CA ARCserve® Backup for Windows

Disaster Recovery Option Guide

r12

CA Product References

This documentation set references the following CA products:

- Advantage™ Ingres®
- BrightStor® ARCserve® Backup for Laptops and Desktops
- BrightStor® CA-1® Tape Management
- BrightStor® CA-Dynam®/B Backup for VM
- BrightStor® CA-Dynam®/TLMS Tape Management
- BrightStor® CA-Vtape™ Virtual Tape System
- BrightStor® Enterprise Backup
- BrightStor® High Availability
- BrightStor® Storage Resource Manager
- BrightStor® VM:Tape®
- CA ARCserve® Backup Agent for Novell Open Enterprise Server for Linux
- CA ARCserve® Backup Agent for Open Files on NetWare
- CA ARCserve® Backup Agent for Open Files on Windows
- CA ARCserve® Backup Client Agent for FreeBSD
- CA ARCserve® Backup Client Agent for Linux
- CA ARCserve® Backup Client Agent for Mainframe Linux
- CA ARCserve® Backup Client Agent for NetWare
- CA ARCserve® Backup Client Agent for UNIX
- CA ARCserve® Backup Client Agent for Windows
- CA ARCserve® Backup Enterprise Option for AS/400
- CA ARCserve® Backup Enterprise Option for Open VMS
- CA ARCserve® Backup for Microsoft Windows Essential Business Server
- CA ARCserve® Backup for Windows
- CA ARCserve® Backup for Windows Agent for IBM Informix
- CA ARCserve® Backup for Windows Agent for Lotus Domino
- CA ARCserve® Backup for Windows Agent for Microsoft Data Protection Manager
- CA ARCserve® Backup for Windows Agent for Microsoft Exchange
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint

- CA ARCserve® Backup for Windows Agent for Microsoft SQL Server
- CA ARCserve® Backup for Windows Agent for Oracle
- CA ARCserve® Backup for Windows Agent for Sybase
- CA ARCserve® Backup for Windows Agent for VMware
- CA ARCserve® Backup for Windows Disaster Recovery Option
- CA ARCserve® Backup for Windows Disk to Disk to Tape Option
- CA ARCserve® Backup for Windows Enterprise Module
- CA ARCserve® Backup for Windows Enterprise Option for IBM 3494
- CA ARCserve® Backup for Windows Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Windows Enterprise Option for StorageTek ACSLS
- CA ARCserve® Backup for Windows Image Option
- CA ARCserve® Backup for Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup for Windows NDMP NAS Option
- CA ARCserve® Backup for Windows Serverless Backup Option
- CA ARCserve® Backup for Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup for Windows Tape Library Option
- CA XOsoft™ Assured Recovery™
- CA XOsoft™
- Common Services™
- eTrust® Antivirus
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM:Operator®

Contact CA

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Provide Feedback

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

If you would like to provide feedback about CA product documentation, please complete our short customer survey, which is also available on the CA Support website.

Contents

Chapter 4: Disaster Recovery on Windows XP and Windows Server 2003 and Windows Server 2008 55

Chapter 5: Disaster Recovery Scenarios 75

Appendix A: Recovering SAN Configurations 107

Appendix B: Recovering Clusters 109

Appendix C: Recovering NEC Clusters 121

Appendix D: Staging Using File System Devices 139

Appendix I: Recovering Data Without Using a Floppy in Windows 2003 and Windows XP 167

Appendix J: Troubleshooting 183

Chapter 1: Introducing the Option

CA ARCserve Backup is a comprehensive, distributed storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, business-critical applications, and network clients. In addition to a wide range of options, CA ARCserve Backup provides disaster protection with the CA ARCserve Backup Disaster Recovery Option.

Disaster recovery is a backup and recovery process used to protect computing environments against the loss of data caused by a catastrophic event or natural disaster. Disasters can be caused by fire, an earthquake, employee sabotage, a computer virus, or a power failure. By their very nature, disasters cannot be predicted in their intensity, timing, or effects.

When a mission-critical server goes down, only one thing matters—time. Each tick of the clock means business lost, opportunities squandered, and efforts wasted. You need to get your system back online quickly, accurately, and safely. The Disaster Recovery Option does this for you.

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 option lets you restore your server reliably with minimal effort, making more efficient use of time by taking you from boot media, to backup media, to an operational state faster than other solutions, and allows users with minimal server configuration experience to recover sophisticated systems.

This section contains the following topics:

Disaster Recovery

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 information 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 emergency data information for disaster recovery when it performs a regular full, incremental full or differential full backup of the computer. For more information about these types of backups, see the *Administration Guide*.

The option also generates or updates emergency data information for disaster recovery for the local backup server whenever the CA ARCserve Backup database is backed up (when the volume on which it resides is backed up).

Note: This does not apply if you use Microsoft SQL Server as the CA ARCserve Backup database.

Features and Functionality

The option provides a flexible, easy-to-use, enterprise-wide solution to protect your data on Windows 2000, Windows Server 2003, Windows Server 2008 and Windows XP based computers. It provides you with the following benefits:

- It protects your local CA ARCserve Backup server and remote client computers with the CA ARCserve Backup Client Agent installed.
- It lets you quickly put an unusable system back online, saving you substantial time when recovering from a disaster.
- It requires minimal user input, provided the recommended measures were performed before the disaster occurred.

Disaster Recovery Methods

Disaster Recovery methods are provided for specific versions of Windows as discussed in the following sections.

Windows 2000

On the Windows 2000 platform, the Disaster Recovery Option supports the local and the remote disaster recovery. The option provides the following three boot methods:

- **Bootable disk method**: Using a modified version of the Windows 2000 setup disks, you can recover any Windows 2000 computer using the Boot Kit wizard. You can start the Windows 2000 computer from the bootable disk, including those with unformatted hard drives, and fully restore your system using the backup media.
- **Bootable CD method**: Rather than using disks and a Windows 2000 CD, this recommended method, a faster way of booting to the Boot Kit wizard, uses only one disk and a recovery CD. The wizard then restores the system using the backup media.
- **Bootable Tape method**: Instead of booting from a disk drive or CD, you can boot Windows 2000 based servers using a tape drive. The option can perform a recovery directly from the backup tapes. The option creates a bootable backup tape for use with compatible tape drives and only requires the most recent backup media.

  Note: You must configure tape drives to act as boot devices. Because tape drive functionality varies by manufacturer, contact your tape drive vendor to determine if your tape drive capabilities meet your needs.

Windows XP and Windows 2003

The Disaster Recovery Option supports local and remote disaster recovery, letting you get Windows XP and Windows 2003 configurations back online quickly, accurately, and safely. The option provides the following boot methods:

- **Bootable CD method**: This solution is built on the Microsoft Windows Automated System Restore (ASR) framework.

  To use this method, you must have the following

  - Windows XP or Windows 2003 installation media
  - A machine-specific recovery disk
  - The CA ARCserve Backup CD

  You can also use the reimaged or remastered Bootable CD for this method. For information about reimaging bootable CD, see Reimage Bootable CD Using Boot Kit Wizard (see page 58).

  Note: The Window XP or Windows 2003 installation media you use to perform disaster recovery must be the same version you used to install the original system.

- **Bootable Tape method**: Rather than booting from a Windows XP or Windows 2003 installation media, you can boot directly from a tape drive. The only required media is the tape media containing the backup data.

  Note: One Button Disaster Recovery (OBDR) is not supported on OEM versions of Windows XP SP2. You must have the Microsoft shipped CD in your possession to perform OBDR.

Windows Server 2008

The Disaster Recovery Option supports local and remote disaster recovery, letting you get Windows Server 2008 configurations back online. The option provides the following boot method:

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

- Windows 2008 installation media
- A machine-specific recovery disk
- The CA ARCserve Backup CD

Note: The Windows Server 2008 installation media you use to perform disaster recovery must be the same version you used to install the original system.

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	Operating System Installation media+CA ARCserve Backup CD/DVD+ Floppy or USB Stick(for Windows Server 2008 only)	Windows 2000 Windows XP, 32 bit Windows XP, x64 Windows Server 2003, 32 bit Windows Server 2003, x64 Windows Server 2003, IA64 Windows Server 2008, 32 bit Windows Server 2008, x64 Windows Server 2008, IA64 Windows Server 2008, Core 32 bit (Remote DR only) Windows Server 2008 Core 64 bit (Remote DR only)
Bootable CD for Windows 2000 ■ Operating System ■ Disaster Recovery Option	CD+ CA ARCserve Backup CD/DVD+ Floppy	Windows 2000

Boot Kit Type	Required Media for Disaster Recovery	Supported Operating Systems
Bootable CD for Windows XP/Windows Server 2003 ■ Operating System ■ Disaster Recovery Option ■ MSD ■ Drivers(NIC and SCSI/RAID/FC)	CD+CA ARCserve Backup CD/DVD+ Floppy **Note:** In Windows 2003, you can integrate everything into a single Bootable CD, so no floppy disk is required.	Windows XP, 32-bit Windows XP, x64 Windows Server 2003, 32-bit Windows Server 2003, x64 Windows Server 2003, IA64
Patched CA ARCserve Backup Disaster Recovery CD	Floppy+ Windows Operating System installation media+ CD **Note**: Created CA ARCserve Backup Disaster Recovery CD will include all device/DR Option/Agent patches applied to CA ARCserve Backup installation.	Windows 2000 Windows XP, 32-bit Windows XP, x64 Windows Server 2003, 32-bit Windows Server 2003, x64 Windows Server 2003, IA64 Windows Server 2008
Bootable Disk	Floppy+ Windows 2000 Operating System CD+ CA ARCserve Backup CD/DVD or Patched CA ARCserve Backup Disaster Recovery CD	Windows 2000
Bootable Tape Image	Tape+ Floppy (XP only) **Note:** For Windows XP, floppy disk is required. For Windows 2000 and Windows Server 2003, no floppy required.	Windows 2000 Windows XP, 32-bit Windows Server 2003, 32-bit
Using Microsoft Remote Installation Server(RIS)	None- Disaster Recovery Option boots using PXE	Windows XP (both 32-bit and 64-bit) Windows Server 2003 (both 32-bit and 64-bit)

Disaster Recovery Global Options

The Disaster Recovery Option supports two global job options.

- **Generate DR information for partially selected nodes**: 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 complete machine node by selecting the green marker completely. The Generate DR information for partially selected nodes allows you to explicitly force disaster recovery information to be generated when backing up a subset of a machine.

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

- **Include filtered sessions when generating restore session information**: When generating disaster recovery information for a machine, the latest backup sessions of all drive volumes and system state are recorded for the machine. By default, the option skips all sessions with a filtered flag set, so these sessions are never used by the option to recover a machine. The Include filtered sessions when generating restore session information allows you to explicitly force the option to include these filtered sessions.

