to connect to the server." How can I find out why this happens?

Solution

To determine why the message "failed to connect to the server" was generated, perform the following steps:

To ensure the remote disaster recovery works

1. Open a command prompt window and ping 127.0.0.1 and localhost.

   If this fails, the protocol stack was not installed. Install the protocol stack.

2. Ping any computer in your sub-network. If this fails, perform the following:

   a. Check physical connectivity of the ethernet cable.

   b. Run ipconfig and check if the IP address and subnet mask are working for each adapter.

    c. If there is more than one network adapter, check that each network adapter is connected to the proper network cable.

    d. If you are restoring to a different system, the media access control (MAC) address of the network adapters may have changed between the backup and restore system. The option uses the MAC addresses to assign IP addresses saved during backup. Therefore, IP addresses may be assigned to the wrong network adapter. Use ipconfig to obtain the MAC address of the new adapters.

    Now you can replace the old MAC address stored in the network configuration file with the new MAC address.

      ■ **For Windows XP/2003/2008**

      You must modify the network configuration file using a plain text editor. Open file AdrNet.ini on the MSD floppy, find the key MacAddress in NetAdptX section and change the MAC address directly.

3. Ping the server using IP.

    If this fails, verify that the Arcserve Backup server is on the network and that the subnet mask is working.

4. Ping the server using *server_name*.

    If this fails, DNS is not working.

5. Verify that DNS is functioning.

    If it is not functioning, place the name of the server in the hosts file in disaster recovery system, reboot the system, and continue with the disaster recovery process.

6. Use the following command to connect to the server:

    net use * \\server_name\Admin$ /user:domain\username

    If this fails, verify the following:

    a. Verify that you have not changed the Arcserve Backup server user name or password since the last full backup.

    b. Verify the Windows workstation and server services are running on the Arcserve Backup server.

    c. Verify that you can connect to any other system in the network by running the "net use" command.

d. Verify that you can connect to the Arcserve Backup server from a different system by running the "net use" command.

e. Verify that you do not have any anti-virus, firewall, or server protection software running on the backup server, thus preventing remote access to the server.

f. If you are running Windows 2003 on the backup server, you must reduce the security level to allow other systems to connect to the backup server. You must also change the local security policy to allow blank password connections if you are using a blank password. See the Microsoft documentation, if necessary.

g. If you are using a non-English version of the option, verify that disaster recovery system and the backup server are in the same code page. If not, change the code page of the disaster recovery system.

Network Driver Not on Product CD

Symptom

My Windows XP or Windows 2003 remote disaster recovery fails with the message, "failed to connect to the server." When I installed the operating system, I had to add the network driver; it was not on the Windows XP or Windows 2003 product CD. Why does my disaster recovery fail?

Solution

Disaster recovery failed because the Windows XP or Windows 2003 CD does not support the network card you have in the machine. This can be resolved using one of the two methods listed below:

- You can use the Bootable CD for Windows XP/2003 integrated with network adapter drivers.

- When creating Machine Specific Recovery Disk using the Boot Kit wizard, select the Copy network adapter driver files to MSD option. This will integrate network adapter driver files to MSD automatically as shown in the illustration below:
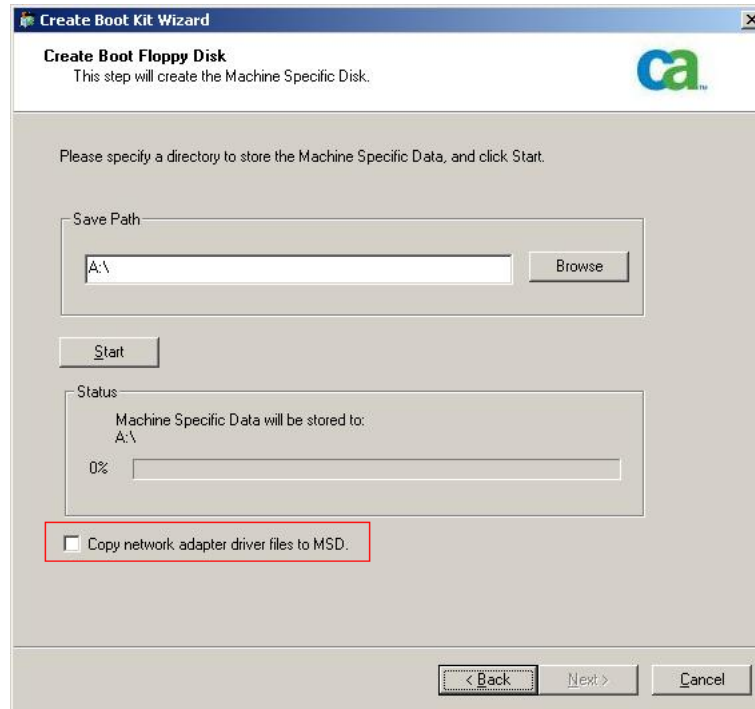
Server Admin error when creating MSD using Floppy Disk

Valid on Windows Server 2008 (x64)

Symptom

When creating Machine Specific Disk for 64-bit (x64) Windows Server 2008 using a floppy disk, you get insufficient floppy disk capacity error.

Solution

You get this error message, when you try to integrate network adapter drivers with the MSD. You must disable "Copy network adapter driver files to MSD" and create MSD without network driver. This will not integrate any device driver to MSD so the capacity of a floppy is enough to store the MSD.

However, for the network device drivers, you can browse to the directory of C:\Program Files\CA\ARCserve Backup\DR\BackupServerName\ClientName\DRV, and copy all the files under that directory to another floppy disk or USB flash disk.

While performing disaster recovery, if you want to install network device driver, insert floppy or USB flash disk which contains the driver files, select the driver file to install it on the device driver install page.

Note: *BackupServerName* is the server name of the backup server and the *ClientName* is the server name of the client agent.

Recover Virtual Hard Disk (VHD) Using Disaster Recovery Option

Valid on Windows Server 2008 R2

Symptom

How can I re-create .vhd files that are mounted as a volume?

Solution

The Arcserve Backup disaster recovery process cannot re-create .vhd files that are mounted as a volume. You can use the following steps to recover .vhd files from a disaster:

To recover .vhd files from a disaster

1. Using the Arcserve BackupDisaster Recovery Option, you must recover the entire computer.

2. Restart the computer.

3. After the computer is restarted, create the virtual hard disk (VHD) and then mount the VHD.

   The mounting of the VHD is complete.

4. Create a new volume on the VHD, and then format the new volume.

   The formatted volume of the VHD is ready.

5. Open the Arcserve Backup Restore Manager.

   The Restore Manager Wizard opens.

6. Recover the VHD by performing a volume level restore of the VHD mounted volume.

   The recovery process is complete.

Note: When you use this process to recover VHDs using Disaster Recovery Option, Arcserve Backup restores the mounted drives as physical disks. For more information about virtual hard disk, see Microsoft documentation.

Also, Arcserve Backup cannot recover VHD boot systems from a disaster. Arcserve Backup demonstrates this behavior because the Automated System Recovery (ASR) writer cannot back up .vhd files. As a result, there are no mechanisms that you can use to recover VHD boot systems from a disaster.

Data is not recovered on a volume that is mounted to a directory on C drive but is not assigned any driver letter

Symptom

Data on volume which is mounted to a directory of a different volume, and is not assigned any drive letter is not restored during Disaster Recovery. After DR reboot, I found the volume is even not formatted.

Solution

Disaster Recovery depends on Windows ASR (Automated System Recovery) to restore disk partitions, volumes and file system of volumes. Volumes on basic disk without assigned drive letter will not be formatted by Windows ASR, but volumes on dynamic disk without drive letter assigned will be formatted by Windows ASR.

Data on these volumes can be recovered manually after disaster recovery. However, if the volume remains unformatted, format it manually. You can use the following procedure to recover data on these volumes:

To recover data on volumes

1. Open Control Panel from Start menu, and select Administrative Tools and then select Computer Management.

   The Computer Management screen appears.

2. Select Disk Management.

3. Right click on the partition/volume which is not formatted, and select Format… option.

4. Format the volume using the same file system format as it was before disaster recovery.

5. Open the Arcserve Backup Manager.

6. Select Restore on the Navigation bar from the Quick Start menu.

   The Restore Manager opens.

7. Click Restore and select Restore by Session from the Source tab.

8. Expand the session and search for the directory into which the volume is mounted.

9. Select this directory, and choose Restore to Original Location, and submit a restore job.

Media Verification

Symptom

During local disaster recovery, I received the message "Please mount media XYZ, Random Id 1234, Sequence 1." How can I verify that the media is in the tape drive or changer?

Solution

The system needs some time to inventory all of the tapes in your library. Click Retry to allow more time for the changer to initialize. You can load only the necessary tapes for recovery to shorten the time the system needs to inventory the tape library.

Verification of Storage Device Attachment

Symptom

How can I verify that the storage device attached to the system is functioning properly during a local disaster recovery?

Solution

It usually takes some time for a changer to initialize. Do not stop the disaster recovery process during this time. See the following instructions.

■ If you are using a changer, use the chgtest utility from the disaster recovery command prompt. This utility is not copied during the disaster recovery process. You must copy it manually from the Arcserve Backup CD/DVD to the disaster recovery directory to use it.

■ If you are performing disaster recovery from a tape drive, run the tapetest utility from the disaster recovery command prompt. This utility can be found in the%WINDIR%\system32\DR directory of the system being recovered.

Windows Setup Message

Symptom

During disaster recovery bluescreen mode, I sometimes see the Windows setup message "Setup has performed maintenance on your hard disk. You must restart your computer to continue with setup. If there is a floppy disk in drive A, remove it. To restart your computer, press Enter." I press Enter to restart my computer and get the message "ntoskrnl.exe is missing" and the disaster recovery fails.

Solution

If you receive this message, you must press Enter to restart your computer and begin the disaster recovery process from the beginning.

Cannot See Partitions

Symptom

I have hardware RAID5 volumes configured in the system and partitions created on the drives. During disaster recovery I cannot see the partitions created by disaster recovery on all the drives. Why?

Solution

If you are using a hardware RAID adapter, you must always enter the manufacturer provided driver for the RAID adapter during the disaster recovery process. If you did not need the driver during the operating system installation, you must still provide it during disaster recovery. If you do not provide the driver for the RAID adapter, you will experience problems accessing the RAID adapter (although you can see the disks).

Process Asks for Missing Files

Symptom

When the disaster recovery process is in the bluescreen text setup mode, it is asking for some missing files and I have to press Esc to proceed with the disaster recovery process. Why?

Solution

This can happen if the CD media is corrupted or if the Microsoft Windows CD being used to create the bootable media is a Microsoft Developer Network (MSDN) pre-release version CD. Recreate the bootable media using the Microsoft Windows CD.

Certificate Server Fails to Start

Symptom

After I perform a disaster recovery, the Certificate Server on the recovered machine fails to start. How can I start it properly?

Solution

If the Certificate Server fails to start after disaster recovery, perform the following procedure to bring it back:

1. Reboot the recovered machine.

2. While the machine is starting, press F8 to put the machine into "Directory services recovery mode".

3. Perform a complete system state restore of the machine.

4. Reboot the machine back to normal mode.

Hard Disk Corrupted Message

Symptom

When performing disaster recovery on a Windows 2003 machine. I booted from the Windows CD and pressed F2. After the system initialized, I received an error message saying that my hard disk may be corrupted and the ASR process failed. What can I do?

Solution

This problem can happen during the disaster recovery process on Windows XP and Windows 2003, including OBDR, due to a Windows ASR problem. To work around this problem, clean the hard disks with a bootable DOS disk and use the FDisk utility, or boot from a normal Windows installation CD and remove all the partitions manually. After the hard disks are cleaned, restart the disaster recovery process.

System Running Out of Free Space

Valid on Windows 2008, Windows 2008 R2

Symptom

When recovering a Windows 2008 machine, DR failed during the restore process and the machine rebooted. The machine cannot start because the system state session is not restored. I checked the system and noticed that the 'X:' volume has no free space.

Because of this, I am not able to install my NIC driver, so the DR process cannot continue.

Solution

In Windows 2008 and Windows 2008 R2, the DR process runs in WinPE. A temporary 'X:\' volume will be created for the WinPE system. DR related binaries and other files (such as drivers, logs) will be copied to the X:\ volume. The DR option creates 10 MB free space to install drivers during DR. If the size of your drivers is more than 10 MB, you must install the required mini-drivers. Only SCSI, FC, and NIC drivers are required during DR.

Another solution is, you can remove all driver files from MSD (MSD is copied to X:\ and consumes some free space), then install the most necessary drivers with 'Utilities->Load Driver Utility' during the DR process.

Applications

This section provides answers to frequently asked questions related to specific applications.

Symptom

After I run a Disaster Recovery on a server running Citrix Presentation Server 4.0, when I start the Citrix Presentation Server Console, I get the error "Pass-though Authentication failed. The service could not be contacted. Make sure the IMA service is installed and running." What should I do?

Solution

To successfully log into the Citrix Presentation Server Console, start the Independent Management Architecture (IMA) service.

Note: If the Citrix Presentation Server was installed using Microsoft SQL Server, you must restore all databases, including the master database before starting the IMA service.

For more information, see the Disaster Recovery section of the *Agent for Microsoft SQL Server Guide*.

Appendix B: Recovering SAN Configurations

The Disaster Recovery Option supports backup servers in Storage Area Network (SAN) configurations. You can recover the primary SAN backup servers and any member SAN servers in Windows Server 2003 environments.

This section contains the following topics:

Recover the SAN

There are no special configurations or settings required to recover primary and member servers. The option can recover any SAN server, as long as a full computer backup was performed using Arcserve Backup.

You must, however, collect all necessary drivers for any SCSI cards, Fibre Channel cards, and network cards.

How SAN Disaster Recovery Works

When recovering primary or member, the option can determine if the current server is a primary server or member server.

- If the current server is a primary server, the option connects to the SAN and uses the devices on the SAN directly.

- If the current server is a member server, the option first contacts the primary server. The option then communicates with the primary SAN server to handle any device operations on the SAN.

Appendix C: Recovering Clusters

Disaster recovery in a Windows-based cluster environment is a complex task. Although Arcserve Backup makes it easier to recover your mission-critical cluster environment, it still requires some planning and effort. It is important that you understand the concepts described in this guide and test the scenarios suitable for your specific environment.

A server cluster is a group of independent servers running cluster services and working collectively as a single system. Server clusters provide high-availability, scalability, and manageability for resources and applications by grouping multiple servers running Windows 2003, Windows 2008, Windows 2008 R2, and Windows Server 2012 operating systems.

Note: Windows 2008, Windows 2008 R2, and Windows Server 2012 do not support performing disaster recovery operations using traditional methods. For more information, see the Knowledge Base document on the Arcserve Support Online website named How to Recover Windows 2008 Cluster from a Disaster.

This appendix provides information about recovering cluster-shared disks, failed cluster nodes, or an entire cluster quickly, with minimum interruption to the service.

This section contains the following topics:

Cluster Failure Scenarios

Several types of failures can occur in the cluster environment. The following types of failure can happen separately or at the same time:

- Some cluster nodes fail (primary node failure and secondary node failure)

- Shared disk fails (cluster non-quorum disk failure)

- Partial shared disk fails

- Entire cluster fails including cluster nodes and shared disks

The scenarios specified in this section outline the steps you can take to recover from various types of cluster failure.

Note: If no tape device is attached to any of the cluster nodes, you can remotely recover a cluster service using the option. To do so, follow the instructions on performing a remote disaster recovery.

Requirements

The requirements in this section specifies the Disaster Recovery Option to recover a cluster.

Software Requirements

To perform disaster recovery on clusters, you must meet the following software requirements:

- Microsoft Windows 2003, Windows 2008, Windows Server 2008 R2, or Windows Server 2012 installed on all computers in the cluster.

- A name resolution method, for example, Domain Naming System (DNS), Windows Internet Naming Service (WINS), or HOSTS.

- A Terminal Server for administering remote clusters.

- Arcserve Backup for Windows and the Disaster Recovery Option, if backup devices such as tape devices or tape library devices are attached to one or all cluster nodes. If no backup devices are attached to the cluster setting, the Client Agent for Windows should be installed on all cluster nodes that require data protection.

Hardware Requirements

To perform disaster recovery on clusters, you must meet the following hardware requirements:

- The hardware for a cluster service node must meet the hardware requirements for Windows 2003, Windows 2008, or Windows 2008 r2 Enterprise Server.

  Note: For information about the hardware requirements for Windows 2008, Windows Server 2008 R2, and Windows Server 2012 operating systems, see the Knowledge Base document on the Arcserve Support Online website named How to Recover Windows 2008 Cluster from a Disaster.

- Cluster hardware must be on the Cluster Service Hardware Compatibility List (HCL).

- Two HCL-approved computers comprised of the following:

  - A boot disk with Windows 2003 Enterprise Server installed. The boot disk cannot be located on the shared storage bus.

  - Boot disks and shared disks must be on separate SCSI channels (SCSI PathID); separate adapters (SCSI PortNumber) are not required. You can use a single multi-channel SCSI or Fibre Channel adapter for both boot and shared disks.

  - Two PCI network adapters on each computer in the cluster.

  - An HCL-approved external disk storage unit that connects to all computers. This is used as the clustered disk. A RAID is recommended.

- All hardware should be identical, slot for slot, card for card, for all nodes. This makes configuration easier and mitigates potential compatibility problems.

- Backup devices such as tapes or tape library devices can be attached to one or all cluster nodes. It is not always necessary to have backup devices attached to the cluster nodes. If you do not have backup devices attached to the cluster nodes, the Client Agent for Windows should be installed in all cluster nodes that require data protection.

Shared Disk Requirements

To recover your clusters, you must meet the following requirements:

- All shared disks, including the quorum disk, must be physically attached to a shared bus.

- Verify that disks attached to the shared bus can be seen from all nodes. This can be checked at the host adapter setup level. See the manufacturer's documentation for adapter-specific instructions.

- SCSI devices must be assigned unique SCSI identification numbers and properly terminated, as per manufacturer's instructions.

- All shared disks must be configured as basic, as opposed to dynamic.

We strongly recommend the use of fault-tolerant RAID configurations (for example, RAID level 5) for all disks, rather than stripe sets without parity (for example, RAID level 0) although this is not a shared disk requirement.

Special Considerations

The following provides information about special considerations for clusters:

- We do not recommend a partial shared disk configuration in which some disks are owned by one node and some disks are owned by another node.

- To avoid complications when matching disks, shared disks should be the last disks and have the highest number when viewed from Administrative Tools, Computer Management, and Disk Management.

■ For Windows 2003, run the dumpcfg.exe utility (available on the Windows Server 2003 Resource Kit) to save the cluster quorum disk signature. It is good practice to preserve the important hard disk signatures if this information is not often used.

For remote backup jobs, run the utility from the cluster machine.

For local backup jobs, use the Global Options dialog to run dumpcfg.exe as a pre-job during a backup to ensure that up-to-date information about the critical hard disk is available. To configure the pre-job, perform the following steps:

■ For Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012, run the DiskPart utility, to obtain and record the signature of the disk and to shift focus to a unique identifier (signature) of the disk.

To configure the pre-job

1. From the Global Options dialog, click the Pre/Post tab.

2. In the field Enter the name of the file/application to execute before the job starts, enter the following command:

c:\dumpcfg > C:\cluster\DR\[Server_Name]\[Machine_Name]\dumpcfg.txt
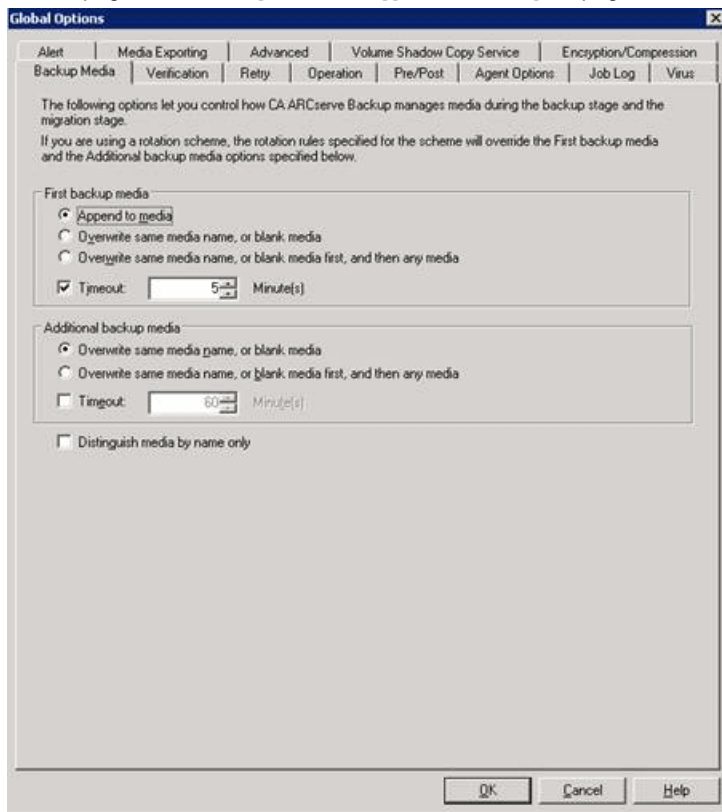
■ You can configure disaster recovery information to be saved to an alternate location on a different computer to further protect disaster recovery information

■ On most cluster computers, there is no need to stop the shared disks. The cluster can continue to function during disaster recovery. Check your hardware documentation for more information about how to avoid shutting down the hard disks.

Terminology

The following defines common cluster terms.

Primary node

The node that owns all shared disk resources during backup.

Secondary node

A node that does not own any shared disk resources during backup.

Quorum Disk

A shared disk used to store cluster configuration database checkpoints and log files that help manage the cluster. This disk is critical to restore the cluster service. The failure of the quorum disk causes the entire cluster to fail.

Non-quorum Disk

A shared disk used to store shared resources including data, database, and application information. These disks are used in the typical fail-over scenario so that the data on the non-quorum shared disks information is always available. The failure of the non-quorum disk does not, in general, cause the entire cluster to fail.

Partial Shared Disk

A specific type of shared disk. In a partial shared disk configuration, shared disks can have a unique, one-to-one relationship with individual nodes. Some shared disks are owned by one node and some disks are owned by another node during backup.

The following diagram illustrates a typical two-node cluster setting:
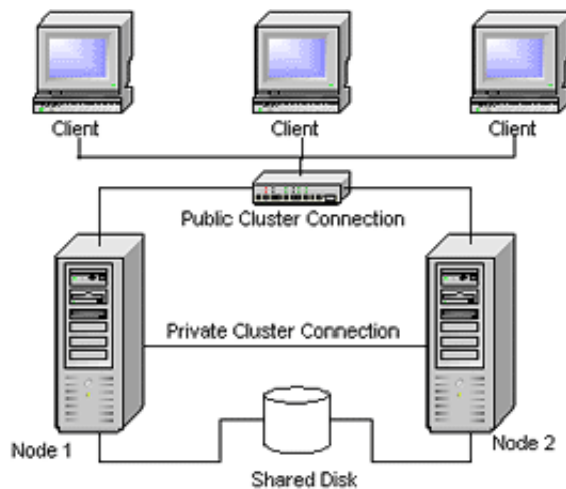
Cluster Disaster Recovery Requirements

You must have the following information to recover failed clusters:

■ Cluster name

■ Cluster IP address and subnet mask

■ Cluster node names

■ Cluster node IP addresses

■ The assignment of all drive letters including all private and shared hard disks

■ All disk signatures (To obtain disk signatures, run one of the following utilities:)

■ dumpcfg.exe for Windows 2003

■ DiskPart for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012

- All disk numbering schemes (to find these schemes, select Administrative Tools, Computer Management, Disk Management and note the disk number matching each physical disk for each computer)

- Cluster group name

- Cluster preferred nodes

- Cluster fail over policies

- Cluster resource names

- Cluster resource types

- Cluster group membership

- Cluster resource owners

- Cluster resource dependencies

- Cluster restart properties

Scenario 1: No Shared Disk Failure

The cases specified in this section are the most common failures in the Windows cluster environment.

Recover Secondary Node

To recover a secondary node in the cluster

1. Disconnect the shared disks from the secondary node.

   Note: On most cluster computers, there is no need to shut down the shared disks. This allows the cluster to function during disaster recovery. However, shutting down the cluster service on some cluster computers on the primary node might be required. Check your hardware guide for more information about how to avoid shutting down shared disks.

2. Follow the usual disaster recovery process to recover the secondary node.

3. Connect the shared disks to the secondary node when the restoration is complete.

4. Reboot the secondary node.

Your cluster should now be back online.

Recover the Primary Node

To recover a failed primary node and ensure that the cluster is working properly

1. Disconnect the shared disks from the primary node.

   Note: On most cluster computers, there is no need to shut down the shared disks. This allows the cluster to function during disaster recovery. However, shutting down the cluster service on some cluster computers on the primary node might be required. Check your hardware guide for more information about how to avoid shutting down shared disks.

2. Follow the usual disaster recovery process to recover the primary node.

3. Connect the shared disks when the restoration is complete.

4. Reboot the primary node.

Your cluster should now be back online.

Scenario 2: Shared Disk Failure

There are several possible causes for shared disk failure and these are illustrated in the cases specified in this section. The first five cases discuss non-partial shared disk cluster configurations and the sixth discusses partial shared disk cluster configurations.

Recover Cluster Non-quorum Shared Disks with No Node Failures

To recover cluster non-quorum shared disks with no node failures in the cluster

1. Stop the cluster service on the secondary node and disconnect the shared disks from the secondary node.

2. If a non-quorum shared disk is physically damaged, perform the following steps:

   a. Shut down the primary node.

   b. Replace the cluster non-quorum shared disk with new disks.

   c. Have the Cluster Disaster Recovery Requirements readily available for reference. For more information, see the Cluster Disaster Recovery Requirements (see page 172).

   d. To restore the original disk signature for the shared disk, run one of the following utilities:

      ■ dumpcfg.exe for Windows 2003 (See the output file created by this utility during the backup.)

      ■ DiskPart for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012

  e. Restart the primary node and the cluster services.

  f. Recreate the partitions on the non-quorum shared disk.

  g. Format the partitions according to the Cluster Disaster Recovery Requirements.

3. Run a restore job from the Arcserve Backup machine to restore the data to a non-quorum shared disk. Select the full volume restore to recover all lost non-quorum volumes in the shared disks.

4. When the restore job finishes, use the Cluster Administrator to bring the shared disk back on line.

5. Reconnect the shared disks and restart the cluster service on the secondary node.

Your cluster should now be back online.

Recover Cluster Quorum Disks with No Node Failures

To recover cluster quorum disks with no node failures

1. Stop the cluster services on the secondary node.

2. Shut down the secondary node.

3. On the primary node, from the Windows Service Control Manager, set the cluster service startup type to Manual.

4. From the Device Manager View menu, select Show Hidden Devices and disable the Cluster Disk Driver setting.

5. If the cluster quorum disks are physically damaged, perform the following steps:

  a. Shut down the primary node.

  b. Replace the cluster quorum shared disk with new disks.

  c. Start the primary node.

   Note: Have the Cluster Disaster Recovery Requirements readily available for reference.

  d. To restore the original disk signature for the shared disk, run one of the following utilities:

   ■ dumpcfg.exe for Windows 2003 (See the output file created by this utility during the backup.)

   ■ DiskPart for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012

  e. Recreate and reformat the partitions on the non-quorum shared disk.

6. From the Device Manager View menu, select Show Hidden Devices and enable the Cluster Disk Driver setting.

7. Restore the system state backup. In Arcserve Backup, select System State session and right-click to select the local option.