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

You can access the two global job options from the Advanced tab of the Options dialog when creating a backup job.

Create a Disaster Recovery Plan

As part of your disaster recovery preparations, you should develop a disaster recovery plan. To create and test your plan, complete the following steps:

1. Create a set of disaster preparation materials to be kept off site. Follow the instructions in the subsequent chapters of this guide to complete this step.
2. Set up a test server with a similar configuration to your original server.
3. Simulate a recovery on your test server by following the disaster recovery instructions in this guide.

Special Considerations for Database Applications

CA ARCserve Backup has special agents available to back up database applications such as Oracle, Microsoft SQL Server, Microsoft Exchange Server, and Lotus Notes. If you have backed up one or more of these databases using CA ARCserve Backup database agents, the databases are not automatically restored as part of the disaster recovery process.

When CA ARCserve Backup backs up database application data, additional media sessions are created, separate from the rest of the machine backup. Disaster recovery does not automatically restore these database sessions. However, after restoring the rest of the server using the Disaster Recovery Option, it is a simple process to start CA ARCserve Backup and begin a normal database restore procedure using the corresponding application agent. See the corresponding agent guide for more information.

Chapter 2: Installing the Option

The following chapter discusses information you need to know when you install the option. It provides the procedure to install the Disaster Recovery Option and post-installation considerations to help you fine-tune the option after it is installed.

This section contains the following topics:

Preinstallation Tasks

This section describes information you should review and have available before you install the option and when configuring the option.

Prerequisite Software

Verify that you have CA ARCserve Backup installed before installing the option. You can install CA 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 file**: 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 root level on the product CD.
- **Implementation Guide**: Provides an overview of product features and functions, basic concepts, installation information, and a introduction to the product. It is provided in hardcopy and in Adobe Portable Document Format (PDF) on the product CD.
- **Release Summary**: Lists new features and changes to 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 CA ARCserve Backup client computer, the CA ARCserve Backup server saves the computer-specific information required to perform disaster recovery tasks.

If the CA ARCserve Backup server fails, 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 recovery disks even if the CA ARCserve Backup server fails.

Note: If you are upgrading or migrating from an earlier version of CA ARCserve Backup or BrightStor Enterprise Backup, and you had previously configured an alternate location in which 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 configure the option to send information to that shared folder.

Set Up Alternate Machine Locations to Replicate Disaster Recovery Information

The Disaster Recovery process creates a temporary operating system working environment, sets the environment's configuration to be the same as the disk and the network, and restores data to the system so that the machine can return to its latest backup state. These operations cannot be executed automatically if there is no record of the original system settings. Therefore, relevant system information must be gathered during backup operations for disaster recovery purposes.

When you perform a full backup of a machine, specific disaster recovery information is generated for that machine. This information is stored on the backup server and is used to create the disaster recovery media to recover the protected machines in the event of a disaster. We strongly recommend that you set up an alternate location for disaster recovery to allow you to replicate the information to a remote machine as backup copies. If the backup server itself fails, you can recover it automatically using disaster recovery.

Setting up an alternate location for disaster recovery information is a two step process. First, you create a shared folder on the remote machine to receive the replicated information. Second, you run the Boot Kit wizard and enter information about the alternate location after you click on the Config option.

System Requirements

The remote machine that hosts the shared folder should be running one of the following server editions of the Windows operating system:

- Windows XP Professional
- Windows 2000
- Windows Server 2003
- Windows Server 2008

Create Shared Folders for Disaster Recovery Alternate Locations

You can create shared folders for the disaster recovery in alternate locations.

To create the shared folder

1. Create a new folder and name it. You can create this folder anywhere on the system 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.
3. In the Properties dialog, 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.

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

6. In the Permission dialog, 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

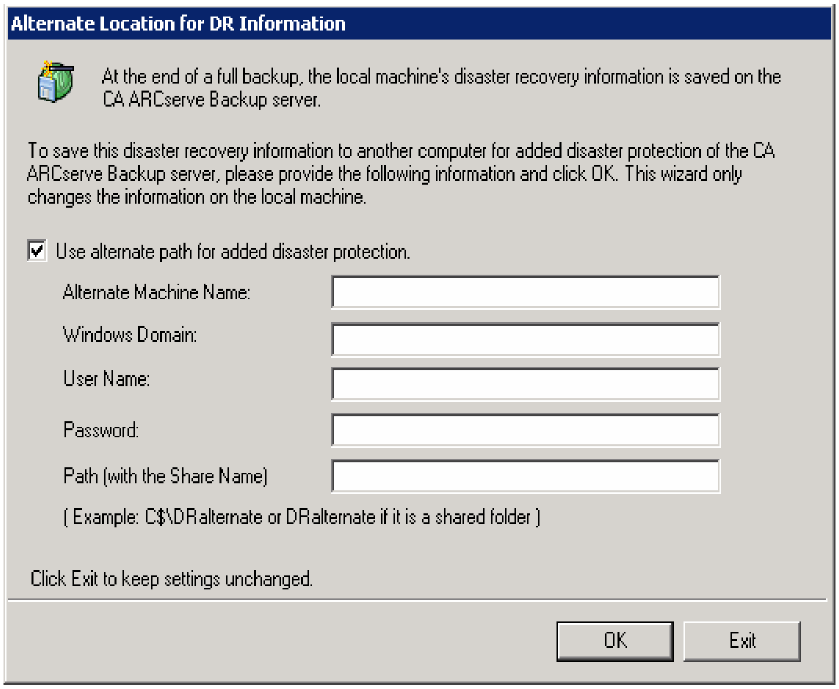
   > If the user account exists on the machine and is part of a local user group, you can add the entire local user group to add the user account implicitly.

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

You can set up an alternate location for disaster recovery information when you install the Disaster Recovery Option or you use the Config option from the Boot Kit wizard to set up an alternate location.

In the Disaster Recovery wizard, the Alternate Location page allows you to specify information about the alternate location in which to store disaster recovery information.



Alternate Location for DR Information

At the end of a full backup, the local machine's disaster recovery information is saved on the CA ARCserve Backup server.

To save this disaster recovery information to another computer for added disaster protection of the CA ARCserve Backup server, please provide the following information and click OK. This wizard only changes the information on the local machine.

☑ Use alternate path for added disaster protection.

Alternate Machine Name:

Windows Domain:

User Name:

Password:

Path (with the Share Name)

(Example: C$\DRalternate or DRalternate if it is a shared folder)

Click Exit to keep settings unchanged.

This page provides 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**: If you specified domain information in the User Name field, this field is ignored.

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 replicated disaster recovery information.

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

General Considerations

The following section provides general information to consider 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 one 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 Microsoft KB article at http://support.microsoft.com/

Create Machine-specific Recovery Disks from Alternate Locations

You can create machince specific recovery disks from alternate locations.

To create a machine-specific recovery disk from the 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 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: Only the files should be copied to the floppy and not the directory.

4. Run the following steps to recover the Windows system:

   - **For Windows XP or Windows 2003**,

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

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

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

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

   - **For Windows 2008 (32-bit)**,

     a. Locate the folder “drpatch.xp” in the alternate location configured to stored to locate the disaster recovery information.

     b. Copy "drlaunch.ex_" and "drlaunchres.dl_" under directory "drpatch.xp" to a temporary directory, then open a command line console and switch to the temporary directory.

     c. Run command “expand –r *_”. to decompress these 2 files.

     d. Copy the decompressed file to floppy disk.

     e. Copy the file "drlaunchres.dl_" under directory "drpatch.xp\ENU" to a temporary directory.

     f. Open a command line console and switch to the temporary directory to run command “expand drlaunchres.dl_ drlaunchenu.dll”.

     g. Copy “drlaunchenu.dll” and “drpatch.w2k8\autounattend.xml” to a floppy disk.

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

   - **For Windows 2008 (x64-bit)**,

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

     b. Copy "drlaunch.ex_" and " drlaunchres.dl_" under directory "drpatch.xp\X64" to a temporary directory.

c. Open a command line console and switch to the temporary directory, run command "expand –r *_" to decompress these 2 files.

d. Copy the decompressed file to floppy disk.

e. Copy the file "drlaunchres.dl_" from the "drpatch.xp\X64\ENU" directory to a temporary directory.

f. Open a command line console, switch to the temporary directory and run command "expand drlaunchres.dl_ drlaunchenu.dll".

g. Copy "drlaunchenu.dll" to floppy disk.

h. Copy "drpatch.w2k8\autounattend_amd64.xml" to a temporary directory, rename it to "autounattend.xml", then copy it to a floppy disk.

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

- **For Windows 2008 (IA64-bit),**

a. Locate the folder "drpatch.xp\IA64" in the alternate location configured to store disaster recovery information.

b. Copy "drlaunch.ex_" and " drlaunchres.dl_" under directory "drpatch.xp\IA64" to a temporary directory, then open a command line console, switch to the temporary directory, run command "expand –r *_". This will decompress these 2 files.

c. Copy the decompressed file to a floppy disk.

d. Copy the file "drlaunchres.dl_" under directory "drpatch.xp\IA64\ENU" to a temporary directory.

e. Open a command line console and switch to the temporary directory, run command "expand drlaunchres.dl_ drlaunchenu.dll".

f. Copy "drlaunchenu.dll" to a floppy disk.

g. Copy "drpatch.w2k8\autounattend_ia64.xml" to a temporary directory and rename it as "autounattend.xml", then copy it to floppy disk.

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

Install and Configure the Option

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

For specific details about installing CA ARCserve Backup, see the *CA - 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 CA ARCserve Backup and the option at the same time, the installation prompts you to select your database, set your password, and enter system account information.

   The Product List appears.

3. You can verify the components to be installed and Click Next.

   Setup copies files and installs the CA licensing information.

4. You are prompted with licensing information and license verification. Click Next.

   Setup copies files and installs the option.

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

   The configuration wizard appears.

6. You are prompted to 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 recovery disks even after a disaster on your backup server.

   To configure an alternate location, select the Alternate Location for DR information by clicking on the Config option and enter the 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 previously have 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 do so, start the Disaster Recovery Configuration Wizard and choose the option Config to configure Disaster Recovery Alternate Location. For more information about this feature, see the section Set Up Alternate Machine Locations to Replicate Disaster Recovery Information in this guide.

   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 /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.

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

2. Create a machine specific disk after all backups are run or after every incremental or differential backup. The MSD would have information about all backups (full and incremental / differential) that were performed before MSD was created.

   In case, an alternate location was configured, MSD can also be created just before the disaster recovery.

3. Run the disaster recovery process.

   Note: The Disaster Recovery Option will not automatically scan any additional sessions backed up after creation of MSD.

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

Post-installation Tasks

We recommend that you review the online help after installing the option. 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.