    The System State Restore Options dialog opens.
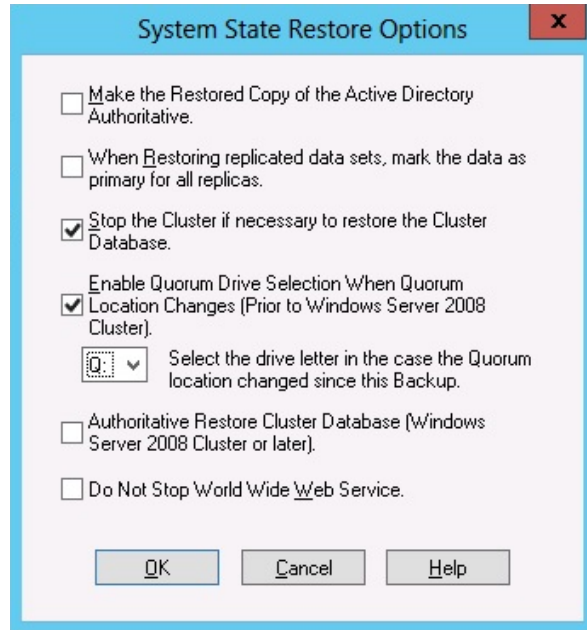
    Note: If the cluster nodes are Active Directory Servers, you must reboot the primary node into directory restore mode when restoring the system state session.

8. Restart the primary node.

9. If the cluster files are not restored to the quorum disk, run the caclurst.exe utility to load the cluster database from the following:

    %windir%\clusbkup

    caclurst.exe is available in the Home directory.

    caclurst /s c:\%SystemRoot%\cARCservelusbkup /q Q:

    If this is a remote disaster recovery, copy the caclurst.exe file to the Client Agent for Windows directory.

10. Reboot the primary node.

11. Connect the shared disks to the secondary node.

12. Start the secondary node.

Recover All Shared Disks with No Node Failures in the Cluster

To recover all shared disks with no node failures in the cluster, restore the quorum disk and then restore the other shared disks. For information about restoring the quorum disk, see section Recover Cluster Quorum Disks with No Node Failures (see page 175).

Recover Primary Nodes with Shared Disk Failure in the Cluster

To recover a primary node with shared disk failures in the cluster

1. Shut down the secondary node.

2. Disconnect the shared disks from the secondary node.

3. Follow the disaster recovery procedure to recover the primary node.

4. When the restoration is complete, reboot the primary node.

5. Start the cluster services on the primary node.

6. Connect the shared disks to the secondary node.

7. Reboot the secondary node.

8. If necessary, start the cluster services on the secondary node.

Your cluster should now be back on line.

Recover Entire Clusters

To recover an entire cluster

1. To recover all secondary nodes, perform the following procedure:

   a. Stop the cluster services on all nodes.

   b. Disconnect the shared disks from the secondary node.

   c. Shut down all nodes.

   d. Follow the disaster recovery procedure to recover the secondary node.

   e. If there is more than one secondary node, repeat the previous steps to recover all secondary nodes.

   f. Shut down all secondary nodes while recovering the primary node with shared disks resources.

   Note: All nodes and shared disks should be shut down at this time.

2. To recover the primary node with shared disks failure, perform the following tasks:

   a. Follow the disaster recovery procedure to recover the primary node.

   b. Start all shared disks.

   c. When the restoration is complete, reboot the primary node.

    d.   Start the cluster services on the primary node.

    e.   Restart all secondary nodes.

    f.   Start the cluster services on the secondary node.

Your cluster should now be back online.

Recover Clusters with Partial Shared Disk Configurations

In an environment with a partial shared disk configuration, shared disks can have a unique, one-to-one relationship with individual nodes. We recommend that you have the Cluster Disaster Recovery Requirements readily available for reference when performing this disaster recovery process.

You must perform the following tasks:

1. Recover one node with some shared disks first while other shared disks that are not owned by this node are shut down.

2. Recover another node with some shared disks. You must shut down all shared disks not owned by the node.

3. Repeat this process until you have recovered all nodes with shared disk resources.

After performing these actions, you can recover the nodes with no shared disk resources.

To recover a cluster with a partial shared disk configuration

1. Recover one node with some shared disk resources by performing the following steps:

    a.   Stop the cluster services on all nodes.

    b.   Disconnect shared disks not owned by this node during backup. Refer to the Cluster Disaster Recovery Requirements and dumpcfg.txt to identify which shared disks are not owned by this node.

    c.   Follow the disaster recovery procedure to recover the node.

2. Repeat the previous step until you have recovered all nodes with some shared disk resources.

3. Recover nodes with no shared disk resources. Follow the disaster recovery procedure to recover the node.

4. Restart all nodes in the following order:

    a.   Restart all nodes with shared disk resources.

    b.   Restart all nodes without shared disk resources.

Your cluster should now be back online.

Appendix D: Recovering NEC Clusters

Disaster recovery in a Windows-based cluster environment is a complex task. Although Arcserve Backup makes it easier to recover your mission-critical cluster environment, it still requires some planning and effort. It is important that you understand the concepts described and test the scenarios suitable for your specific environment.

A server cluster is a group of independent servers running cluster services and working collectively as a single system. Server clusters provide high-availability, scalability, and manageability for resources and applications by grouping multiple servers running Windows 2003 Advanced Server.

The following sections provide information about recovering the cluster-shared disks, failed cluster nodes, or the entire cluster, quickly and with minimum interruption to the service.

This section contains the following topics:

Disaster Recovery Requirements

This section provides the hardware and software requirements for the Disaster Recovery Option to recover an NEC cluster.

Software Requirements

You must satisfy the following software requirements to install Arcserve Backup as a CLUSTERPRO/ExpressCluster-aware application:

- Install Arcserve Backup on a switched disk of the cluster with the same drive letter assigned to the volume from all nodes for Active/Passive job failover capability.

- Install the same Arcserve Backup components on all nodes. You must configure each of these components in the same way.

■ Use the same Arcserve Backup Device Group Name for the same devices in the Arcserve Backup configuration on each node of the cluster. To ensure this, use the default Device Group Names assigned by Arcserve Backup when you use Device Configuration.

■ Use the same Arcserve Backup system accounts for all Arcserve Backup servers installed on each of the cluster nodes.

■ Ensure that the Cluster nodes are in the same domain during the installation.

Hardware Requirements

You must meet the following hardware requirements to install Arcserve Backup as a CLUSTERPRO/ExpressCluster-aware application:

■ Ensure that all cluster nodes have identical hardware configurations (for example, SCSI adapters, Fiber Adapters, RAID Adapters, network adapters, and disk drives).

■ Use separate SCSI/Fiber adapters for disk and tape devices.

   Note: Ensure that the hardware for all nodes is similar, if not identical, to make configuration easier and eliminate any potential compatibility problems.

Requirements for NEC CLUSTERPRO/ExpressCluster Shared Disks

You must satisfy the following minimum requirements for the NEC CLUSTERPRO/ExpressCluster Shared Disk:

■ All shared disks, including the cluster disk, shared disk, and switched disk, must be physically attached to a shared bus.

■ Disks attached to the shared bus must be visible from all nodes. To verify this at the host adapter setup level, see the manufacturer's documentation for adapter-specific instructions.

■ SCSI devices must be assigned unique SCSI identification numbers and properly terminated, as per manufacturer's instructions.

■ All shared disks must be configured as basic (as opposed to dynamic).

Note: We recommend the use of fault-tolerant RAID configurations (for example, RAID level 5) for all disks, rather than stripe sets without parity (for example, RAID level 0), although this is not a shared disk requirement.

Disaster Recovery Considerations

You should consider the following information when protecting NEC clusters:

■ We do not recommend that you use partial shared disk configuration, in which some disks are owned by one node and some disks are owned by another node.

■ To avoid complications when matching disks, shared disks should be the last disks and should have the highest number when viewed from Administrative Tools, Computer Management, Disk Management.

■ You can configure disaster recovery information to be saved to an alternate location on a different machine to further protect disaster recovery information

■ You must back up the local disk of each cluster node with a physical hostname and shared disks with the virtual computer name (switched disk, cluster disk, or shared disk).

Information Required to Recover Cluster Nodes

We recommend that you collect the following information to successfully perform disaster recovery on cluster nodes:

■ Cluster name

■ Cluster IP address (Public and interconnect IP) and subnet mask

■ Cluster node names

■ Cluster node IP addresses

■ All drive letter assignments, including all private and shared hard disks

■ All disk numbering schemes. This can be obtained by selecting Administrative Tools, Computer management. Select Disk Management. Note the disk number matching each physical disk for each machine.

■ Partitioning information for the shared disk

■ All cluster letters assign schemes. Select Start, NEC ExpressCluster Server, Disk Administrator, and select Assign cluster letters.

■ Cluster group information, including the following:

– Group name

– Resources name and configurations

– Registry information

– Failover policies

- – Monitor group information

- – Failover server lists

- – Resource dependencies

Disaster Recovery on NEC CLUSTERPRO/ExpressCluster SE

Several types of failures can occur in a cluster environment. The following types of failure can happen separately or at the same time:

- Shared disk fails

- Some cluster nodes fail (primary node failure and secondary node failure)

- Entire cluster fails, including cluster nodes and shared disks

This section provides the procedures to follow to recover from various types of cluster failure.

Note: If the cluster node is not a backup server (no tape device is attached to the cluster node), follow the instructions for performing a remote disaster recovery.

Arcserve Backup Installed Outside NEC CLUSTERPRO/ExpressCluster SE Cluster

This section provides procedures to resolve cluster failures when Arcserve Backup is installed outside the cluster.

Recover Data on Failed NEC CLUSTERPRO/ExpressCluster SE Shared Disks

If the shared disk fails, but the cluster nodes are undamaged, perform the following steps to recover data residing on the shared disks:

To recover data residing on the shared disks

1. On each cluster node, select Control Panel, Services, and change the Startup Type of the following services to Manual:

   - NEC ExpressCluster Server

   - NEC ExpressCluster Log Collector

2. Shut down the cluster and turn off all servers.

3. Turn off the shared disk and replace the shared disk if necessary.

4. Turn on the shared disk, and set the parameters for the shared disk.

   If RAID reconstruction or LUN configuration change is necessary, use the setting tool attached with the shared disk. See the shared disk documentation for information about the setting tool.

   To perform any setting or configuration from a cluster node, turn on only one server at a time.

5. On the primary cluster node only, perform the following procedure:

   a. Write a signature (identical to the original) to the disk with the operating system's disk administrator, if one does not already exist.

   b. Recreate the original partitions on the disk. If X-Call settings have been performed to HBA, you must connect the partition using the NEC ExpressCluster disk administrator before formatting.

      Note: X-Call is a setting that enables viewing of the shared partition from both the active and passive sides. See the CLUSTERPRO/ExpressCluster products document for more information about the setting for X-Call.

   c. Using the operating system's disk administrator, specify the original drive letter to the shared disk.

   d. Use Arcserve Backup to restore the backed up data to the shared disk.

   e. If you have performed X-Call settings for a disk, start the NEC ExpressCluster disk administrator and specify the recovered shared disk as X-CALLDISK in X-CALL DISK configuration.

      If you have performed X-Call settings for HBA, these settings are not changed. Go on to the next step.

   f. If the disk access path has been dualized, confirm that the access path is dualized. For example, if the NEC dual port utility 2000 Ver.2.0 (UL1214-102) is used, see the manual attached with the product.

   g. Reboot the server.

   h. Confirm that the drive letter is identical to the one you set in the previous step using the operating system's disk administrator.

   i. Check the cluster letters on the CLUSTER disk partition with the NEC ExpressCluster disk administrator. If the cluster letter does not appear, set it to the original letter.

   j. Shut down the cluster node.

6. Perform the following steps on all cluster nodes:

   a. Boot up the cluster node.

   b. Using the operating system's disk administrator, specify the original drive letter to the shared disk, if necessary.

     c.   Set the Startup type of the following services from Manual to Automatic:

■   NEC ExpressCluster Server

■   NEC ExpressCluster Log Collector

     d.   Shut down the server and shut down the cluster node.

7.   Start all cluster nodes and perform the Return to cluster(R) operation from the NEC ExpressCluster Manager. Recover all servers to Normal.

Recover One Failed Cluster Node on NEC CLUSTERPRO/ExpressCluster SE

A cluster node that fails is automatically isolated from the cluster and all Cluster Groups active on the node are failed over to other healthy nodes.

To recover the failed cluster node

1.   Shut down the failed node.

2.   Disconnect shared disks from the node.

3.   Follow the normal remote disaster recovery process to recover the node.

    Note: Restore only the local disk partitions during the disaster recovery.

4.   Connect the shared disks to the node.

5.   Reboot the node after restoration.

6.   Perform the NEC ExpressCluster Server Return to Cluster operation, using one of the following methods:

■   Select a server name and select Control, Return to Cluster.

■   Right-click a server and select Return to Cluster from the pop-up menu.

■   Select a server and click the Return to Cluster icon on the toolbar.

The Return to Cluster operation corrects inconsistencies in the configuration information of the cluster node where the fault occurred and returns it to normal cluster operation.

Recover Entire Clusters on NEC CLUSTERPRO/ExpressCluster SE

You can recover an entire cluster.

To recover an entire cluster

1.   Stop the cluster services on all nodes.

2.   Disconnect shared disks from the all nodes.

3.   Ensure that all cluster nodes are shut down.

4. To recover all cluster nodes one by one, follow the procedure provided in the section Recover One Failed Cluster Node on NEC CLUSTERPRO/ExpressCluster SE in this document.

   Note: Perform the recovery of one node at a time, and ensure that all other nodes are shut down and the shared disk is disconnected during this process.

5. Shut down all cluster nodes.

6. To recover the cluster shared disks, perform the procedure provided in the section Recover Data on Failed NEC CLUSTERPRO/ExpressCluster SE Shared Disks in this document.

Arcserve Backup Installed on the NEC CLUSTERPRO/ExpressCluster SE Cluster

Performing disaster recovery with Arcserve Backup installed on an NEC CLUSTERPRO/ExpressCluster cluster requires special consideration when creating your backup jobs:

■ Do not use filters to exclude files or folders residing on volumes containing the Arcserve Backup installation when submitting backup jobs using the physical node name.

■ You can use filters to exclude files or folders residing on other shared disk or mirrored volumes from backups when creating backup jobs using the physical node name. These volumes should be backed up using the virtual hostname.

Shared Disk Failure on NEC CLUSTERPRO/ExpressCluster SE

This section provides the procedures to follow to recover your data if your shared disk fails.

Recover Data with Arcserve Backup Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disks

To recover the data residing on the shared disks, if the Arcserve Backup was installed on the shared disk, perform the following procedure:

To recover the data residing on the shared disks

1. On each cluster node, select Control Panel, Services, and change the Startup Type of the following services to Manual:

   ■ NEC ExpressCluster Server

   ■ NEC ExpressCluster Log Collector

2. Shut down the cluster and turn off all servers.

3. Turn off the shared disk. Replace the shared disk, if necessary.

4. Turn on the shared disk and set the shared disk parameters.

   If you must reconstruct a RAID configuration or change a LUN configuration, use the setting tool belonging to the shared disk. See the shared disk product documentation for more information about the setting tool.

   If you perform any settings or configuration from a cluster node, turn on only one server at a time.

5. Perform the following steps on the primary cluster node:

   a. Perform local disaster recovery on the primary cluster node. Ensure that the data on the shared disk containing the Arcserve Backup installation is restored.

   b. If you have performed X-Call settings for a disk, start the NEC ExpressCluster Disk Administrator and specify the recovered shared disk as X-CALLDISK in the X-CALL DISK configuration.

      If you have performed X-Call settings for HBA, these settings are unchanged. No action is necessary.

   c. Confirm that the disk access path is dualized, if applicable. For example, if the NEC dual port utility 2000 Ver.2.0 (UL1214-102) is used, see the product manual for more information.

   d. Reboot the server.

   e. From the NEC ExpressCluster Disk Administrator, verify that the cluster letters on the CLUSTER disk partition are the same as the original letters.

   f. Shut down the cluster node.

6. Perform the following steps on all cluster nodes:

   a. Boot up the cluster node.

   b. Using the operating system disk administrator, specify a drive letter for the shared disk, if necessary. This letter should be the same as the original drive letter.

   c. Reset the Startup type of the following services to Automatic:

      ■ NEC ExpressCluster Server

      ■ NEC ExpressCluster Log Collector

   d. Shut down the server and shut down the cluster node.

7. Start all cluster nodes and, from the NEC ExpressCluster Manager, perform the Return to Cluster(R) operation to recover all servers to Normal.

Recover Data with Arcserve Backup Not Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disks

If the shared disk fails, but the cluster nodes are undamaged, perform the following steps to recover data residing on the shared disks:

To recover data residing on the shared disks

1. On each cluster node, select Control Panel, Services, and change the Startup Type of the following services to Manual:

   ■ NEC ExpressCluster Server

   ■ NEC ExpressCluster Log Collector

2. Shut down the cluster and turn off all servers.

3. Turn off the shared disk and replace the shared disk, if necessary.

4. Turn on the shared disk and set the shared disk parameters.

   If you must reconstruct a RAID configuration or change a LUN configuration, use the setting tool belonging to the shared disk. See the shared disk product documentation for more information.

   To perform any setting or configuration from a cluster node, turn on only one server at a time.

5. On the primary cluster node, perform the following procedure:

   a. Write a signature (identical to the original) to the disk with the operating system's disk administrator, if one does not already exist.

   b. Recreate the original partitions on the disk. If X-Call settings have been performed to HBA, you must connect the partition using the NEC ExpressCluster Disk Administrator before formatting.

   c. Using the operating system's disk administrator, specify the original drive letter to the shared disk.

   d. Use Arcserve Backup to restore the backed up data to the shared disk.

   e. If you have performed X-Call settings for a disk, start the NEC ExpressCluster Disk Administrator and specify the recovered shared disk as X-CALLDISK in the X-CALL DISK configuration.

   If you have performed X-Call settings for HBA, these settings are not changed. No action is necessary.

   f. Confirm that the disk access path has been dualized, if applicable. For example, if the NEC dual port utility 2000 Ver.2.0 (UL1214-102) is used, see the product manual for information.

   g. Reboot the server.

   h. Confirm that the drive letter is identical to the one you set in the previous step using the operating system's disk administrator.

i. From the NEC ExpressCluster Disk Administrator, ensure that the cluster letter appears on the CLUSTER disk partition. If the cluster letter does not appear, set it to the original letter.

j. Shut down the cluster node.

6. Perform the following steps on all cluster nodes:

a. Boot up the cluster node.

b. Using the operating system disk administrator, specify the original drive letter to the shared disk, if necessary.

c. Reset the Startup type from Manual to Automatic for the following services:

■ NEC ExpressCluster Server

■ NEC ExpressCluster Log Collector

d. Shut down the server and shut down the cluster node.

Start all cluster nodes and perform the Return to Cluster(R) operation from the NEC ExpressCluster Manager to recover all servers to Normal.

Recover One Failed NEC CLUSTERPRO/ExpressCluster SE Cluster Node

A cluster node that fails is automatically isolated from the cluster and all Cluster Groups active on the node are failed over to other healthy nodes.

To recover the failed cluster node

1. Shut down the failed node.

2. Disconnect shared disks from the node.

3. Follow the normal remote disaster recovery process to recover the node.

   Note: Restore only the local disk partitions during the disaster recovery.

4. Connect the shared disks to the node.

5. Reboot the node after restoration.

6. Perform the NEC ExpressCluster Server Return to Cluster operation, using one of the following methods:

■ Select a server name and select Control, Return to Cluster.

■ Right-click a server and select Return to Cluster from the pop-up menu.

■ Select a server and click the Return to Cluster icon on the toolbar.

The Return to Cluster operation corrects inconsistencies in the configuration information of the cluster node where the fault occurred and returns it to normal cluster operation.

Recover Entire NEC CLUSTERPRO/ExpressCluster SE Clusters

You can recover an entire cluster using the following procedure.

To recover an entire cluster

1. Stop the cluster services on all nodes.

2. Disconnect shared disks from the all secondary nodes.

3. Ensure that all cluster nodes are shut down.

4. To recover the primary cluster node, perform the procedure provided in section Recover Data with Arcserve Backup Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disk (see page 185).

5. To recover all other cluster nodes one by one, perform the procedure provided in section Recover One Failed NEC CLUSTERPRO/ExpressCluster SE Cluster Node (see page 188).

   Note: You must recover one node at a time, and ensure that all other nodes are shut down and that the shared disk is disconnected during this process.

6. Shut down all cluster nodes.

7. To recover the cluster shared disks, perform the procedure provided in section Recover Data with Arcserve Backup Not Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disk (see page 187).

Disaster Recovery on NEC CLUSTERPRO/ExpressCluster LE

Several types of failures can occur in a cluster environment. The following types of failure can happen separately or at the same time:

- Mirror disk fails

- Cluster nodes fail (primary node failure and secondary node failure)

- Entire cluster fails including cluster nodes and mirror disks

The scenarios in this section outline the steps you can take to recover from various types of cluster failure.

Note: If no tape device is attached to any of the cluster nodes, you can remotely recover a cluster service using the Disaster Recovery Option. To do so, follow the instructions on performing a remote disaster recovery.

Arcserve Backup Installed Outside NEC CLUSTERPRO/ExpressCluster LE Cluster

This section provides procedures to help you recover your data if Arcserve Backup is installed outside the cluster.

NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk is Damaged

If any disk in a mirror set becomes damaged, but the cluster nodes are undamaged, you must replace the disk without halting the current application. See the NEC document *NEC ExpressCluster System Construction Guide [Operation/Maintenance] 4.2.9 Replacement of Damaged Disk* for information.

Recover Data if NEC CLUSTERPRO/ExpressCluster LE Mirrored Disk Data is Corrupted

If the data on the mirrored disk becomes corrupted or inaccessible from any cluster node, but the cluster nodes are undamaged, perform the following procedure to recover your data:

To recover your data from the cluster node

1. From the Start menu, select Programs, and select Computer Management. Select Services and change the Startup type of the NEC ExpressCluster Server services to Manual:

    Perform this task on all servers.

2. Shut down the cluster and replace the failed mirrored disk, if necessary.

3. Reboot the servers.

4. Start the Mirror Disk Administrator on the server to be restored.

5. From the Mirror Disk Administrator menu bar, select Disk Operation, Enable Access, and set the mirrored disk to make it accessible.

6. Use Arcserve Backup to restore data to the mirrored disk.

    Note: Use your normal restore settings when restoring this data.

7. From the Mirror Disk Administrator menu bar, select Disk Operation, Disable Access, and return the mirrored disk setting to restrict access.

8. Open Services and set the startup type of the NEC ExpressCluster Server service to Automatic.

    Perform this task on all servers.

9. From the Start menu, select Shut Down to reboot all of the servers.

Recover if One NEC CLUSTERPRO/ExpressCluster LE Cluster Node Fails

When a problem occurs on the server system disk and the system does not operate properly, you must replace the disk and restore the data. To do so, perform the following procedure:

To recover the cluster

1. If the server to be recovered is running, from the Start menu select Shut Down to shut down the server. If NEC ExpressCluster is running, wait until the failover finishes.

2. If NEC ExpressCluster is running, select the cluster from the NEC ExpressCluster Manager, choose CLUSTER(M), Property(P) from the menu bar, and check Manual return(F) on the Return mode tag.

3. Follow the normal disaster recovery process to recover the node.

4. From the Start menu select Settings, Control Panel, and select Date and Time to confirm that the Date and Time of the server operating system to be restored is identical to the other servers in the cluster.

5. On the server to be restored, change the Startup type of the following NEC ExpressCluster-related services to Manual:

   ■ NEC ExpressCluster Server service

   ■ NEC ExpressCluster Log Collector service

   ■ NEC ExpressCluster Mirror Disk Agent service

6. From the Start menu, select Shut Down to shut down the server to be restored.

7. On the server to be restored, start the operating system disk administrator and, if necessary, modify the drive letter of the switched partitions so that it is the same as when the backup was performed. Close the disk administrator.

8. On the server to be recovered, set the Startup type of the following services to Manual and reboot:

   ■ NEC ExpressCluster Server services

   ■ NEC ExpressCluster Log Collector services

   Note: The NEC ExpressCluster Mirror Disk Agent service Startup type should remain set to Automatic.

9. On the server to be recovered, from the Start menu, select Programs, and select NEC ExpressCluster Server.

10. Start the Mirror Disk Administrator, select Change, and click Reconstitution.

11. Check the name of target mirror sets and click OK.

12. On the server to be restored, reset the startup type of the following services to Automatic and reboot:

   ■ NEC ExpressCluster Server services

   ■ NEC ExpressCluster Log Collector

13. On the other server, shut down the cluster and reboot.

14. When the servers have been restarted, from the NEC ExpressCluster Manager, return the server to be recovered to the cluster.

15. Select the cluster from the NEC ExpressCluster Manager, select CLUSTER(M), and Property(P) from the menu bar, and reset the Return Mode setting to Auto Return.

16. Shut down the cluster.

Recovery if All NEC CLUSTERPRO/ExpressCluster LE Nodes Fail

To recover an entire cluster, follow the normal disaster recovery process to recover the primary node and the secondary node. To return all nodes to the cluster, see the NEC documentation for more information.

Active/Passive Configuration

Performing disaster recovery in this configuration requires special considerations while creating your backup jobs:

■ Do not use filters to exclude files or folders residing on volumes containing the Arcserve Backup installation (either shared disk volume or mirrored volume) when submitting backup jobs using the physical node name.

■ You can use filters to exclude files or folders residing on other shared disks or mirrored volumes while creating backup jobs using the physical node name. Back these volumes up using the virtual hostname.

Damaged Mirrored Disk in Active/Passive Configuration

If a disk in a mirror set becomes damaged, you must replace the disk without halting the current application.

Note: See the NEC document *NEC ExpressCluster System Construction Guide [Operation/Maintenance] 4.2.9 Replacement of Damaged Disk* for information.

Corrupted Mirrored Disk Data in Active/Passive Configuration

If the data on the mirrored disk becomes corrupted or inaccessible from any cluster node, but the cluster nodes are undamaged, perform one of the procedures specified in this section, depending upon whether Arcserve Backup is installed on the mirrored disk.

Recover Data with Arcserve Backup Installed on Mirrored Disks

If the data on the mirrored disk becomes corrupted or inaccessible from any cluster node, but the cluster nodes are undamaged, and Arcserve Backup is installed on the mirrored disk, perform the following procedure to recover your data:

1. Shut down the cluster.

2. Replace the damaged mirrored disk, if necessary.

3. Perform local disaster recovery on the primary cluster node. Ensure that the data on the mirrored disk containing the Arcserve Backup installation is restored.

   Note: See the special considerations in section Active/Passive Configuration (see page 192).

4. From the Start menu, select Shut Down to reboot all servers.

Arcserve Backup Not Installed on Mirrored Disks

If any disk in a mirrored set becomes damaged, but the cluster nodes are undamaged, and Arcserve Backup is not installed on the mirrored disk, you must replace the disk without halting the current application.

Note: See the NEC document *NEC ExpressCluster System Construction Guide [Operation/Maintenance] 4.2.9 Replacement of Damaged Disk* for information.

Recover One Failed Cluster Node in Active/Passive Configuration

A cluster node that fails is automatically isolated from the cluster and all Cluster Groups active on the node are failed over to other healthy nodes.

To recover the failed cluster node

1. Shut down the failed node.

2. Disconnect shared disks from the node.

3. Follow the normal remote disaster recovery process to recover the node.

   Note: Restore only the local disk partitions during the disaster recovery.

4. Connect the shared disks to the node.

5. Reboot the node after restoration.

6. Perform the NEC ExpressCluster Server Return to Cluster operation, using one of the following methods:

   ■ Select a server name and select Control, Return to Cluster.

   ■ Right-click a server and select Return to Cluster from the pop-up menu.

   ■ Select a server and click the Return to Cluster icon on the toolbar.

   The Return to Cluster operation corrects inconsistencies in the configuration information of the cluster node where the fault occurred and returns it to normal cluster operation.

All Cluster Nodes Fail in Active/Passive Configuration

You can recover an entire cluster node using the following procedure.

To recover an entire cluster

1. To recover the primary node, perform the procedure provided in section Recover Data with Arcserve Backup Installed on Mirrored Disk (see page 193).