Post-installation Tasks for the Backup Server on Windows XP

For remote disaster recovery to connect to the backup server successfully, you must set the value of following registry key to zero on the backup server machine:

HKEY_LOCAL_MACHINE\Software\Polices\Microsoft\Windows XP\RPC\RestrictRemoteClients

Note: If you are using an earlier version of the backup server, or if the Software\Computer Associates\CA ARCserve Backup\Base\Tapeengine\DR\UseNetBIOS registry key is set to 1, change the option Network access: Sharing and security model for local accounts security policy to Classic – local users authenticate as themselves.

Chapter 3: Disaster Recovery on Windows 2000

To prepare for a disaster on your Windows 2000 system, use the Disaster Recovery procedures described in the following sections.

This section contains the following topics:

Boot Media Creation Methods

Use one of the following methods to create boot media to bring your Windows 2000 server back online quickly:

- **Bootable CD**: This method uses a bootable CD and one machine-specific recovery disk containing configuration information. The CD and floppy disk let you start any Windows 2000 computer, even one with an unformatted hard drive, from a bootable CD and fully restore the system using the backup media.

  Note: This is the recommended method.

- **Bootable disk**: This method uses 3.5-inch floppy disks containing a modified version of the Windows 2000 setup software and configuration information for a specific computer. These disks let you start the Windows 2000 computer (with or without a formatted hard drive) from a bootable disk and fully restore the system using the option's backup media. The Windows 2000 installation media is required during this recovery process. The CA ARCserve Backup CD is also required during the recovery.

- **Bootable tape:** This method uses a bootable tape. This bootable tape also contains a full backup. It lets you start any Windows 2000 computer, even one with an unformatted hard drive, from a bootable tape and fully restore the system without any CD or disks.

  Note: You can create boot media at any time, even after the system has failed. However, you must ensure that the computer has been fully backed up by an available, functioning CA ARCserve Backup server.

To protect your CA ARCserve Backup server itself, you must create boot media before a disaster occurs, or use the alternate location feature. For more information about this feature, see the section Install and Configure the Option (see page 29) in the “Installing the Option” chapter of this guide.

Disaster Preparation

This section describes how to protect your local Windows 2000 computer from a potential disaster by creating boot disks, CDs, or tapes. You can create them at any time, even after the workstation fails.

Bootable Disk Method

The Bootable Disk method uses five disks of which the fourth disk contains the Windows 2000 disk partition layout information and the fifth disk contains configuration information for that specific computer.

Bootable Disks for Specific Computers

Use this method to create a boot disk for a specific computer. The option uses this disk to automatically partition your hard disk into the original configuration.

For information about, and procedures for, recovering your data, see the section "Disaster Recovery in Windows 2000" in this chapter. Review this material and have a practice disaster recovery session to prepare for a disaster.

Update Bootable Disks for Specific Computers

If you make changes to your hardware or your computer configuration, such as changing your network card, you must run a full backup again and use the Disaster Recovery Wizard to update all the boot disks created.

To update your bootable disk

1. From the Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit wizard dialog opens.

2. Select Machine Specific Disk and click Next.
3. The Select CA ARCserve Backup Server dialog appears, containing a list of available servers. Select the appropriate server and click OK.
4. The Create Boot Disk wizard displays a list of computers that have been backed up by CA ARCserve Backup. The list is empty if CA ARCserve Backup has not backed up any computers. Select the Windows 2000 computer for which you are updating the bootable disks and click Next.
5. The Boot Kit wizard information dialog opens. Click Next.
6. When prompted, insert the disk labeled Windows 2000 Setup Boot Disk and click Start.
7. When complete, click Next.
8. When prompted, insert the disk labeled Windows 2000 Setup Disk 4 and click Start.
9. When complete, click Next.
10. When prompted, insert the disk labeled CA ARCserve Backup machine specific disk and click Start.
11. When the copying finishes, the screen displays the backup sessions that will be used to recover the system if this machine specific recovery disk is used. Click Next and click Finish.

You have now updated your set of disaster recovery disks.

Copy the Windows 2000 Setup Disks

Create copies of the Windows 2000 setup disks and label each disk accordingly (for example, Windows 2000 Setup Boot Disk 1, Windows 2000 Setup Boot Disk 2, and so on). To do this, use the MAKEBT32 utility. You can run this utility from the network directory containing the master files for Windows 2000, or you can run this utility from the Windows 2000 CD. The utility is located in the bootdisk directory on the Windows 2000 CD. Enter the following command to create the setup disks:

```
MAKEBT32
```

You can also create these disks by running MAKEBOOT under DOS or Windows. For more information about how to create Windows 2000 setup disks, see the *Microsoft Windows 2000 Installation Guide*.

Note: When you recover your system, you must use the Windows 2000 CD.

Bootable Disk Creation Prerequisites Windows 2000

In addition to the Windows 2000 Setup disks, you need another disk for machine specific recovery.

Before proceeding, ensure that you have performed a full backup of your computer using CA ARCserve Backup, and that you have one formatted, high-density disk. Label this disk CA ARCserve Backup machine specific recovery Disk.

Create Bootable Disks on Windows 2000

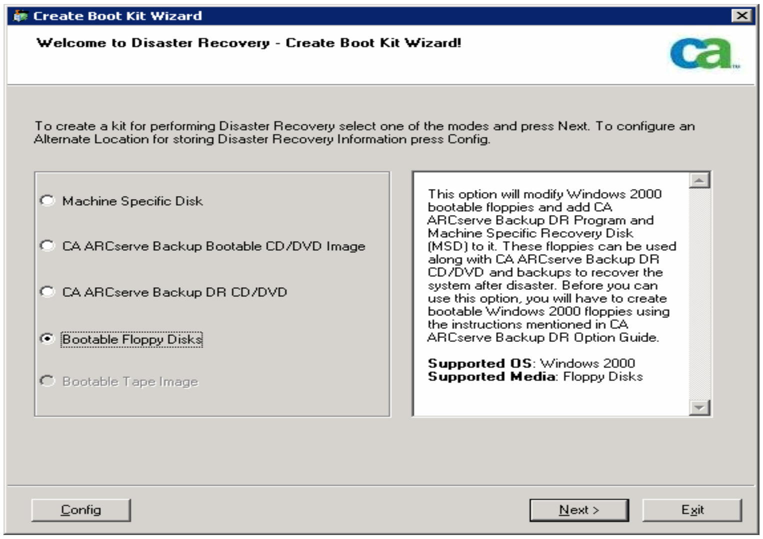
You can create bootable disks on Windows 2000 using the following procedure:

To create the disks used for recovery

1. From the Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit Wizard dialog opens.

2. Select Bootable Floppy Disks and click Next.



Create Boot Kit Wizard

Welcome to Disaster Recovery - Create Boot Kit Wizard!

To create a kit for performing Disaster Recovery select one of the modes and press Next. To configure an Alternate Location for storing Disaster Recovery Information press Config.

○ Machine Specific Disk

○ CA ARCserve Backup Bootable CD/DVD Image

○ CA ARCserve Backup DR CD/DVD

● Bootable Floppy Disks

○ Bootable Tape Image

This option will modify Windows 2000 bootable floppies and add CA ARCserve Backup DR Program and Machine Specific Recovery Disk (MSD) to it. These floppies can be used along with CA ARCserve Backup DR CD/DVD and backups to recover the system after disaster. Before you can use this option, you will have to create bootable Windows 2000 floppies using the instructions mentioned in CA ARCserve Backup DR Option Guide.

Supported OS: Windows 2000
Supported Media: Floppy Disks

3. Enter the CA ARCserve backup domain user name and password in the Connect to CA ARCserve Backup Server dialog that appears, and click Next.

4. The Create Boot Disk wizard displays a list of computers that have been backed up by CA ARCserve Backup.

   The panel appears blank if CA ARCserve Backup has not backed up a computer.

5. Select the Windows 2000 computer for which you are creating the bootable disks and click Next.

   The Boot Kit wizard information dialog appears. Click Next.

6. When prompted, insert the disk labeled Windows 2000 Setup Boot Disk 1 into drive A and click Start. The option copies all necessary disaster recovery files to the disk.

7. When complete, click Next.

8. When prompted, insert the disk labeled Windows 2000 Setup Boot Disk 4 into drive A and click Start. The option copies all necessary disaster recovery files to the disk.

   Note: The fourth Windows 2000 setup disk contains the disk layout information of a specific machine and you cannot use this for other machines. After applying the necessary changes to disk layout, you must repeat all the steps described in this section to recreate Boot Disks.

9. When complete, click Next.
10. When prompted, insert the disk labeled CA ARCserve Backup machine specific disk and click Start.
11. When complete, the screen displays the backup sessions that will be used to recover the system if this machine specific recovery disk is used. Click Next.
12. Click Finish.

You have now created a set of disaster recovery disks you can use in the event of a disaster.

Remove Unnecessary Network Driver Files from Machine Specific Information

When you back up an entire Windows 2000 machine (including all drives and the system state), information is generated or updated for that machine for disaster recovery purposes. This Machine Specific Information (MSI) contains the machine's disk settings, network settings, network driver files, CA ARCserve Backup configuration, and the backup session records. The MSI is stored on a floppy disk and used during the disaster recovery process.

Because this information is saved to a floppy disk, the total size of the MSI cannot exceed 1.44MB. If the size of the MSI does exceed 1.44MB, you must manually remove files from the MSI before creating the disaster recovery floppy disk. Typically, removing unnecessary network driver files reduces the MSI size to well under 1.44MB.

Note: This information does not apply to machines running Windows 2003 or Windows XP. The disaster recovery solution for Windows XP and Windows 2003 is built on top of the Windows Automated Systems Recovery (ASR) model.

Determine Unnecessary Network Driver Files

Network driver files are identified by the extensions SYS and INF in the MSI.

In local disaster recovery, when you recover from a locally attached backup device (except distributed SAN servers), all operations are performed locally and there is no need to establish a network connection. Therefore, none of the network driver files are needed for the disaster recovery process to be successful.

In remote disaster recovery, when you recover data remotely from the backup server, the only necessary network driver is the one for the network adapter that can connect to the CA ARCserve Backup server. Your backup administrator should know which network adapter is on the machine and be able to supply the MAC address of the adapter.

To identify the driver files for that network adapter

1. Log in to the client machine, not the backup server machine.
2. From the Start menu, go to Settings, Network Connections.
3. Right-click the connection used to communicate with the backup server and select Properties.

   To determine the network adapter on the client machine that connects with the backup server, follow these steps:

   a. From a command prompt on the backup server, ping the client machine and note the reply IP address.

   b. On the client machine, check the IP addresses assigned to each network adapter.

   c. The adapter owning the reply IP address you noted is the network adapter that connects to the backup server.
4. From the pop-up dialog, note the name for the adapter description in the Connect Using field.
5. Log in to the backup server machine.
6. In the folder %ARCserve Home%\DR\%Server Name%\%Client Machine Name% (where %ARCserve Home% is the folder in which CA ARCserve Backup is installed), the folder containing the MSI of the client machine, open the file CardDesc.txt.
7. The INF file and SYS file names appear in the InfFile field and the DriveFile field in the section where DeviceDesc=%Recorded Card Description from step 5 above%.