2. To recover the secondary nodes, perform the procedure provided in section Recover One Failed Cluster Node in Active/Passive Configuration (see page 193).

3. Return all nodes to the cluster. To do so, see the NEC documentation for more information.

Arcserve backup fails to start after recovery using the Disaster Recovery Option on CLUSTERPRO X2.0 in mirrored disk environment

After performing a cluster active node disaster recovery, when you restart your computer, if the NEC cluster shows abnormal status for Windows and do not start some of its resources then the mirror disk cannot be accessed. As a result most of the Arcserve services and programs fail to run, including the AsRecoverDB.exe.

To access the mirror disk on CLUSTERPRO X2.0

1. Close the NEC Cluster group. On the NEC Cluster Manager, right-click Cluster group, select Stop to stop the cluster group resources.

2. Transform mirror disk status to normal. On the Cluster Manager, right-click mirror disk resource, and select Details.

3. On the Mirror Disk Helper dialog that appears, click the computer icon in red.

4. You can see the mirror disk showing inactive status.

5. Click on the red computer icon.

    The comments show "Data for XXX is the latest".

6. Click Execute. After finishing successfully, the computer icon changes to green closing the dialog.

    The mirror disk status shows normal.

7. Close the Mirror Disk Helper dialog.

8. Start NEC cluster group. On NEC Cluster manager, right click Cluster group, select Start, then select correct cluster server, click OK.

9. Wait for the NEC cluster group resources to start, and access the mirror disk. You can now simultaneously start the Arcserve services.

10. Restart the Arcserve Universal Agent Services to recover disk partition information.

    a. From the Start menu, select Programs, CA, ARCserve Backup, and Backup Agent Admin.

    b. In the ARCserve Backup Agent Admin tool, select Options, Services, stop service and start service.

        The Arcserve services start.

11. Run AsRecoverDB.exe in Arcserve home directory to recover the database.

Appendix E: Staging Using File System Devices

Arcserve Backup lets you create backup sessions that can be used for disaster recovery operations and store the sessions on file system devices using Arcserve Backup disk staging functionality. When you migrate the backup sessions one location (staging devices) to another location, or purge backup data on the staging devices, an update of your disaster recovery information is automatically triggered. This ensures that your machine-specific recovery information is always up-to-date.

This section contains the following topics:

Special Considerations for Staging (see page 197)

Special Considerations for Staging

When using the disk staging feature, there are some special considerations that can potentially affect the disaster recovery process. The following is a list of best practices and considerations specifically for disaster recovery:

- Do not stage the backup of the local backup server itself on disks.

- When performing remote disaster recovery, if the restore process cannot locate a backup session in the staging devices, the backup session may have been purged from the staging device. If so, create a new machine-specific recovery disk from the backup server and restart the disaster recovery process using the new recovery disk.

Appendix F: Recovering Servers with StorageTek ACSLS Libraries

If your backup server machine has a connection to a StorageTek ACSLS tape library, the option supports local recovery of the backup server using the library. To do so, the backup server machine must meet the following requirements:

■ You must have installed the Arcserve Backup Enterprise Module

■ You must have installed the StorageTek LibAttach Service

■ The machine must be running on a supported Windows Server 2003 or 32-bit Windows Server 2008 platform

This section contains the following topics:

Disaster Preparation

For a typical Windows Server 2003 disaster recovery operation, you must create or obtain the following media:

■ Microsoft Windows Server 2003 CD. You must use the same version and edition you installed on your machine.

■ The Arcserve Backup CD/DVD.

■ The machine-specific recovery disk created for the system to be recovered.

In addition, you must create an additional disk, the Disaster Recovery ACSLS disk, to support local disaster recovery using a StorageTek ACSLS library.

To create the Disaster Recovery ACSLS disk, you must have at least one full backup of the local backup server. If not, take a full local backup of the backup server machine. You can only create the disk from the local backup server itself and cannot use the Create Boot Kit wizard from a remote backup server.

Create Disaster Recovery ACSLS Disks

Important! Arcserve has signed an agreement with STK that stipulates that you, as a Arcserve customer, can copy and reproduce directly a single copy of the StorageTek Library Attach from each of your computers to a User Disaster Recovery disk and a single copy for archival purposes. You can replace this single copy from time to time. Additionally, if you have multiple off-site disaster recovery locations, you can make this number of copies of the StorageTek Library Attach for each offsite disaster recovery location.

To create the Disaster Recovery ACSLS disk

1. From the Manager, open the Create Boot Kit wizard, select the Create Machine Specific Recovery Disk option, and click Next.

2. Select your local backup server from the list of backup servers and click OK.

3. Select your local backup server from the list of protected client machines and click Next.

4. Insert an empty floppy disk into the floppy drive and click Start. The wizard creates the machine-specific recovery disk for the local backup server.

5. The wizard checks whether a Disaster Recovery ACSLS disk is needed to recover the local backup server. You can choose whether to create the disk or not.

   ■ Click Yes to create this disk if this is the first time the disk is being created.

   ■ You do **not** have to create this disk if all of the following conditions apply:

      ■ A Disaster Recovery ACSLS disk has already been created for the local backup server machine.

      ■ The backup media (Tape Library Option or Enterprise Option for StorageTek ACSLS) configuration has not changed since the last disk was created.

      ■ The StorageTek LibAttach configuration has not changed since the last disk was created.

   If these conditions are met, exit the wizard.

6. Insert an empty floppy disk into the floppy drive and click Start.

7. The wizard locates all the necessary files and copies these files onto the floppy disk. If the wizard fails to locate any of the files, it prompts you to locate each missing file manually.

Your Disaster Recovery ACSLS disk has been created.

Note: We strongly recommend that you create the Disaster Recovery ACSLS disk immediately after the first full backup of the local backup server machine.

Create the Disaster Recovery ACSLS Disk from an Alternate Location

If you have configured an alternate location in which to store disaster recovery information, you can create the Disaster Recovery ACSLS disk even after a disaster.

If the local backup server machine crashes and you do not have the Disaster Recovery ACSLS disk, you can create the disk from the remote Disaster Recovery alternate location. To create this disk, copy all of the files in the following directory to an empty floppy disk:

\\%remote machine%\%shared folder%\%backup server name%\acsls

Recover from Disaster Using ACSLS Libraries

You can recover from disaster using ACSLS libraries.

To perform disaster recovery of the local backup server using a StorageTek ACSLS library

1. Boot from the Microsoft Windows Server 2003 CD and press F2 to enter Windows ASR mode.

2. The machine reboots after the bluescreen setup. After the reboot, the machine enters the GUI mode setup and starts the Disaster Recovery wizard.

3. The Disaster Recovery wizard prompts you to insert the Arcserve Backup CD/DVD and the machine-specific recovery disk.

   Note: The machine specific recovery disk is also called the machine specific disk (MSD).

4. After copying all files from the CD and floppy disk, the Disaster Recovery wizard determines whether the Disaster Recovery ACSLS disk is required.

   If it is not required, the wizard sets up the network and starts the main Restore wizard.

   If the Disaster Recovery ACSLS disk is required, you are prompted to insert the disk.

5. The Disaster Recovery wizard copies all files from the Disaster Recovery ACSLS disk and restores the StorageTek ACSLS services on the local computer. If it fails to restore the StorageTek ACSLS services, or if you cannot supply the Disaster Recovery ACSLS disk, a warning message appears indicating that the restore process may not be able to use the StorageTek ACSLS library.

6. The main Restore wizard starts.

   Continue with the normal disaster recovery procedure.

Appendix G: Recovering Windows 2003 Small Business Server

Windows Small Business Server 2003 is an important member of the Microsoft Windows product family, providing a comprehensive IT solution for small to medium enterprises. The Windows Small Business Server 2003 installation package provides some commonly used Windows services and applications including Internet Information Service (IIS), ASP.Net, Microsoft Exchange Server and Microsoft SharePoint service. This appendix describes how to back up and restore these services and applications appropriately for disaster recovery purposes.

Note: This appendix contains information on backing up and restoring the default configurations of Windows Small Business Server 2003. It does not serve as a comprehensive reference for all Windows Small Business Server 2003 recovery procedures.

This section contains the following topics:

Windows Small Business Server 2003 Default Settings

By default, Microsoft Windows Small Business Server 2003 installs the following components when setting up a computer:

- Microsoft Active Directory: Also creates a new domain and updates the machine to a Domain Controller.

- IIS 6 integrated with ASP.net: Creates a default website and configures it with Microsoft Frontpage extension.

- DNS

- Microsoft Exchange Server 6.5 integrated with Active Directory

- Microsoft SQL Desktop Engine 2000

- Windows Microsoft SharePoint Services 2.0: Creates a virtual website, called companyweb, and configures it using the Microsoft SharePoint extension.

- Other common network services (for example, optional DHCP, Firewall, and Windows Cluster)

Arcserve Backup Requirements

In addition to the Arcserve Backup base, the following options are required to back up Windows Small Business Server 2003 data correctly:

- Arcserve Backup Agent for Open Files for Windows

- Disaster Recovery Option

- Arcserve Backup Agent for Microsoft Exchange Server

- Other options relevant to your storage devices

The Windows Small Business Server 2003 Premium Edition also installs the Microsoft SQL 2000 Server (Service Pack 3) and uses it instead of Microsoft Desktop Engine (MSDE). If you install the Premium Edition, you must also install the Arcserve Backup Agent for Microsoft SQL Server.

Disaster Preparation for Windows Small Business Server 2003

In addition to a regular full machine backup, the following backups are required to protect the applications:

- **Microsoft Exchange Server**: Using the Agent for Microsoft Exchange Server, you can back up your Microsoft Exchange Server data at two levels: Database level and Document level. Database level backups treat all Microsoft Exchange data as a whole and back up all data as one information store (database). Document level backups can provide more subtle granularity. For disaster recovery purposes, we recommend using the Database level backup.

- **Microsoft Desktop Engine (MSDE)**: Windows Small Business Server 2003 installs MSDE as the primary storage container for Microsoft SharePoint Services. Certain other applications (such as SBSMonitor) also save data in the MSDE. The Arcserve Backup Client for Microsoft VSS Software Snap-Shot MSDEwriter is used to back up MSDE data.

- **Microsoft SQL Server**: Windows Small Business Server 2003 Premium Edition allows you to use Microsoft SQL Server 2000 instead of MSDE. If you use Microsoft SQL Server, use the Agent for Microsoft SQL Server to back up the Microsoft SQL Server data.

Windows Small Business Server 2003 Disaster Recovery

To recover a Windows Small Business Server 2003 server machine, first follow the normal disaster recovery procedure for Windows 2003. The regular disaster recovery procedure brings the machine back to its last full backup state but without any database data. This section provides procedures to recover the databases.

For information about recovering Windows 2003 machines, see section "Disaster Recovery on Windows 2003 and Windows XP (see page 77)".

Other Applications

Windows Small Business Server 2003 default services can be recovered during the operating system disaster recovery process. If you have installed third party applications other than those covered in this section, see the appropriate Arcserve Backup agent or option guide for information about recovering these applications.

Microsoft SharePoint Service Restoration

If you do not update your Microsoft SharePoint data frequently (for example, if you use the Agent for Open Files), the Microsoft SharePoint Service may run without any special recovery procedures after the disaster recovery process finishes. However, this data can become corrupted and we strongly recommend that you use the following procedures to fully recover your Microsoft SharePoint Service data.

How Microsoft SharePoint Service Data is Recovered

The following process allows you to fully recover your Microsoft SharePoint Service data:

1. Delete the Microsoft SharePoint website and uninstall Microsoft SharePoint.

2. Reinstall Microsoft SharePoint and MSDE to create the MSDE meta databases.

3. Restore the Microsoft SharePoint Service.

This section provides information and procedures relating to each step in the process.

Delete the Microsoft SharePoint Website and Uninstall Microsoft SharePoint

You can delete the Microsoft SharePoint website and uninstall Microsoft SharePoint.

To delete the Microsoft SharePoint website and uninstall Microsoft SharePoint

1. From the Start menu, select Control Panel and click Add or Remove Programs.

2. Select Microsoft SharePoint 2.0 and all MSDE components (SharePoint and SBSMonitoring) to uninstall them.

3. From the Internet Information Service (IIS) Manager Console Administrative Tools, under Websites, delete the companyweb and SharePoint Central Administration Web sites.

4. In the IIS Manager, under Application Pools, right-click StsAdminAppPool and select Delete from the pop-up menu.

5. Delete or rename the Microsoft SharePoint and companyweb folders.

6. Delete the following registry keys:

    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MicrosoftSQL Server\SHAREPOINT
    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SmallBusinessServer\Intranet

Reinstall Microsoft SharePoint and MSDE

When you have uninstalled Microsoft SharePoint, you must reinstall Microsoft SharePoint and MSDE to create the MSDE meta databases. To do so, perform the following procedure:

To reinstall the Microsoft SharePoint and MSDN

1. From the Windows Small Business Server 2003 installation CD, reinstall the Microsoft SharePoint Service from:

    X:\SBS\CLIENTAPPS\SHAREPT\setupsts.exe

    where X is the drive letter of your CD-ROM drive.

    Note: If your installation CD has the MSDE core file digital signature issue and it has expired, download the updated Microsoft SharePoint Services setup program (STSV2.exe) to reinstall Microsoft SharePoint Services.

2. During the last stage of the reinstallation, an error message appears, informing you that there has been a Microsoft SharePoint Setup error, and that the installation has failed to update your default website. This error message is specific to the Windows Small Business Server 2003 Microsoft SharePoint installation and can be ignored.

    Close the page and click OK.

3. After installation, STS creates the Microsoft SharePoint Central Administration site and the Microsoft SharePoint configuration database, called STS_config.

   If the Microsoft SharePoint configuration database, STS_config, is missing, you may have an expired MSDE core file digital signature issue. Perform the following steps to address this problem:

   a. Delete the Microsoft SharePoint website and uninstall Microsoft SharePoint.