Note: We strongly recommend that you make a copy of the MSI and keep it in a safe location before deleting any files.

Remove Unnecessary Network Driver Files

The INF and SYS files you identify should be the only necessary network driver files. All other network INF and SYS files can be remove from the MSI to reduce its total size. (When you recover a distributed SAN machine, the only network driver needed is the one that connects to the primary SAN server.)

To remove the unnecessary network driver files

1. Log in to the backup server machine and open the following folder:

   %ARCserve Home%\DR\%Server Name%\%Client Machine Name%

   where %ARCserve Home% is the folder in which CA ARCserve Backup is installed and %Client Machine Name% is the hostname of the client machine.

2. Remove any INF and SYS files that are not used by the network adapter to connect to the backup server.

Note: After the files have been removed, launch the Boot Kit Wizard to create the disaster recovery machine-specific recovery disk.

To ensure that no required driver files have been accidentally removed, perform a test of your disaster recovery plan and verify that the disaster recovery process can connect to the backup server and finish the system restoration successfully. If not, the driver files you removed may have been required. Repeat the process using the original MSI and carefully select the files to remove.

Identify Unnecessary Network Driver Files After Failure

We strongly recommend that you record which network adapter on the client machine is used to connect to the backup server. If the client machine has already failed and this information is not available, there is no simple way to determine which network driver files are needed.

Note: We strongly recommend that you keep a copy of the MSI in a safe location before deleting any files.

To identify the driver files after your machine has failed

1. Log in to the backup server machine.
2. In the folder %ARCserve Home%\DR\%Server Name%\%Client Machine Name% (where %ARCserve Home% is the folder where CA ARCserve Backup is installed, %Server Name% is the hostname of backup server, and %Client Machine Name% is the hostname of the client machine), open the CardDesc.txt file. The CardDesc.txt file allows you to view the description of the network cards.
3. Identify the network card used to connect to the backup server. The CardDesc.txt file also lists the driver files required by each adapter.

Remove Unnecessary Network Driver Files After Failure

The INF and SYS files you identify should be the only network driver files needed. All other network INF and SYS files can be removed from the MSI to reduce its total size.

To remove unnecessary network driver files

1. Log in to the backup server machine and open the following folder:

   ```
   %ARCserve Home%\DR\%Server Name%\%Client Machine Name%
   ```

   where %ARCserve Home% is the folder where CA ARCserve Backup is installed, %Server Name% is the hostname of backup server, and %Client Machine Name% is the hostname of the client machine.

2. Remove the INF and SYS files that are not used by the network adapter to connect to the backup server.

Note: After the files have been removed, launch the Boot Kit Wizard to create the disaster recovery machine-specific recovery disk.

To ensure that no required driver files have been accidentally removed, perform a test of your disaster recovery plan and verify that the disaster recovery process can connect to the backup server and finish the system restoration successfully. If not, the driver files you removed may have been required. Repeat the process using the original MSI and carefully select the files to remove.

Bootable Tape Method

You can use the bootable tape disaster recovery method to recover from a loss of system volumes on Windows 2000 production servers without using bootable disks or CDs. You can only use this method to protect a local CA ARCserve Backup computer.

To prepare for a disaster using this method

1. From the Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit Wizard dialog opens.

2. Choose the Bootable Tape Image and click Next.

   Note: This option is not available if a bootable tape drive is not detected.

3. When prompted, insert the Windows 2000 installation media into the optical drive, select the CD-ROM drive from the list, and click Next.

4. When the utility has finished creating the bootable image, click Finish.

   The bootable tape image file tober.iso is created under CA ARCserve backup home directory.

5. Format the tape using the Device Manager or Device wizard to write the image to the tape.

   After bootable tape image created, it will be written to the tape every time you format a tape.

6. Perform a full backup of the local CA ARCserve Backup server using the tape you just 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.

Bootable CD Method

On Windows 2000, the option provides a quick way to boot to the Disaster Recovery Wizard. Rather than using five disks and a Microsoft 2000 CD, you need only one disk and a CD.

When you create a bootable CD image (cdboot.iso file), your CD recorder need not be attached to the CA ARCserve Backup server. After creating the image, you can create a CD from the cdboot.iso image from any computer with a CD recorder and the necessary CD creator software.

Before proceeding, ensure that you have performed a full backup of your computer using CA ARCserve Backup, and that you have one formatted, high-density disk. Label this disk CA ARCserve Backup Machine-specific Disk.

Create CA Bootable Images for the Bootable CD Method

You can create bootable images for the bootable CD method using the boot kit wizard.

To create a bootable CD for the bootable CD method

1. From the Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit wizard dialog appears.

2. Select CA ARCserve Backup DR CD/DVD Image option and click Next.
3. Create the Boot kit wizard utility help appears, click OK.

   The Choose Operating System Type screen appears.

4. Select Windows 2000 system and click Next.
5. Specify the path to the Windows installation media and click Next. The wizard creates a file called cdboot.iso in the CA ARCserve Backup home directory.

   You can create a bootable CD from this image.

Create Machine-specific Recovery Disks for the Bootable CD Method

This section describes how to create a disk to be used with the bootable CD to perform disaster recovery on a specific computer.

To create a disk for the bootable CD ROM method

1. From the Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit Wizard dialog appears.

2. Select the Create Machine-specific Recovery Disk option and click Next.
3. Select the CA ARCserve Backup server from the list of available servers and click OK.
4. The Create Boot Disk Wizard displays a list of computers that have been backed up by CA ARCserve Backup. The list is empty if CA ARCserve Backup has not backed up any computers. Select the Windows 2000 computer for which you are creating the machine-specific recovery disk and click Next.

5. When prompted, insert the disk labeled CA ARCserve Backup machine-specific disk into Drive A and click *Start.* The option copies all necessary disaster recovery files to the disk.
6. When the copying finishes, the screen displays the backup sessions that will be used to recover the system if this machine-specific recovery disk is used. Click Finish.

You have now created a disaster recovery disk that you can use to recover your computer in the event of a disaster.

Disaster Recovery on Windows 2000

You can recover from a disaster on Windows 2000 using the bootable disk, bootable tape, or bootable CD method.

Recover from Disaster Using the Bootable Disk Method in Windows 2000

You can recover from a disaster using the following guidelines and disaster recovery method.

Bootable Disk Method Guidelines

To recover from a disaster using the bootable disk method

- The set of disaster recovery boot disks you created using the instructions in the section Bootable Disk Method.
- A Microsoft Windows 2000 CD that matches the version used to create the boot disks.
- A backup device connected to the server (can be a remote CA ARCserve Backup server) with backup media containing the data you want to restore. The media must contain at least one full backup session.

For information about disaster recovery for non-standard configurations, see the section Disaster Recovery Scenarios on Windows 2000.

Important! During the disaster recovery process, the option partitions your hard disk into the original configuration. You can only use this set of bootable disks to perform a disaster recovery on this computer.

Start Disaster Recovery Using the Bootable Disk Method

You can perform disaster recovery using the following procedure:

To perform disaster recovery using the bootable disk method

1. Start the computer you want to recover, using the Windows 2000 Setup Boot Disk 1 created in Bootable Disk Method.

   To install additional SCSI drivers, press F6 when prompted at the bottom of the Windows Setup dialog.

2. When prompted, insert the disks labeled Windows 2000 Setup Disk 2.
3. If you pressed F6 in step 1, insert OEM driver floppy, and select S to specify additional drivers when prompted. After you install the additional drivers, you must put the Machine Specific Disk in the drive and click Enter.
4. When prompted, insert the disk labeled Windows 2000 Setup Disk 3, and Windows 2000 Setup Disk 4.

   Note: In Japanese, Simplified Chinese, and Traditional Chinese procedure, the disk loading sequence will be Windows 2000 Setup Disk 3, Windows 2000 Setup Disk 4, MSD floppy, Windows 2000 Setup Disk 4.

5. Insert the Windows 2000 CD, when prompted.
6. When prompted, select a partition to set up Windows. Select the partition that has original Windows 2000 operating system installed. Typically, it is the first partition with drive letter C. The option installs a temporary operating system.

   Note: If any disk is replaced, you find the file system partitions on that disk display as Unformatted or Damaged, when partitions size is more than 8 GB. However, this is not an error. Select the partition (same as your original system) and press Enter to continue. You may be prompted to format partition, select the file system type and continue. DR will restore the file system to original status later.

7. You will be prompted to insert the driver disk again if you choose to load any driver in step 3.
8. You will be prompted to insert the CA ARCserve Backup CD.

   Insert the CA ARCserve Backup CD.

9. When prompted, insert the Windows 2000 CD again.

   Setup copies Windows 2000 files to your hard disk.

10. When you receive the message that Setup has completed successfully, remove all disks and CDs, and press Enter to restart your computer.

    The computer reboots and the Disaster Recovery wizard opens.

Recover from Disaster Using the Disaster Recovery Wizard

To perform the disaster recovery process using the Disaster Recovery Wizard

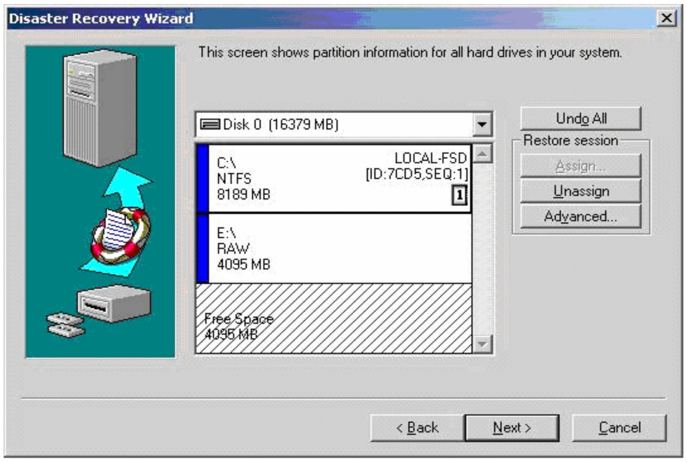
1. When the Disaster Recovery Wizard appears, click Next.
2. When prompted, insert the disk labeled CA ARCserve Backup Machine Specific Disk and click OK.
3. The computer must be restarted at this point. Remove any CDs or disks and click OK to restart the computer. If you are performing a remote disaster recovery, usually a summary of installed drivers is displayed. Select Yes, if you want to install additional drivers.