      Note: See section Delete the Microsoft SharePoint Website and Uninstall Microsoft SharePoint (see page 206) for more information about deleting and uninstalling.

   b. Download the updated Microsoft SharePoint Services setup program (STSV2.exe).

   c. Return to the beginning of this topic to reinstall Microsoft SharePoint and MSDE

4. In the IIS Manager, under Websites, create a new virtual Website, name it companyweb, and select its home path. The default path is typically c:\inetpub\companyweb. If you use the default location, the path will be restored to the original after all restore operations are complete.

5. In the STS installation procedure, the setup selects a random TCP port to create the Microsoft SharePoint Central Administration Site. To be consistent with your original settings, use the IIS Manager to change the port to 8081, the original setting before the backup.

6. Launch the Microsoft SharePoint Central Administration Site: http://localhost:8081 from Microsoft Internet Explorer to create a new Microsoft SharePoint website to restore the original Microsoft SharePoint content.

   The Microsoft SharePoint Central Administration home page opens.

7. Click Extend or upgrade virtual server and select companyweb from the virtual site list.

8. From the Virtual Server List, select the server you want to update.

9. On the Extend Virtual Server page, select Extend and create a content database.

10. On the Extend and Create Content Database page, enter the appropriate information in the required fields.

    A new, randomly named, content database is created in MSDE.

Restore Microsoft SharePoint Service

Once the Microsoft SharePoint configuration databases have been rebuilt, you must restore the Microsoft SharePoint content databases. To do so, perform the following procedure:

To restore Microsoft SharePoint service

1. Using the Arcserve Backup Manager, restore all content database backups (STS_Config and STS_%machine_name%_1) to their original positions. The MSDE writer recreates the original content databases.

   Important! Restore only the content databases, STS_Config and STS_%machine_name%_1 under the MSDE writer.

2. Set the restored databases as the current content databases. To do so, perform the following steps:

   a. Launch the SharePoint Central Administration Site and select Configure virtual server settings and select the companyweb website.

   b. Select Virtual Server management and select Manage Content databases.

   c. On the Manage Content databases page, click the content databases created by the reinstallation process and enable the Remove content database option.

   d. Click OK.

3. On the same page, click Add a content database to add the restored databases as the current content databases.

   The Add a content database screen opens.

4. Enter the appropriate information in the required fields and click OK.

5. Launch http://companyweb/ to verify the result.

   The original Microsoft SharePoint data should be restored.

Microsoft Exchange Restoration

To restore Microsoft Exchange application data, select the Microsoft Exchange backup session from the Backup Manager and restore the session to its original location. However, you must ensure the following:

- You must be a member of the Exchange Administrator Group to restore Microsoft Exchange Server data.

  Note: In the Windows Small Business Server 2003 default settings, the administrator is automatically the administrator of the Microsoft Exchange Server.

- Before submitting the restore job, you must enter the Exchange Administrator user name and password

For more information about restoring Microsoft Exchange Server data, see the *Agent for Microsoft Exchange Server Guide.*

Appendix H: Recovering Data from a Physical to Virtual Machine

This section provides you with the information on how to perform Disaster Recovery from physical machines to virtual machines (P2V) using the Arcserve Backup Disaster Recovery Option. The following diagram illustrates a typical P2V setting:
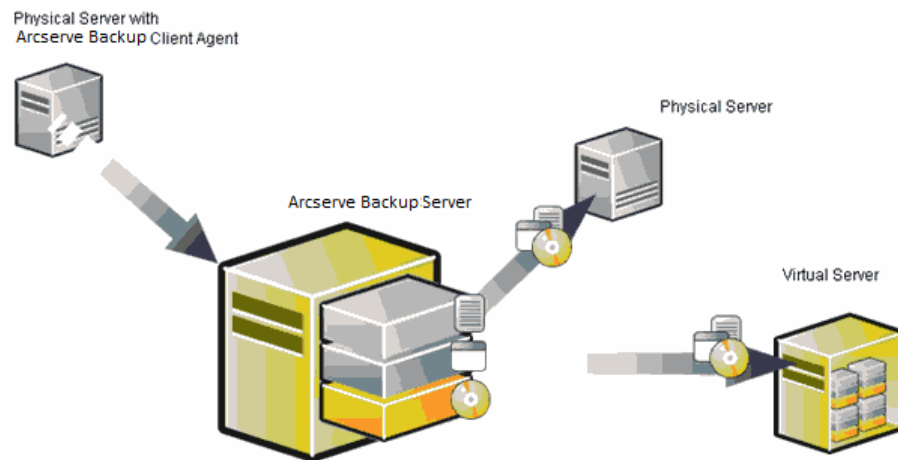
Now, using the Disaster Recovery Option you can recover a physical server to a virtual machine that is depot in some virtual infrastructures like VMware ESX Server and Microsoft Hyper-V Server.

This section contains the following topics:

Prerequisites

You must have knowledge on Arcserve Backup Disaster Recovery Option, Microsoft ASR, network configuration utility netsh, and the usage of VMware ESX server and Microsoft Hyper-V Server.

Operating Systems

The operating systems supporting the disaster recovery from physical machines to VMware virtual machines include:

■ Microsoft Windows 2008 (R2)

■ Microsoft Windows 2003 (R2)

■ Microsoft Windows XP Professional

The operating systems supporting the disaster recovery from physical machines to Hyper-V virtual machines include:

■ Microsoft Windows 2008

■ Microsoft Windows 2003 (R2)

Virtual Infrastructures

This feature is supported on VMware ESX Server 2.5 and higher virtual infrastructures from VMWare and Microsoft Hyper-V Server .

Software Requirements

The following information provides some information about the software requirements:

■ Arcserve Backup Base r15 or later versions

■ Arcserve Backup Disaster Recovery Option

■ Arcserve Backup Client Agent (for remote recovery)

Scenarios for Local and Remote Restore

The backup images could be local or remote and you can perform a local restore or remote restore of these images. This section provides best practices for the following scenarios:

■ Local Backup and Local Restore (see page 213)

■ Remote Backup and Remote Restore (see page 214)

■ Local Backup and Remote Restore (see page 216)

Note: Arcserve Backup is designed to restore the backup image to the machine with similar hardware configuration. Ensure that both the virtual machine and the physical machine are configured similarly to perform a P2V restore.

Local Backup and Local Restore

You must perform a full backup of your physical machine to the local tape and create a machine specific recovery disk (MSD). Use the bootable CD or the installation CD and the floppy disk to restore the backup data from the backup tape to the virtual machine using the similar method you use to restore to the physical machine.

Note: Microsoft Hyper-V VM can boot from the first IDE disk only, so you must configure the VM properly to ensure that the system disk is restored to the first IDE disk.

Network Interface Card (NIC) is Nonfunctional after a Local Restore to a VM Hosted on VMWare ESX Server

The Network Interface Card (NIC) does not function properly when the system restarts after a local restore.

You can use one of the following solutions to solve this problem:

■ Install the VMware Tools on the virtual machine for the NIC to work properly.

■ Uninstall the network driver and reinstall it as shown:

a. Log into the recovered system on the virtual machine.

b. Click Start, Control Panel, Administrative tools, Computer Management and Device Manager.

c. Right-click on the network adapter and click uninstall as shown:
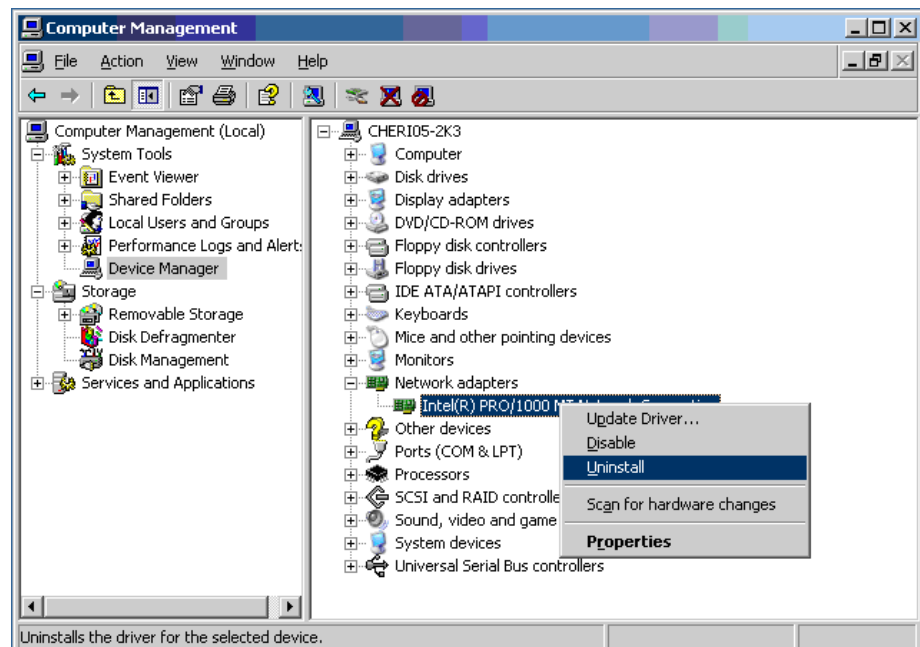
d. Right-click on the host name after uninstall and select Scan for hardware changes to scan the hardware changes. The network adapters are automatically reinstalled.

e. Configure the IP address of the host machine to DHCP, after installing the network adapter.

Remote Backup and Remote Restore

You can perform remote backup and remote restores.

Restore to a Hyper-V Virtual Machine

Before you can perform a remote restore on a Hyper-V virtual machine you must perform the following procedure on the Windows Server 2003(x64).

Note: Microsoft does not provide a driver for Legacy Network Adapter for Windows 2003 (x64), so you must use the default Network Adapter to perform recovery.

To perform recovery on a Hyper-V virtual machine

1. Start the disaster recovery process.

2. When Disaster Recovery wizard appears, from Hyper-V VM console, select Action, and insert Integration Service Setup Disk.

3. Open a command window from disaster recovery wizard.

4. Switch to the CD / DVD drive and switch to folder support\amd64 and enter setup.exe.

5. Run the setup wizard to complete setup process using the default settings.

   Important! Do not reboot the server when the setup prompts you to reboot.

6. Switch backup to disaster recovery wizard and start recovery.

For Windows 2003(x86) and 2008(x86, x64), starting the disaster recovery process, add a Legacy Network Adapter to the virtual machine.

To add Legacy Network Adapter

1. Select Settings, and then select Add Hardware.

   The Add Hardware dialog appears.

2. Select the Legacy Network Adapter.

   The network adapter dialog appears.

   The legacy network adapter is added.

Driver of the Legacy Network Adapter is included in Windows installation media, so do not install integration service during disaster recovery process.

Note: In Windows 2003 (x86), you must install Hyper-V Integration Services after performing disaster recovery and reboot, else the NIC and other services included in Integration Services will not work.

Unable to Establish a Connection with tape engine

The connection to the tape engine is not established when the Disaster Recovery restore begins.

Note: For Windows XP / 2003 / 2008 you can configure IP address on disaster recovery wizard.

To establish a connection with Tape Engine

1. Open command prompt from Restore Manager.

2. Execute the following command:

    ipconfig

    Note: You must configure a new IP address when the available IP address is 169.254.159.XXX or there is no IP address assigned. Arcserve Backup cannot restore original IP address of the new NIC when a new MAC address is assigned.

3. Execute the windows command netsh to add an address to the NIC.

4. Modify the following files by adding Server IP address and the Server name:

    Microsoft Windows XP/ 2003/ 2008(R2)

    C:\WINDOWS\system32\drivers\etc\hosts

5. Go to the following directories of the respective platforms and execute drw command to start the usual restore process:

    Microsoft Windows XP/ 2003/ 2008(R2)

    C:\WINDOWS\system32\DR

    This establishes the connection with the Tape Engine.

Network Interface Card (NIC) Nonfunctional after a Remote Restore

The NIC does not function properly when the system restarts after a remote restore.

For more information, see Network Interface Card (NIC) Nonfunctional after a Remote Restore to VM Hosted on VMWare ESX Server (see page 213).

Local Backup and Remote Restore

You can perform local backup and remote restore by following the scenarios provided in this section.

Network Interface Card (NIC) Nonfunctional after a Remote Restore to VM Hosted on Microsoft Hyper-V Server

The NIC does not function properly when the system restarts after a remote restore. For Windows 2003 (x64), after disaster recovery the network adapter does not work and you may not be able to install integration service properly. You must perform the following steps below to install integration service.

To install the integration service

1. Remove file C:\Windows\System32\Drivers\wdf01000.sys.

2. Remove registry key HKLM\System\CurrentControl\Services\wdf0100.

3. Reboot the VM and log in.

4. Select Action, insert Integration Service Setup Disk from VM console and install.

   Integration service is installed.

Scenario 1

In this scenario, assume that TEST-SERVER is a locally backed up server with an IP address of 192.168.1.224.

To recover TEST-SERVER on a virtual machine, you must manually update some files in the Machine Specific Recovery Disk (MSD) floppy to the new server, as TEST-SERVER-REP with an IP address of 192.168.1.226, to avoid IP conflict and complete the recovery. You can then rename the new server with the physical machine host name and IP address.

Note: To avoid IP address conflict, you must disconnect the physical machine when you reboot the virtual machine after completion of the restore job.

To modify the MSD floppy for Windows Server 2003 or Windows Server 2008

1. Modify the following file using a text editor .

    ■ **AdrCfg.ini**

       In [ClientConfig], modify the value ClientName from TEST-SERVER to TEST-SERVER-REP.

       In [ServerConfig], modify the value ClientName from TEST-SERVER to TEST-SERVER-REP.

       In [DRConfig], modify the value DrType from Local to Remote.

    ■ **AdrNet.ini**

       In [SystemInfo], modify the value MachineName from TEST-SERVER to TEST-SERVER-REP.

       Modify the record IP address from 192.168.1.224 to 192.168.1.226

2. Rename the following files:

    ■ TEST-SERVER.ses to TEST-SERVER-REP.ses

Scenario 2

In this scenario, assume that the server has been locally backed up, the server name is TEST-SERVER with an IP address of 192.168.1.224. To recover this server to a virtual machine from another server DR-SERVER, perform the following procedure to modify the MSD floppy. You can modify the MSD floppy for Windows Server 2003 file using a text editor:

AdrCfg.ini
In [ClientConfig], modify the value BrightStorServer from TEST-SERVER to DR-SERVER.
In [ServerConfig], modify the value BrightStorServer from TEST-SERVER to DR-SERVER.
In [DRConfig], modify the value DrType from Local to Remote.