   However, if you are using the USB backup device, you must load drivers for some specific USB backup devices. For more information about loading drivers, refer to section "Disaster Recovery Using Locally-attached USB Backup Devices".

   Note: You may have to reboot the system several times, depending on your original hard disk configuration.

   As the disaster recovery session has to be restored during this period, you will be prompted to provide session password, if the session encryption/password protection option is enabled.

4. The Disaster Recovery Wizard displays a list of available devices on the local computer or remote CA ARCserve Backup server. Click Next to continue. The original hard disk configuration is now restored and appears in the wizard.



Disaster Recovery Wizard

This screen shows partition information for all hard drives in your system.

Disk 0 (16379 MB)

C:\ NTFS 8189 MB — LOCAL-FSD [ID:7CD5,SEQ:1] 1

E:\ RAW 4095 MB

Free Space 4095 MB

The dialog provides the following information:

Formatted partitions

Space that is partitioned and formatted. These partitions are formatted when sessions are assigned to them.

Unformatted partitions

Space that is partitioned but not formatted. These partitions are formatted when sessions are assigned to them.

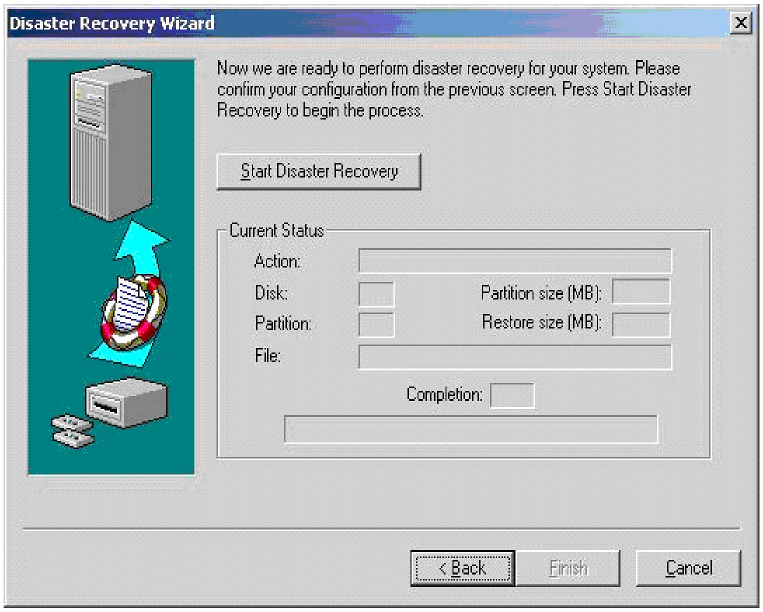
Free space

Disk space that is not formatted and not partitioned. Free space is created when a partition is deleted. You should not modify the partitions from the original configuration.

Note: The Advanced option tells about the sessions allocated to each drive, in hard disk and also helps assign session password. You can also recover incremental/differential backup sessions simultaneously.

5. Click Next. The wizard is ready to begin recovery for each partition to which a backup session is assigned.

6. Click Start Disaster Recovery to start the disaster recovery process.



Disaster Recovery Wizard

Now we are ready to perform disaster recovery for your system. Please confirm your configuration from the previous screen. Press Start Disaster Recovery to begin the process.

7. The Disaster Recovery Wizard copies the data from the specified sessions to the specified partitions. A progress bar indicates the progress of the restore process. When the restore operation is complete, click Finish. Your computer reboots and returns to the state it was in at the time the backup media was created.

Note: The option creates a directory called drboot.tmp during the restore process. It is deleted automatically the next time you start the CA ARCserve Backup Tape Engine, or the next time the client machine is started. On a remote site, you may want to delete this file due to its large size.

Press Ctrl+Shift and double-click on the image on the left side of the Disaster Recovery wizard dialog to display a DOS prompt window. You can run most of the 32-bit Windows programs, such as regedit.exe from the DOS prompt window.

Recover from Disaster Using the Bootable Tape Method in Windows 2000

You can recover from a disaster using the following guidelines and disaster recovery method.

Bootable Tape Method Guidelines

You can retrieve lost data on a server using the bootable tape method if both of the following conditions are met:

- A disaster occurs causing the loss of at least the server's Windows 2000 system volume so that the server no longer boots.
- The server was backed up using the Create CA Bootable Tape Option to a tape drive capable of acting as a bootable device.

Disaster Recovery Using the Bootable Tape Method

To recover from a disaster using the 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. The booting process begins and the option reads all boot data from the tape. The tape formats and partitions drives.
5. After the necessary Windows 2000 files have been copied to the server, reboot the server when prompted.

6. After the server is up, the wizard starts to restore data.

   Note: You may be required to reboot several times, depending upon your original hard disk configuration.

7. When the restoration process is complete, the wizard prompts to reboot the server. Reboot the server when prompted.

   The server is now restored to its original state and contains the data it contained as of its last complete backup.

Recover from Disaster Using the Bootable CD Method in Windows 2000

You can recover from a disaster using the following guidelines and disaster recovery method.

Bootable CD Method Guidelines

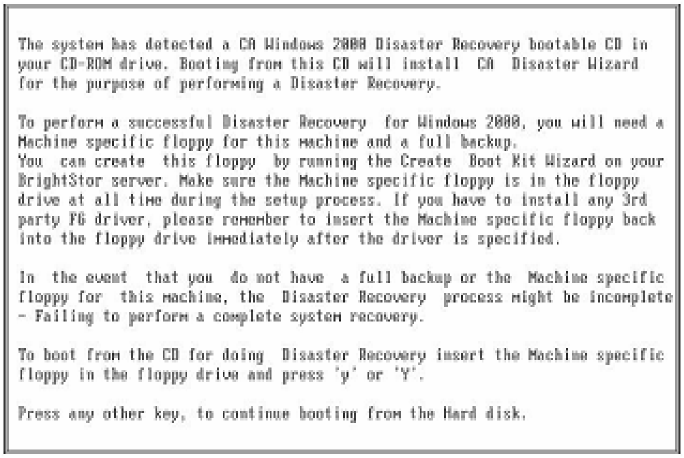
On Windows 2000, this option provides a quick way to boot to the Disaster Recovery Wizard. Rather than using five disks and a Microsoft 2000 CD, this option uses only one disk and one CD. To recover from a disaster using the bootable CD method, you need the following items:

- The recovery disk you created using the instructions in the section Disaster Preparation on Windows 2000.
- The CA ARCserve Backup disaster recovery CD. For more information about creating a bootable CD, see the section "Bootable CD Method" in this chapter.

Disaster Recovery Using the Bootable CD Method

To perform disaster recovery using the bootable CD method

1. To boot from the CD, insert the CD created in the section Create CA Bootable Images for the Bootable CD Method into the CD drive and reboot the computer. When you boot from the CD, you are warned that the option is about to install a temporary Windows 2000 operating system.

   ```
   The system has detected a CA Windows 2000 Disaster Recovery bootable CD in
   your CD-ROM drive. Booting from this CD will install  CA  Disaster Wizard
   for the purpose of performing a Disaster Recovery.

   To perform a successful Disaster Recovery  for Windows 2000, you will need a
   Machine specific floppy for this machine and a full backup.
   You  can create  this floppy  by running the Create  Boot Kit Wizard on your
   BrightStor server. Make sure the Machine specific floppy is in the floppy
   drive at all time during the setup process. If you have to install any 3rd
   party F6 driver, please remember to insert the Machine specific floppy back
   into the floppy drive immediately after the driver is specified.

   In  the event  that you  do not have  a full backup or the  Machine specific
   floppy for  this machine, the  Disaster Recovery  process might be incomplete
   - Failing to perform a complete system recovery.

   To boot from the CD for doing  Disaster Recovery insert the Machine specific
   floppy in the floppy drive and press 'y' or 'Y'.

   Press any other key, to continue booting from the Hard disk.
   ```

2. Insert the disk labeled machine specific disk you created in the section Create Machine specific Disks for the Bootable CD Method. Press Y to start DR procedure.

   Important! The CA ARCserve Backup machine specific disk is required when recovering from a disaster using the Bootable CD method.

3. To install additional SCSI drivers, you need to press F6 when prompted. The prompt message is on the bottom of the screen. If you pressed F6, select S to specify additional drivers when prompted. Load the device driver floppy disk into the floppy drive. After you have loaded the additional drivers, you must put the Machine Specific Disk in the drive and press Enter.

4. When prompted, select a partition to set up Windows. Choose the first partition (typically, C). The option installs a temporary operating system.

   Note: If any disk is replaced, you find the file system partitions on that disk display as Unformatted or Damaged, when partitions size is more than 8 GB. Select the partition (same as your original system) and press “Enter” to continue. You may be prompted to format partition, select the file system type and continue. However, this is not an error, DR will restore the file system to original status later.

   You may be prompted to reinsert the additional drivers, if any were loaded, at this point.

5. You are prompted to reboot the computer. Remove all disaster recovery media and reboot the computer.

   The Disaster Recovery Wizard appears.

6. Continue with the steps described in the section Recover from Disaster Using the Disaster Recovery Wizard (see page 46) in this chapter.

Disaster Recovery Using Locally-attached USB Backup Devices

The option supports the use of USB backup devices in disaster recovery operations.

Note: You must connect and power 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 local disaster recovery, if you used 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:

Original Device List

This 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

This 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 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.

Command Prompt

Click this button to open a command prompt in a separate window. From this prompt, you can map to a remote shared folder containing the drivers, using a command like NET USE, and install the drivers sequentially from the remote location. The command prompt is also useful for debugging purposes.

Install

Click this button to open a dialog allowing you to 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.

Refresh

Click this button to manually refresh the Current Device List after installing a driver. It can take some time before the installed driver begins to work with the device.