Note: Ensure that the name does not exceed 15 characters.

Other Known Issues

This section describes some issues that may occur when recovering data from a physical to a virtual machine.

Unable to Load the SCSI Disk

When you restore the Microsoft Windows XP machines to virtual machines on the ESX, use F6 to add additional SCSI drivers and set the SCSI to use LSIlogic mode. Now you can use the LSI Logical SCSI driver, which you can download from http://www.vmware.com/

Multi SCSI Adapter and Multiple Hard Disks

You must consider the following:

■ The number of disks on the virtual machines must be equal to the number of disks on the physical machines.

■ The size of the disk on the virtual machine must be equal or greater than the size of the disk on the physical machine.

■ When configuring virtual hard disks, you must make sure that the virtual disks are in the same sequence as the disk numbers displayed in disk manager on the physical machine.

■ The boot disk should be same as the original one. You may need to configure the boot sequence of hard disks in BIOS setup of virtual machine as shown in the following illustration:
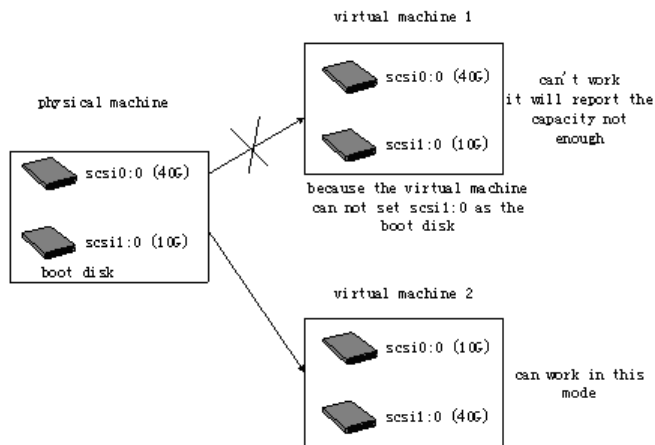
Note: Check with the specification of each disk.

Modify a Registry File

You can modify a registry file using the following procedure:

To modify a registry file:

1. Run the registry editor and select KEY_LOCAL_MACHINE.

2. Select Load Hive from the menu, and select the file you want to edit.

3. Assign a temporary name to the key, for example, tmpKey as shown in the screen:
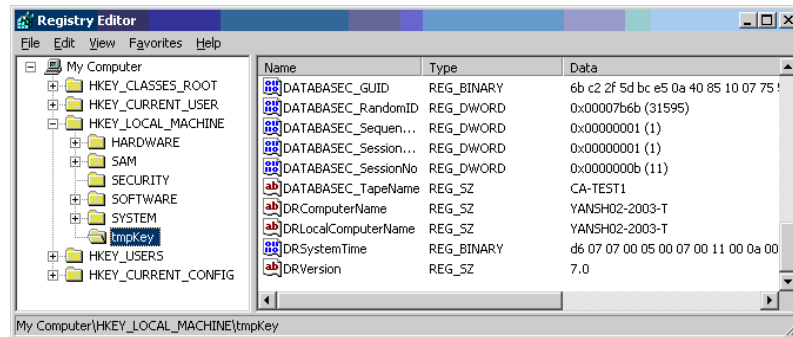
4. You can see the values in this key in the right panel of the registry editor.

5. Double-click the row you want to modify and then edit it.

6. Select tmpKey in the left panel of the registry editor to verify the modified registry values, and go to the File menu, Unload Hive. The changes are applied to the file you just modified.

   For more information , refer the *VMWare ESX User Manual and MSDN*.

Appendix I: Recovering Data Without Using a Floppy in Windows 2003 and Windows XP

You can recover data without using a floppy disk or a CD-ROM in Windows XP and Windows Server 2003.

This section contains the following topics:

Remote Installation Service (RIS)

The Remote Installation Service (RIS) based floppy-less Disaster Recovery using Arcserve Backup is currently supported on the following operating systems:

- Microsoft Windows XP

- Microsoft Windows Server 2003

How to Prepare for a Disaster Recovery without Using Floppy

You must perform the following steps to prepare for RIS based bare metal recovery:

- Check with prerequisites

- Install and configure RIS

- Prepare OS images

- Prepare setup answer file for each OS image

- Prepare DR binaries for each OS images

Installation Prerequisites

This section provides the prerequisites for hardware and software installation.

RIS Server Hardware Requirements

The following are the hardware prerequisites for the RIS server:

- Minimum hardware requirements to install Microsoft Windows Server 2003.

- 4 GB hard disk drive

  Note: Dedicate a complete hard disk or a partition specifically to store the RIS directory tree. For this, you can use SCSI-based disk controllers and disks.

- 10 or 100 Mbps network adapter that supports TCP/IP. However, the 100 Mbps is preferred.

Before you install the RIS, you must format the hard disk drive with the NTFS file-system on the server. Make sure you have enough disk drive space to install the operating system and the RIS remotely.

Note: Do not install the RIS on the same drive or partition on which Microsoft Windows Server 2003 is installed.

Client Hardware Requirements

Before you install the RIS on the client machines, you must meet the following hardware requirements:

- You must meet the minimum hardware requirement to install the operating system.

- PXE DHCP-based boot ROM Network adapter version 1.00 or later. You can also use a network adaptor that is supported by RIS boot disk.

Note: Contact the manufacturer of the network adapter to obtain the latest version of the PXE DHCP-based boot ROM.

Software Requirements

You must activate network services to use for RIS. Install and activate the following services on the RIS server or on other servers available on the network:

- Domain Name System (DNS Service)

- Dynamic Host Configuration Protocol (DHCP)

- Active Directory Service

How to Install and Configure RIS

Installing and configuring RIS includes the following five major steps:

- Install RIS

- Configure RIS

- Authorize the RIS in Active Directory

- Set user permissions

- Enable the RIS troubleshooting option

Install Windows Server 2003 RIS

You must install the Remote Installation Service on the Windows Server 2003 using the following procedure:

Note: If you are prompted for the Windows Server 2003 installation files, insert the Windows Server 2003 installation CD and click OK. Click No if you are prompted to upgrade the operating system.

To install the Windows Server 2003 RIS:

1. Click Start, Control Panel, select Add or Remove Programs.

   The Add/Remove windows components dialog appears.

2. Select the Remote Installation Service option and click Next.

   You will be asked to provide the OS CD and the RIS installation will be launched.

3. Click Finish.

   You will be prompted to restart your computer.

4. Click Yes.

   The Windows Server 2003 RIS installation is complete.

Initialize RIS

You can initialize the RIS using the following procedure:

To initialize the Remote Installation Service

1. Log in to your machine using the administrator privileges.

2. Click Start, Run.

3. Enter risetup.exe in the Run dialog and click OK to start the RIS Setup Wizard.

4. Click Next on the Welcome screen.

5. Enter the path of the folder in which the RIS files are located, and click Next.

   The RIS Setup Wizard copies the files from the location you specified.

6. Select from the following options to control the client computers:

   Respond to client computers requesting service

   Enables the RIS that responds to the client machines which request for the services.

   Do not respond to unknown client computers

   Enables RIS to respond to only the known client machines.

   Select the Respond to client computers requesting service, and click Next. You are prompted to specify the location of the client operating system installation files.

7. Insert the Client operating system installation CD and click Next to enter the folder name for the client operating system installation files on the RIS server and click Next.

8. Enter the description for the operating system image. It is displayed when you start the remote client and run the Client Installation Wizard.

9. Click Next and Finish.

   The RIS initialization is complete.

How to Install and Configure RIS

Set User Permissions

Using RIS, you can allow the users to install the client operating system on their client machines. You must also grant permissions for users to create computer accounts in the domain.

To allow users to create computer accounts in the domain

1. Click Start, Administrative Tools, and Active Directory Users and Computers.

2. Right-click your domain name in the left pane and select the Delegate Control option.

   The Delegation of Control Wizard appears.

3. Click Next, and click Add.

4. Enter the name of the group that requires permission to add computer accounts to the domain, and click OK.

5. Click Next and select the option Join a computer to the domain.

6. Click Finish.

   The user permissions are set.

Appendix I: Recovering Data Without Using a Floppy in Windows 2003 and Windows XP 225

Enable RIS Troubleshooting Option

To enable the Automated System Recovery (ASR) support for RIS service, you must enable the Tools option in the RIS options.

To enable the RIS troubleshooting option

1. Click Start, Administrative Tools, and click Active Directory Users and Computers.

2. Right-click your domain name in the left pane, and click Property.

   The Domain Property Sheet appears.

3. Select Group Policy and click Default Domain Policy.

4. Click Edit.

5. Select User Configuration from the left pane, and then click Windows Settings.

   The Windows Settings dialog appears.

6. Select Remote Installation Service.

7. Double-click Choice Options from the right panel.

   The Choice Options property page appears.

8. Select the options as follows:

   Automatic Setup - Disabled

   Custom Setup - Disabled

   Restart Setup - Disabled

   Tools - Enabled

9. Click OK.

   The troubleshooting option is enabled.

Prepare OS Images

You must create (OS) images for each type of Windows operating system in your environment.

To create OS images

1. Login as a user with administrative privileges and from the Start menu and click Run.

2. Enter risetup.exe in the Run dialog and click OK.

   The RIS Setup Wizard appears.

3. Click Next on the Wizard Welcome screen.

4. Select Add a new OS image to the RIS server and click Next.

5. Specify the location of the client operating system installation files or insert the client operating system installation CD and then click Next.

6. Specify the folder name for the client operating system installation files on the RIS server, and then click Next.

7. Enter the description for the operating system image. It will be displayed to the users when they run the Client Installation Wizard on the remote client machine.

8. Select Use the old installation screens option and click Next.

9. Click Next to copy the OS image to the hard drive.

10. Click Finish.

    The OS images are created.

How to Prepare Setup Answer File for Specific OS Image

You can prepare the setup answer file for specific OS image using the following process:

1. Each OS image has a RIS setup answer file which can be located in the following path on RIS server:

    Drive:\RemoteInstall\Setup\Language\Images\ImageName\I386\template\ristndrd.sif

    The RIS setup answer file is in .ini format. For more information on the RIS setup answer files, see the *Windows deploy document*. By default, this file is configured for normal setup. You must change it to support Windows ASR mode.

2. You must configure the RIS setup answer file for each OS image only once. Open the RIS setup answer file. In the [OSChooser] session, modify the key values:

3. Change the following key-value pair:

    ImageType= Flat

    to

    ImageType = ASR

4. Add the following key-value pairs:

    ASRFile=asrpnpfiles\%guid%.sif

    ASRINFFile=\Device\LanmanRedirector\%SERVERNAME%\RemInst\ASRFiles\%guid%.sif

    Note: The **guid** parameter is the computer UUID which is stored in computer BIOS. To know the UUID, launch remote install on the client machine which is being recovered and go through the OS chooser screens. A *.sif* file is generated in the Drive:\RemoteInstall\temp folder on the RIS server. The file name of this file is the UUID of the client machine.

    The RemInst value in the ASRINFFile must have the same name as RemoteInstall directory. The RemInst is the default share name created by RIS setup.

5. Create the following directories in the Drive:\RemoteInstall\ folder:

    ■   ASR Files

    ■   ASRPN Files

Prepare DR Binaries for OS Image

You must prepare DR binaries and configure them to each OS image only once. Perform the following steps:

To prepare DR Binaries for the OS image

1. Create a directory named BOOTDISK in the image directory as shown in the following example:

   X:\RemoteInstall\Setup\<Language>\Images\<ImageName>\BOOTDISK

2. Insert the Arcserve Backup installation CD on the RIS server and copy all files available in the BOOTDISK directory of the root directory of the CD to the new BOOTDISK directory you just created.

3. Create a directory drpatch.xp in the image directory as shown in the following example:

   X:\RemoteInstall\Setup\<Language>\Images\<ImageName>\drpatch.xp

4. Copy all the files available in the BAB_HOME\drpatch.xp directory from the machine on which Arcserve Backup and Option for Disaster Recovery are installed, to the new drpatch.xp directory you just created.

   Note: To do this, you must have the Arcserve Backup Server on which Disaster Recovery Option is installed. You can find the BAB_HOME\drpatch.xp on the Arcserve Backup server machine in the following location:

   C:\Program Files\CA\ARCserve Backup

5. For 32-bit Windows, create a Windows batch file named "DR_ASR.BAT" manually and copy it to the image directory as shown:

   X:\RemoteInstall\Setup\<Language>\Images\<ImageName>\DR_ASR.BAT

   The content of this batch file is as follows:

   rem X:\RemoteInstall\Setup\<Language>\Images\<ImageName>\DR_ASR.BAT

   ```
   echo off
   echo Creating DR directories ...
   if not exist "%SystemRoot%\SYSTEM32\DR"(
   call mkdir "%SystemRoot%\SYSTEM32\DR"
   )
   if not exist "%SystemRoot%\SYSTEM32\DR\DRIF" (
   call mkdir "%SystemRoot%\SYSTEM32\DR\DRIF"
   )
   if not exist "%SystemRoot%\SYSTEM32\DR\DISK" (
   call mkdir "%SystemRoot%\SYSTEM32\DR\DISK"
   )
   if not exist "%SystemRoot%\SYSTEM32\DR\ENU" (
   call mkdir "%SystemRoot%\SYSTEM32\DR\ENU"
   )
   ```

```
echo Creating DR directories done
echo Copying DR binary files ...
pushd "%systemdrive%\$win_nt$.~ls\drpatch.xp\"
call expand -r * %SystemRoot%\SYSTEM32\
popd
if exist "%systemdrive%\$win_nt$.~ls\drpatch.xp\ENU\" (
pushd "%systemdrive%\$win_nt$.~ls\drpatch.xp\ENU\"
call expand drlaunchres.dl_ %SystemRoot%\SYSTEM32\drlaunchenu.dll
popd
)
pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\"
call expand -r * %SystemRoot%\SYSTEM32\DR\
popd

if exist "%systemdrive%\$win_nt$.~ls\BOOTDISK\ENU\" (
pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\ENU\"
call expand -r * %SystemRoot%\SYSTEM32\DR\ENU\
popd
)

echo Copying DR binary files done
echo Copying DR emergency data ...

pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy *.exe "%SystemRoot%\SYSTEM32\DR\" /Y
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy *.dll "%SystemRoot%\SYSTEM32\DR\" /Y
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call expand -r *_ %SystemRoot%\SYSTEM32\DR\
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy * "%SystemRoot%\SYSTEM32\DR\DRIF\" /Y
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy * "%SystemRoot%\SYSTEM32\DR\DISK\" /Y
popd
if exist "%SystemRoot%\SYSTEM32\DR\OBDRSIGN" (
call del "%SystemRoot%\SYSTEM32\DR\OBDRSIGN" /Q
)
if exist "%SystemRoot%\SYSTEM32\DR\OBDRDTCT" (
call del "%SystemRoot%\SYSTEM32\DR\OBDRDTCT" /Q
)

echo Copying DR emergency data done
echo on
```

6. For 64-bit Windows, create a Windows batch file named "DR_ASR.BAT" manually and copy it to the image directory as shown:

X:\RemoteInstall\Setup\<Language>\Images\<ImageName>\DR_ASR.BAT

The content of this batch file is as follows:

```
rem E:\RemoteInstall\Setup\English\Images\W2K3\DR_ASR.BAT
echo off
echo Creating DR directories ...
if not exist "%SystemRoot%\SYSWOW64\DR" (
call mkdir "%SystemRoot%\SYSWOW64\DR"
)
if not exist "%SystemRoot%\SYSWOW64\DR\DRIF" (
call mkdir "%SystemRoot%\SYSWOW64\DR\DRIF"
)
if not exist "%SystemRoot%\SYSWOW64\DR\DISK" (
call mkdir "%SystemRoot%\SYSWOW64\DR\DISK"
)
if not exist "%SystemRoot%\SYSWOW64\DR\ENU" (
call mkdir "%SystemRoot%\SYSWOW64\DR\ENU"
)
if not exist "%SystemRoot%\SYSWOW64\DR\Agent" (
call mkdir "%SystemRoot%\SYSWOW64\DR\Agent"
)
echo Creating DR directories done
echo Copying DR binary files ...

pushd "%systemdrive%\$win_nt$.~ls\drpatch.xp\"
call expand -r * %SystemRoot%\SYSWOW64\
popd
if exist "%systemdrive%\$win_nt$.~ls\drpatch.xp\ENU\" (
pushd "%systemdrive%\$win_nt$.~ls\drpatch.xp\ENU\"
call expand drlaunchres.dl_ %SystemRoot%\SYSWOW64\drlaunchenu.dll
popd
)
pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\"
call expand -r * %SystemRoot%\SYSWOW64\DR\
popd
if exist "%systemdrive%\$win_nt$.~ls\BOOTDISK\ENU\" (
pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\ENU\"
call expand -r * %SystemRoot%\SYSWOW64\DR\ENU\
popd
)
pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\%3\"
call expand -r * %SystemRoot%\SYSWOW64\DR\Agent\
popd
pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\Agent\%3\"
call expand -r * %SystemRoot%\SYSWOW64\DR\Agent\
popd
pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\Agent\%3\%2\"
call expand -r * %SystemRoot%\SYSWOW64\DR\Agent\
```

```
popd

pushd "%systemdrive%\$win_nt$.~ls\BOOTDISK\ETPKI\%3\"
call expand -r * %SystemRoot%\SYSWOW64\DR\Agent\
popd
echo Copying DR binary files done
echo Copying DR emergency data ...

pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy *.exe "%SystemRoot%\SYSWOW64\DR\" /Y
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy *.dll "%SystemRoot%\SYSWOW64\DR\" /Y
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call expand -r *_ %SystemRoot%\SYSWOW64\DR\
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy * "%SystemRoot%\SYSWOW64\DR\DRIF\" /Y
popd
pushd "%systemdrive%\$win_nt$.~ls\DR\%1\"
call copy * "%SystemRoot%\SYSWOW64\DR\DISK\" /Y
popd
if exist "%SystemRoot%\SYSWOW64\DR\OBDRSIGN" (
call del "%SystemRoot%\SYSWOW64\DR\OBDRSIGN" /Q
)
if exist "%SystemRoot%\SYSWOW64\DR\OBDRDTCT" (
call del "%SystemRoot%\SYSWOW64\DR\OBDRDTCT" /Q
)

echo Copying DR emergency data done
echo on
```

How to Perform a Floppy-less Disaster Recovery

You can use the following steps to perform bare metal disaster recovery:

- Copy DR emergency data.

- Modify, copy and rename ASR.SIF

- Copy and rename ASRPNP.SIF

- Boot client via PXE.

- Run the RIS setup wizard and select the OS image.

How to Prepare DR Emergency Data

You must follow the given procedure each time you perform a disaster recovery:

To prepare DR Emergency data

1. Copy DR emergency data to OS image directory: Locate the DR directory in the home directory of the Arcserve Backup Server and copy the data to the following location on the RIS server:

   Drive:\RemoteInstall\Setup\Language\Images\ImageName

   Note: If you have multiple Operating System images to be supported in your environment, you must copy the DR directory to each OS image directory. For example, if you have machines with Windows XP Professional and Windows Server 2003 Standard editions installed, you should create two images on your RIS server, and copy the DR directory to both the image directories.

2. Configure ASR.SIF: Locate ASR.SIF in the DR\MachineName directory in the Arcserve Backup server home directory.

   a. Copy the ASR.SIF file from the DR directory to the following location on the RIS server and rename it to **UUID.SIF** :

   Drive:\RemoteInstall\ASRFiles.

   Note: You must remove all the hyphens in the UUID string, if there are any.

   For example, if you get the following UUID from some source (utility, BIOS): D4E493CA-BB82-4561-8D76-CFFE3D4885BA after you remove all the hyphens file name appears as D4E493CABB8245618D76CFFE3D4885BA.SIF.

   b. Open the file UUID.SIF, and make the modifications:

   For 32-bit Windows:

   [COMMANDS]

   1=1,3000,0,"%SystemRoot%\system32\asr_fmt.exe","/restore"

   2=1,4990,1,"%SystemRoot%\system32\asr_pfu.exe","/restore"

   3=1,2000,1,"%SystemRoot%\system32\asr_ldm.exe","/restore"

   4=1,4000,1,"%systemdrive%\win_nt.~ls\DR_ASR.BAT","BKServerName\MachineName >%systemdrive%dr_asr.log"

   5=1,4000,1,"%SystemRoot%\system32\drlaunch.exe",""

   For Windows 2003 x64:

   1=1,3000,0,"%SystemRoot%\system32\asr_fmt.exe","/restore"

   2=1,4990,1,"%SystemRoot%\system32\asr_pfu.exe","/restore"

   3=1,2000,1,"%SystemRoot%\system32\asr_ldm.exe","/restore"

   4=1,4000,1,"%systemdrive%\win_nt.~ls\DR_ASR.BAT","BKServerName\MachineName W2K3 X64>%systemdrive%\dr_asr.log"

   5=1,4000,1,"%SystemRoot%\syswow64\drlaunch.exe",""

   For Windows XP x64:

   1=1,3000,0,"%SystemRoot%\system32\asr_fmt.exe","/restore"

   2=1,4990,1,"%SystemRoot%\system32\asr_pfu.exe","/restore"

   3=1,2000,1,"%SystemRoot%\system32\asr_ldm.exe","/restore"

   4=1,4000,1,"%systemdrive%\win_nt.~ls\DR_ASR.BAT","BKServerName\MachineName WXP X64>%systemdrive%\dr_asr.log"

   5=1,4000,1,"%SystemRoot%\syswow64\drlaunch.exe",""

BKServerName refers to the one of the directory under DR directory, it means a backup server; MachineName refers to one of the directory name under BKServerName directory.

Note: You must modify this file each time you perform Disaster Recovery. This file records disk and volume settings of the client machine and helps ensure it matches with the latest configuration of the client machine you are recovering.

3. Configure ASRPNP.SIF: Locate this file in the DR\MachineName directory in the Arcserve Backup Server home directory and copy it to the following location on the RIS Server and rename it to UUID.SIF:

   Drive:\RemoteInstall\ASRPNPFiles

4. Configure scan session signature file: The drscans file invokes DRScansession utility for retrieving DR session from tape.

   While using RIS floppy-less Disaster Recovery, set the value FDUPDATE to FALSE, as you are not using the floppy.

Perform Bare Metal Recovery without Floppy

Before initiating Disaster Recovery without floppy, make sure that your network adapter supports PXE boot. You must also check that the capacities of all hard disks connected to the system being recovered are same or larger than the original hard disks capacities.

To perform a floppy-less bare metal recovery with RIS

1.   Remove all floppy disks (if any) and CDs from drive, and restart your machine.

2.   Press F12 key when POST screen appears.

     Important! For different machines, the key to invoke PXE bootstrap may be different. Please refer to your product manual for the correct key.

     The message Press F12 for network service boot appears if the RIS server is installed and configured properly.

3.   Click F12 on keyboard.

4.   Click Enter to go through the Operating System chooser welcome screen.

5.   Enter the domain credentials when prompted.

6.   Use the Up and Down arrow keys to select an Operating System image and click the Enter to continue.

     The Windows remote installation starts, and you may be prompted to confirm the installation.

7.   Click C on your keyboard and wait for the Arcserve Backup Disaster Recovery wizard to appear.

8.   The wizard appears.

     You can now start the recovery procedure.

Glossary

ACSLS Configuration

ACSLS (StorageTek Automated Cartridge System Library Software) is configured during backup time if all related ACSLS configurations and libraries are saved as part of the Disaster Recovery information. Disaster Recovery restores ACSLS configuration information automatically.

Advanced Mode

Advanced Mode assists you in customizing the restore process.

Alternate Machine Name

The Alternate Machine Name is the hostname of the machine where the shared folder resides. The IP address of this machine can also be used but we do not recommend this, particularly in DHCP environments.

ASDB Recovery Configuration

ASDB Recovery Configuration lets you recover your sessions automatically when you recover a primary or standalone server with Arcserve Backup Database installed locally.

Boot Volume

A boot volume is the disk volume that contains the Windows operating system files and its supporting files.

Bootable CD Method

The Bootable CD method is supported by Windows Server 2003 and Windows XP and uses only one disk and a recovery CD. It supports the protected client computer and the backup server. This method is built on the Windows ASR framework.

Bootable Tape Method

The Bootable Tape method is supported by Windows Server 2003 and can be used to protect only the backup server without having to create a machine specific disk. This method is built on the Windows ASR framework.

Client Agent Service

The Client Agent Service is a critical service used to communicate with backup servers for data recovery. Disaster Recovery will always start this service if the disaster recovery is local. If disaster recovery is remote, you can maintain the connection by clicking the link "Click Here" in the bottom pane of the screen to restart the Client Agent Service.

Cluster Configuration

Cluster Configuration displays in the Pre-flight Check screen if the backup server is a cluster node. If it is a cluster node, WinPE searches for an available cluster virtual node. If the cluster virtual node is available, WinPE DR omits the restore process of the cluster shared disk, otherwise Disaster Recovery will restore the cluster shared disk.

Disaster Recovery

Disaster recovery is a backup and recovery process used to protect computing environments against the loss of data caused by a catastrophic events or natural disasters.

Express Mode

Express Mode recovers the system automatically with minimal user intervention by using the machine default settings stored during backup time.

Hard Disk Status

The Hard Disk Status is a potential item that may show up on the Pre-flight Check screen describing the status of a hard disk. The status can be one of the following:

- If a hard disk is not available, the status indicates an error.

- If a hard disk is available, this item will not be displayed.

ISCSI Configuration

ISCSI Configuration enables you to configure ISCSI connections. This screen displays ISCSI connections during backup time and ISCSI connections during disaster recovery time.

Machine Specific Disk

The machine specific disk is the recovery disk used with the Windows XP or Windows Server 2003 installation media and the Arcserve Backup CD to perform disaster recovery using the Bootable CD method.

Note: The Machine Specific Disk (MSD) is also called the Machine Specific Recovery Disk.

Network Status

The Network Status is a potential item that may show up on the Pre-flight Check screen describing the status of the network connection. The status can be one of the following:

- If there is no network connection for Disaster Recovery, the status indicates no connection.

- If the network connection for Disaster Recovery is remote, the status indicates an error.

- If the network connection for Disaster Recovery is local, the status indicates a warning.

- If the network connection for Disaster Recovery is OK, this item will not be displayed.

Password

The password for the specified user account.

Password Management

Password Management is an item that shows up on the Pre-flight Check screen only if it is used during backup time. A Click Here link appears for you to open the Enter caroot password screen.

Path

The path for the shared folder in which to store the replicated disaster recovery information.

Pre-flight Check

The Pre-flight Check option provides a configuration list for you to detect and resolve potential environment issues. Essentially, for each item selected from the Configuration list, a description of that item is displayed at the bottom of the screen describing the issue.

System Volume

A system volume is the disk volume that contains the hardware-specific files required to start Windows, such as BOOTMGR.

Tape Engine Service

The Tape Engine Service is used only for local Disaster Recovery (DR).
From the Pre-flight Check screen, a Click Here link is displayed at the bottom of the screen to let you restart the Tape Engine Service in order to maintain the connections when there are remote file system devices or data deduplication devices.

USB Backup Device Configuration

The USB Backup Device Configuration is used during backup time where you configure backup devices (for example, tape drives, Iomega changers, and digital storage drives. For some USB backup devices, you may need to install additional drivers.

User Name

The User Name is the user account used to connect to the machine on which the alternate location resides. The domain part of the user name is optional. For example, if the full user account name is domainX\userX, you can enter userX.

WinPE

WinPE (Windows Preinstallation Environment) is a minimal Win32 Operating System that lets you prepare computers for Windows installations, copy disk images from network shared folders, and initiate Windows setup. Arcserve Backup lets you recover Windows Server 2003 and 2008 systems running Windows PE from a disaster using a Windows PE recovery CD.

Index