Install USB Devices After Backup

You are prompted to 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
```

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

The Disaster Recovery process described in the following sections saves you time when a disaster occurs on a local or remote computer running Windows XP or Windows Server 2003 or Windows Server 2008. Windows XP and Windows 2003 provide a feature called Automated System Recovery (ASR). ASR is a framework in which CA ARCserve Backup can run a recovery application to quickly and safely restore user data. These sections provide information about preparing for a disaster and recovering from a disaster on Windows XP, Windows Server 2003 and Windows Server 2008 using Disaster Recovery procedures.

This section contains the following topics:

Disaster Recovery Methods on Windows Server 2003 and Windows XP

Disaster Recovery on Windows XP and Windows Server 2003 supports both the Bootable CD method and the Bootable Tape method also known as One Button Disaster Recovery (OBDR). The Bootable CD method supports the protected client machines as well as the backup server itself. The Bootable Tape method can only be used to protect the backup server itself. 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 XP and 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 CA ARCserve Backup CD.

Machine Specific Recovery Disks

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

- Install CA 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, high-density disk CA ARCserve Backup Machine-specific Disk

Create Machine Specific Disks

The machine-specific disk is the recovery disk used with the Windows XP or Windows Server 2003 installation media and the CA ARCserve Backup CD to perform disaster recovery on a Windows XP or Windows Server 2003 computer using the Bootable CD method.

To create a machine-specific disk

1. Insert the disk labeled CA ARCserve Backup Machine-specific Disk into the server’s disk drive.
2. From the Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit Wizard dialog opens.
3. Select the Machine Specific Disk and click Next.

   The Connect to CA ARCserve Backup Server screen appears.
4. Confirm the appropriate server and domain details. You can enter the domain user name and password and click Next.

   The Select Client Server screen appears.
5. In the Select Client Server pane, the Create Boot Disk Wizard displays a list of computers that have been backed up by CA ARCserve Backup. The panel appears blank if CA ARCserve Backup has not backed up a computer.

6. Choose the appropriate computer and click Next.
7. In Summary of Backup Information, verify the available list of sessions that must be recovered, and click Next.
8. Insert a blank floppy disk.

   The Create Boot Floppy Disk screen appears.
9. Select Copy Network Adapter driver to MSD, click Start to begin copying files to your machine-specific recovery disk.

   Note: Enable Copy Network Adapter driver files to MSD option in the following environments:

   - Disaster recovery of a remote machine
   - Disaster recovery of member servers in a SAN environment
10. When the copying finishes, the screen displays the backup sessions that will be used to recover the system if this machine-specific recovery disk is used. Click Next.
11. Click Finish.

The newly created disk is a CA 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, CA ARCserve Backup Disaster Recovery applications along 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 called 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 Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit Wizard dialog opens.

2. Select the CA ARCserve Backup Bootable CD/DVD Image option and click Next.

   The license agreement screen appears. Click OK.

3. Select the Windows operating system and click Next.

   The Specify Bootable CD/DVD Image location screen appears.

4. Specify the location for creating the Image and click Next.

   The Customize Bootable CD/DVD Image screen appears.

5. You can select the necessary options and click Next.

   When creating Windows XP (64-bit) and Windows 2003 integrated CD, as the 64-bit client agent has to copy from the CA ARCserve Backup installation media, you must select the Machine Specific Disk, device drivers, the CA ARCserve Backup Disaster Recovery Integrated option and the client machine and then integrate.

   Note: While creating the 64-bit Windows Bootable CD, if you select CA ARCserve Backup Disaster Recovery Integrated option, you will be prompted to insert CA 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.

6. Specify the path of the Windows installation media source files and click Next.

   The Summary screen appears.

7. Click Next to start the bootable CD/DVD imaging process.

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

8. The reimaging process is complete.

   You can now burn the ISO image to a bootable media.

Bootable Tape Method (OBDR) in Windows XP and Windows Server 2003

The bootable tape method for Windows XP and Windows 2003 allows you to protect the backup server without having to create a machine-specific recovery 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 XP or Windows 2003 CD and the CA ARCserve Backup CD are not required during the recovery process.

Bootable tape method supports only 32-bit Windows XP and Windows Server 2003.

To prepare for a disaster using this method

1. From the Utilities menu in the Navigation Bar on the Home Page, click Create Boot Kit wizard.

   The Create Boot Kit Wizard dialog opens.

2. Choose Create CA Bootable Tape Image and click Next.

   Note: This option is not enabled if a bootable tape drive is not detected.

3. Specify the path of the Microsoft Windows installation media, and click Next.

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

4. For Windows XP only, when you create the boot image, the Wizard prompts you for an empty floppy disk and copies the ASR files into it. This disk, the ASR Recovery Disk, is required at the beginning of the disaster recovery process.

   This does not apply to Windows 2003.

5. When the utility has finished creating the bootable image, click Finish.

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

7. Perform a full backup of the local CA ARCserve Backup server using the tape you just 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

The following section describes how to 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 CA ARCserve Backup machine-specific recovery disk for the computer that failed. This is the disk you created following the instructions in the section Create Machine Specific Recovery Disks in this chapter.
- If Windows XP Professional was installed on the original system, a Microsoft 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 CA ARCserve Backup CD.

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.

Start the Disaster Recovery Process using the Bootable CD Method

You can start the disaster recovery process using the Bootable CD method.

To perform a disaster recovery on a Windows XP or Windows 2003 computer

1. Start the computer you want to recover with the Windows XP Professional or Windows 2003 CD.
2. When prompted, press any key to boot from the CD.

   Note: To install additional SCSI drivers that are not supported on the Windows CD, press F6.

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

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

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

   If you previously pressed F6, you are prompted to insert device driver floppy disks.

5. 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 F3 to quit. This screen does not appear if disk partitions are not being recreated.

6. If you installed additional SCSI, FC or RAID drivers, you are prompted to insert device driver floppy disk.

7. Based on the configuration of the computer you are recovering, you may be prompted several times to insert the Windows Automated System Recovery disk. This disk is identical to the disk labeled CA ARCserve Backup Machine Specific Disk. Press Enter again. Setup copies files to the Windows installation folders.

8. Remove the CA 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. In consequence, the data on these volumes will not be restored.

9. When prompted, insert the CA ARCserve Backup CD and the machine-specific recovery disk and click OK.

   The Disaster Recovery wizard appears the recovery process begins.

Complete the Disaster Recovery Process

You can complete the disaster recovery process on the Windows operating system.

To complete the disaster recovery process on Windows XP and Windows 2003 computer

1. Select from the following modes that appear on the Choose Mode screen:

   Express Mode

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

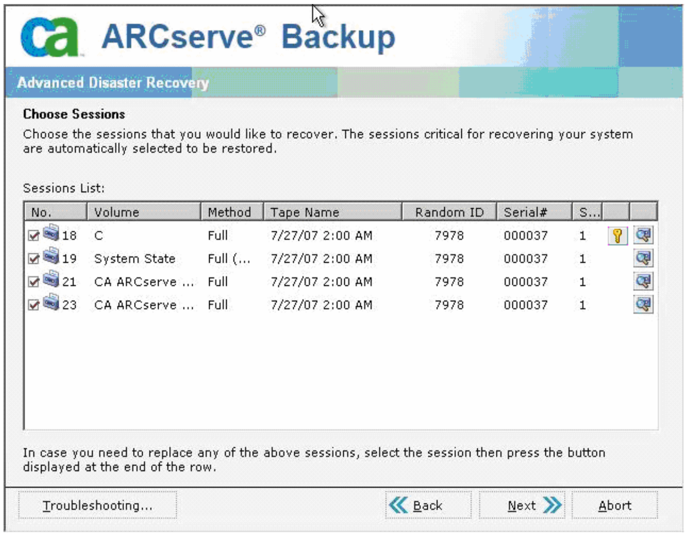
   Advanced Mode

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

   Click Next. The CA ARCserve Backup displays all the available sessions.

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

   Note: Each encrypted session has a button on right side of the session list, you can enter the session password using this button as shown in the illustration:



Choose Sessions

Choose the sessions that you would like to recover. The sessions critical for recovering your system are automatically selected to be restored.

Sessions List:

No.	Volume	Method	Tape Name	Random ID	Serial#	S...		
☑ 18	C	Full	7/27/07 2:00 AM	7978	000037	1	🔑	
☑ 19	System State	Full (...	7/27/07 2:00 AM	7978	000037	1		
☑ 21	CA ARCserve ...	Full	7/27/07 2:00 AM	7978	000037	1		
☑ 23	CA ARCserve ...	Full	7/27/07 2:00 AM	7978	000037	1		

In case you need to replace any of the above sessions, select the session then press the button displayed at the end of the row.

   Each full session of local DR has a button on the right side of the session list. Select a session and click on this button if you want to replace selected session with a different session.

   The Summary screen appears.

3. Verify the Summary list.

4. Click Start Disaster Recovery to start the process.

   The Advanced Disaster Recovery wizard copies the data from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

   Note: Click on the Troubleshooting option and select Open Console 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.

5. Enter Windows credentials, DB credentials and session password when prompted.

   Note: If this is a primary server DR, and the CA ARCserve database is located on same server, you will be prompted for CA ARCserve database information. If SQL server is configured as mixed authentication method, you must provide SQL credentials. This is critical for recovering CA ARCserve Backup database.

6. The Disaster Recovery process is complete.

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

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. For more information about how to create the Reimaging or remaster CD, see Reimage Bootable CD Using Boot Kit Wizard (see page 58).

Important! During recovery, the disaster recovery process automatically partitions your hard disk into the original configuration.

Start the Disaster Recovery Process using the Reimaged CD

You can perform disaster recovery using the Reimaged or the remastered CD.

To perform a disaster recovery on a Windows XP or Windows 2003 computer

1. Start the computer you want to recover with the reimaged CD.
2. When prompted, 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. Press F2.

   Depending on the operating system:

   For Windows XP, insert the machine specific disk after you press F2.

   For Windows Server 2003, press F2 and continue.

   Important! You must press F2. Otherwise, the normal Windows installation procedure starts.
3. The Automated System Recovery 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 F3 to quit. This screen does not appear if disk partitions are not being recreated.
4. Setup copies files to the Windows installation folders.
5. Remove any kind of floppy disks from the system except the reimaged CD.
6. The computer will reboot automatically, you will be prompted to insert Windows installation media. Insert the reimaged CD. Then Windows Automated System Recovery 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. In consequence, the data on these volumes will not be restored.

   The Disaster Recovery wizard appears the recovery process begins.

Complete the Disaster Recovery Process

You can complete the disaster recovery process using the following procedure:

To complete the disaster recovery process on Windows XP and Windows 2003 computer

1. Select from the following modes that appear on the Choose Mode screen:

   Express Mode

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

   Advanced Mode

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

   Click Next.

2. The CA ARCserve Backup displays all the available sessions.

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

   Note: Each encrypted session has a button on right side of the session list, you can enter the session password using this button as shown in the illustration:

   Each full session of local DR has a button on the right side of the session list. Select a session and click on this button if you want to replace selected session with a different session.

3. The Summary screen appears. Verify the details in the summary screen.

4. Click Start Disaster Recovery to start the process. The Advanced Disaster Recovery wizard copies the data from the specified sessions to the specified partitions. A progress bar shows the progress of the restore process.

   Note: Click the Troubleshooting option and select Open Console 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.

5. Enter Windows credentials, DB credentials and session password when prompted.

   Note: If this is a primary server DR, and the CA ARCserve database is located on same server, you will be prompted for CA ARCserve database information. If SQL server is configured as mixed authentication method, you must provide SQL credentials. This is critical for recovering CA ARCserve Backup database.

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 Windows XP and Windows 2003

To recover 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: There must be at least one full local machine backup of the system on the tape media.
- If Windows XP is installed on the local system, the ASR Recovery Disk is required.

Start the Disaster Recovery Process

You can start the recovery process with bootable tape method using the following procedure.

To recover from a disaster on a Windows XP or Windows Server 2003 computer using the 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. When prompted, press F6 to install any SCSI drivers not supported by the Windows XP or Windows 2003 CD.

7. When prompted, press F2 to begin the Windows ASR process. If a Windows XP CD was used to create the bootable image, the ASR Recovery Disk is required at this point. For Windows 2003, the floppy disk is not required.

8. 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.

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

10. 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 Disaster Recovery Process

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

To complete the disaster recovery process on a Windows XP or Windows Server 2003 computer

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

   Express recovery

   Uses all the default settings as recorded on the backup tape to restore the system with very minimal user interaction.

   Advanced Recovery

   Allows user to specific custom restore parameters to adapt to any change in the environment.

   The disaster recovery machine specific information is restored from the tape media.

2. A list of the backup sessions to be restored appears. In Advanced recovery mode, you can remove backup sessions from the list or replace one session with another session.

   Each of the selected backup sessions is restored one by one.

3. Enter Windows credentials, DB credentials and session password when prompted.

   Note: Enter the DB credentials and the password if necessary.

4. When all the sessions are finished, the system is rebooted.

Disaster Recovery Using Locally-attached USB Backup Devices

The option supports the use of USB backup devices in disaster recovery operations.

Note: You must connect and power 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 local disaster recovery, if you used 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:

Original Device List

This 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

This 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 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.

Command Prompt

Click this button to open a command prompt in a separate window. From this prompt, you can map to a remote shared folder containing the drivers, using a command like NET USE, and install the drivers sequentially from the remote location. The command prompt is also useful for debugging purposes.

Install

Click this button to open a dialog allowing you to 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.

Refresh

Click this button to manually refresh the Current Device List after installing a driver. It can take some time before the installed driver begins to work with the device.

Install USB Devices After Backup

You are prompted to 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

This section describes how you can use the Bootable CD method to protect local and remote Windows XP (64 bit) and Windows 2003 (64 bit) and recover from disaster. The Windows platforms that are supported include:

- Windows 2003 IA64
- Windows 2003 X64
- Windows XP X64

Note: The Windows XP IA64 is not supported.

The Windows 64-bit DR uses the Client Agent to restore the actual data.

Disaster Recovery Requirements in Windows XP and Windows 2003

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

- A CA ARCserve Backup machine-specific recovery disk for the computer that failed. This is the disk you created following the instructions in the section Create Machine-Specific Recovery Disks in this chapter.
- 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 CA ARCserve Backup installation media

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.

Perform Disaster Recovery on Windows XP and Windows Server 2003

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

To perform Disaster Recovery on Windows XP and Windows Server 2003

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

   A prompt appears.

2. When prompted, press any key to boot from the CD.

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

   The Windows Automated System Recovery GUI appears.

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

4. Windows setup formats the system and boot partitions and copy necessary files onto hard drive. After file copy finish, reboot the machine.

5. Windows setup continues installing device drivers and network protocols.

6. You can see the operating system formats the volumes screen.

   Important! Do not press Enter, Esc, or Alt-F4 and interrupt when the Automated System Recovery is formatting the volumes on your Windows XP or Windows 2003, as the formatting process terminates. In consequence, the data on these volumes will not be restored.

   The DRLAUNCH is initiated automatically by the Windows ASR.

7. The DRLAUNCH.exe copies the supplied media files and starts the 64-bit Advanced Disaster Recovery Wizard.

   The ADR GUI ADRMAIN.exe starts and reads the DR information.

8. You can select the Express mode or the Advanced mode in the Choose Mode screen that appears.

   - In Express mode you can recover the system using the machine default settings stored during the backup time.

   - 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 distributed server and local Disaster Recovery using remote FSD.

   Media server is started for the Local DR.

9. Configure the remote FSD page.

   Enter the authentication details, if necessary.

The session list appears. You can make changes to this list.

10. The Summary page appears listing the sessions that you want to restore.

    The restore process begins.

11. Reboot the machine after the restore process is complete.

    Note: If this is a primary server DR, and the CA ARCserve database is located on same server, you will be prompted for CA ARCserve database information. If SQL server is configured as mixed authentication method, you must provide SQL credentials.

Disaster Recovery in Windows Server 2008

The Windows 2008 disaster recovery is based on the Windows Server 2008 Recovery Environment to perform restore operations. Only Bootable CD method is supported for Windows Server 2008 DR. The Windows platforms that are supported include:

- Windows Server 2008 (32-bit)
- Windows Server 2008 (x64-bit)
- Windows Server 2008 (IA 64-bit)

Note: For information about Windows Server 2008, see http://www.microsoft.com/.

Disaster Recovery Requirements in Windows Server 2008

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

- CA ARCserve Backup machine-specific recovery disk or an USB flash media

  Note: Windows Server 2008 machine-specific disk can be stored on floppy disk as well as USB flash media.

  For more information about Create Machine Specific Recovery Disks (see page 56), see section Disaster Recovery Methods.

- The Windows Server 2008 installation media of the correct edition (for example, Web, Standard, or Enterprise Edition)
- CA ARCserve Backup Disaster Recovery CD

Recover Windows Server 2008 from a Disaster

You can perform a disaster recovery on Server 2008 using the Bootable CD method.

To recover Windows Server 2008 from a disaster

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

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

2. The system prompts you for the CA ARCserve Backup Disaster Recovery media.

3. Insert the CA ARCserve Backup Disaster Recovery media and click Next.

   Advanced Disaster Recovery screen appears and starts the recovery process.

4. Specify the path for machine specific disk for restore and click Next.

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

5. Select the Express mode on the Choose Mode screen and click Next.

   You can select the Advanced mode depending in the following conditions:

6. The Load Drivers screen appears.

   Configure and load the drivers, if necessary.

7. 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 distributed server and local Disaster Recovery using remote FSD.

8. Configure the remote FSD page. Enter the authentication details, if necessary.

   The session list appears.

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

   The Summary page appears listing the sessions that you want to restore.

10. The restore process begins.

    Reboot the machine after the restore process is complete.

Chapter 5: Disaster Recovery Scenarios

For remote disaster recovery to connect to the backup server successfully, you must set the value of following registry key to 0 on the backup server machine:

HKEY_LOCAL_MACHINE\Software\Polices\Microsoft\Windows XP\RPC\RestrictRemoteClients

Note: If you are using an earlier version of the backup server, or if the Software\Computer Associates\CA ARCserve Backup\Base\Tapeengine\DR\UseNetBIOS registry key is set to 1, change the option Network access: Sharing and security model for local accounts security policy to Classic – local users authenticate as themselves.

This section contains the following topics:

Disaster Recovery Scenarios on Windows 2000

The following scenarios provide system-specific information and procedures to recover typical Windows 2000 systems.

Scenario 1: Remote Disaster Recovery for a Compaq ProLiant ML370

The following scenario uses the bootable CD disaster recovery method to recover a remote Windows 2000 client.

Client Specifications

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

- System: Compaq ProLiant ML370 with 1.4GHz CPU and 1 GB RAM
- Network Adapter: Intel 82557x-based PCI Ethernet Adapter (10/100)

- Storage
  - Five disks (36 GB) connected to Compaq Smart Array 5i RAID controller
  - First logical disk configured as RAID1 (36 GB)
  - Second logical disk configured as RAID5 (72 GB)
- Partitions
  - Contains Compaq SmartStart 5.40 EISA partition on disk0 (first RAID volume)
  - Drive C—4 GB—disk0—Windows/Boot volume (NTFS)
  - Drive D—30 GB—disk0—data volume (NTFS)
  - Drive E—72 GB—disk1—data volume (NTFS)
- Software Environment
  - Microsoft Windows 2000 Advanced Server with integrated Service Pack 1
  - CA ARCserve Backup Client Agent for Windows

Server Specifications

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

- System: HP tc3100 server connected to Quantum SDLT changer through Emulex LP9000 adapter
- Software Environment:
  - Microsoft Windows 2000 Advanced Server with integrated Service Pack 2
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option
  - CA ARCserve Backup Tape Library Option
  - CA ARCserve Backup SAN Option

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 are adding the Client Agent for Windows to your client computer (Compaq ProLiant ML370):

1. Note the hardware RAID configuration and EISA partition in your system. In this scenario, we have the following:

   - Five disks of 36 GB connected to Compaq Smart Array 5i RAID controller
   - First logical disk configured as RAID1 (36 GB)
   - Second logical disk configured as RAID5 (72 GB)
   - Compaq SmartStart 5.40 EISA partition on disk0 (first RAID volume)

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

2. Add the CD provided by the hardware vendor (the CD used to create RAID volumes and EISA partitions) to the disaster recovery kit for this client computer. In this scenario, it is the Compaq SmartStart CD.

3. Save the extra hardware drivers you installed (by pressing F6) when you initially set up your Windows 2000 client computer. Add these disks to the disaster recovery kit for this client computer. You must provide these drivers again during disaster recovery. In this example, save the Compaq 5i RAID adapter driver disk.

   Note: If you do not know the devices installed on the Windows client computer, look in Device Manager. If your system has failed, open the CardDesc.txt file on the machine specific disk to see a summary of the devices and drivers.

4. Add the Windows client computer (Compaq ProLiant ML370) to the CA ARCserve Backup server and perform a full computer backup.

5. Create a disaster recovery bootable CD using the Create Boot Kit Wizard. For more information, see the section Preparing for Disaster Using the Bootable CD Method in this guide.

6. Create a machine specific disk. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.

7. Add the disaster recovery bootable CD and the machine specific disk to the disaster recovery kit for this system.

Disaster Recovery Prerequisites

You must have performed a full backup using CA ARCserve Backup and have the following items before you can start the disaster recovery process:

- The latest CA ARCserve Backup machine specific disk. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.
- The disaster recovery bootable CD. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.
- Compaq SmartStart CD
- Compaq Smart Array 5i RAID Adapter driver disk
- The original hardware RAID configuration

Recover from Disaster Using the SmartStart CD Setup

To recover from a disaster using the SmartStart CD setup

1. Start the client computer (Compaq ML370) using the SmartStart CD.
2. Follow the Compaq guidelines and your original configuration to recreate the hardware RAID configuration.
3. Use the SmartStart CD to install the EISA partition as it was in the original configuration.
4. Boot the client computer using the disaster recovery bootable CD and follow the on-screen instructions. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.
5. Insert the machine specific disk to start the disaster recovery bluescreen mode.
6. Press F6 to add the Compaq RAID drivers using the Compaq Smart Array 5i RAID Adapter driver disk.
7. After Windows loads the drivers from the Compaq Smart Array 5i RAID Adapter driver disk, insert the machine-specific recovery disk again. The option reads the original system disk configuration from the machine-specific recovery disk

   Note: If you do not insert this disk after the F6 drivers are loaded, the original disk configuration is not restored.
8. After some time, the original partition layout of the computer appears. Select the disk and partition in which Windows 2000 was installed and press Enter. Do not modify the displayed partition structure.

   The disaster recovery bluescreen mode completes and the computer boots to the Disaster Recovery Wizard.

9. Follow the Disaster Recovery Wizard instructions. The wizard installs the network, configures and formats the drives, and connects to the CA ARCserve Backup server over the network. The system may reboot a few times during this process.
10. When prompted by the Disaster Recovery Wizard, start the data restoration process.
11. When the disaster recovery process finishes, boot back to your previous system configuration.

Scenario 2: Local Disaster Recovery for an IBM xSeries 235

The following scenario uses the bootable CD disaster recovery method to recover a local Windows 2000 computer. For this scenario, you can configure an alternate location when the option is installed. You must create a machine-specific recovery disk from this location for disaster recovery.

Server Specifications

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

- System: IBM xSeries 235 with 1.8 GHz CPU and 1 GB RAM connected to Sony LIB-162 StorStation through Emulex LP8000 Adapter and Crossroads 4250 FC Bridge
- Network Adapter: Intel 82557x-based PCI Ethernet Adapter (10/100)
- Storage
  - Five disks/33.9 GB connected to LSI 1030 MPT RAID controller
  - First logical disk configured as RAID1 (33.9 GB)
  - Second logical disk configured as a stand-alone SCSI Disk (33.9 GB)
  - Third logical disk configured as a stand-alone SCSI Disk (33.9 GB)
  - Fourth logical disk configured as a stand-alone SCSI Disk (33.9 GB)

- Partitions
  - Contains IBM NetfinitySP EISA partition on disk0
  - Drive C—4 GB—disk0—Windows/Boot volume (NTFS)
  - Drive E—30 GB—disk0—data volume (NTFS)
  - Drive F—10 GB—disk1—simple volume (NTFS)
  - Drive G—30 GB—disk2/3—spanned volume (NTFS)
  - Drive H—20 GB—disk2/3—striped volume (NTFS)
- Software Environment
  - Microsoft Windows 2000 Advanced Server with integrated Service Pack 2
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option
  - CA ARCserve Backup Tape Library Option

Prepare for Disaster During Local Server Setup

Planning for a successful disaster recovery starts when you set up your server. Perform the following procedure when you install CA ARCserve Backup and the Disaster Recovery Option on your server (IBM xSeries 235):

1. Note the hardware RAID configuration and EISA partition in your system. In this scenario, we have the following:
   - Five disks of 33.9 GB connected to LSI 1030 MPT RAID controller
   - First logical disk configured as RAID1 (33.9 GB)
   - Second, third, and fourth logical disks configured as stand-alone SCSI disks (33.9 GB each)
   - IBM NetfinitySP EISA partition on disk0 (first volume)

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

2. Add the CD provided by the hardware vendor (to create the RAID volumes and the EISA partition) to the disaster recovery kit for this server. In this scenario, we add the IBM ServeRAID 5.10 Support CD to create the RAID volumes, and the ServeGuide 6.0.9a Setup and Installation CD, to create the EISA partition.

3. Save the extra hardware drivers you installed (by pressing F6) when you initially set up your Windows 2000 server. Add these disks to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery. In this example, we save the LSI 1030 MPT RAID controller and the Emulex LP8000 Fiber Channel Adapter driver disks.

   Note: If you do not know the devices installed on the Windows server, look in Device Manager. If your system has failed, open the CardDesc.txt file on the machine-specific recovery disk to see a summary of the devices and drivers.

4. Configure an alternate location, if you did not perform this task when you installed the agent.

   For information about how to install and configure the option see Install and Configure the Option (see page 29) in the "Installing the Option" chapter of this guide.

5. Start CA ARCserve Backup and perform a full backup.

6. Create a disaster recovery bootable CD using the Boot Kit wizard. For more information, see the section Bootable CD Method in the "Disaster Recovery on Windows 2000" chapter of this guide.

7. Create a machine-specific recovery disk.

   In this scenario, we created the machine-specific recovery disk from the alternate location.

8. Add the disaster recovery bootable CD and the machine-specific recovery disk to the disaster recovery kit for this system.

Disaster Recovery Prerequisites

You must have performed a full backup of your computer on the CA ARCserve Backup server and have the following items before you can start the disaster recovery process:

- The most current machine specific disk. For more information, see the section Install and Configure the Option in the "Installing the Option" chapter of this guide.
- Disaster recovery bootable CD. For more information, see the section Bootable CD Method in the "Disaster Recovery on Windows 2000" chapter of this guide.
- IBM ServeRAID 5.10 Support CD
- IBM ServerGuide 6.0.9a Setup and Installation CD
- LSI 1030 MPT RAID controller driver disk.
- Emulex LP8000 Fiber Channel Adapter driver disk
- The original hardware RAID configuration

Recover from Disaster Using IBM Setup CDs

To recover from a disaster using IBM Setup CDs

1. Boot the server (IBM xSeries 235) using the IBM ServeRAID 5.10 Support CD.
2. Follow the IBM guidelines and your original configuration to recreate the hardware RAID configuration.
3. Install the EISA partition as it was in the original configuration using the IBM ServerGuide 6.0.9a Setup and Installation CD.

Set Up Disaster Recovery Bootable CDs

To set up a disaster recovery bootable CD

1. Start the server using the Disaster Recovery Bootable CD and follow the on-screen instructions. For more information, see the section Disaster Recovery Using the Bootable CD Method of this guide.
2. Insert the machine specific disk to start the disaster recovery bluescreen mode.
3. Press F6 to add the LSI 1030 MPT RAID controller drivers using the LSI 1030 MPT RAID controller driver disk and the Emulex LP8000 Fiber Channel Adapter driver disk.
4. After Windows loads the drivers from the LSI 1030 MPT RAID controller driver disk and the Emulex LP8000 driver disk, insert the machine specific disk again. The option reads the original system disk configuration from the machine specific disk.

   Note: If you do not insert this disk after the F6 drivers are loaded, the original disk configuration is not restored.
5. After some time, the original partition layout of the computer appears. Select the disk partition in which Windows 2000 was installed, and press Enter. Do not modify the displayed partition structure.

   The disaster recovery bluescreen mode completes and the computer boots to the Disaster Recovery Wizard.
6. Follow the Disaster Recovery Wizard instructions. The wizard installs the network, and configures and formats the drives. The system may reboot a few times during this process.
7. When prompted by the Disaster Recovery Wizard, start the data restoration process.
8. When the disaster recovery process finishes, boot back to your previous system configuration.

Scenario 3: Primary SAN Disaster Recovery for an IBM Netfinity 6000R

The following scenario uses the bootable CD disaster recovery method to recover a primary SAN Windows 2000 computer.

Server Specifications

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

- System: IBM Netfinity 6000R with one 700 MHz CPU and 512 MB RAM
- Fiber Environment: QLA2310F PCI Fiber Channel Adapter connected to Sony LIB-162 StorStation through Brocade 12000 switch and Crossroads 4250 FC Bridge
- Network Adapters:
  - IBM Netfinity Fault Tolerance PCI Adapter
  - Linksys EG1032/EG1064 Instant Gigabit Network Adapter
- Storage: Two disks of 18.2 GB and four disks of 36.4 GB connected to IBM ServeRAID-4H controller, configured as a single RAID 5 logical disk of 86.785 GB data space and 17.357 GB parity space
- Partitions
  - Drive C—19.53 GB—disk0—Windows/system volume (NTFS)
  - Drive D—58.59 GB—disk0—data volume (NTFS)
  - Drive E—6.62 GB—disk0—data volume (NTFS)
- Software Environment
  - Microsoft Windows 2000 Server with Service Pack 2
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option
  - CA ARCserve Backup Tape Library Option
  - CA 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 CA ARCserve Backup and the CA ARCserve Backup Disaster Recovery Option on your primary server (IBM Netfinity 6000R):

Note: This scenario does not use an EISA partition.

1. Note the hardware RAID configuration. In this scenario, we have the following:

   - Two disks of 18.2 GB and four disks of 36.4 GB connected to IBM ServeRAID-4H controller.
   - All six disks configured into a single RAID 5 volume of 86.785 GB data space and 17.357 GB parity space

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

   This scenario does not use an EISA partition.

2. Add the CD provided by the hardware vendor (to create the RAID volumes) to the disaster recovery kit for this server. In this example, it is the IBM Server Guide 6.0.9a Setup and Installation CD.

3. Save the extra hardware drivers you installed (by pressing F6) when you initially set up your Windows 2000 server. Add these disks to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery. In this example, we save the Qlogic QLA2310F PCI Fiber Channel Adapter and the IBM Server RAID 5.10 adapter driver disks.

   Note: If you do not know the devices installed on the Windows server, look in Device Manager. If your system has failed, open the CardDesc.txt file on the machine-specific recovery disk to see a summary of the devices and drivers.

4. Start CA ARCserve Backup and perform a full backup.

5. Create a disaster recovery bootable CD using the Boot Kit Wizard. For more information, see the section Disaster Recovery using the Bootable CD Method of this guide.

6. Create a machine-specific recovery disk. For more information, see the section Disaster Recovery in Windows 2000 using the Bootable CD Method of this guide.

7. Add the disaster recovery bootable CD and the machine-specific recovery disk to the disaster recovery kit for this system.

Disaster Recovery Prerequisites

You must have performed a full backup of your computer on the primary SAN CA ARCserve Backup server and have the following items before you can start the disaster recovery process:

- The latest CA ARCserve Backup machine-specific recovery disk (for more information, see the section Install and Configure the Option in the "Installing the Option" chapter of this guide)
- Disaster recovery bootable CD (for more information, see the section Disaster Recovery Using the Bootable CD Method of this guide)
- QLogic QLA2310F PCI Fiber Channel Adapter driver disk
- IBM ServeRAID 5.10 adapter driver disk.
- IBM ServerGuide 6.0.9a Setup and Installation CD
- The original hardware RAID configuration

Recover from Disaster Using IBM Setup CDs

To recover from a disaster using IBM Setup CDs

1. Stop the Tape Engine in all of the Distributed Servers.
2. Boot the server (IBM Netfinity 6000R) using the IBM Server Guide 6.0.9a Setup and Installation CD.
3. Follow the IBM guidelines and your original configuration to recreate the hardware RAID configuration.

Set Up Disaster Recovery Bootable CDs

To set up a disaster recovery bootable CD

1. Start the server using the disaster recovery bootable CD and follow the on-screen instructions. For more information, see the section Bootable CD Method in the "Disaster Recovery on Windows 2000" chapter of this guide.
2. Insert the machine-specific recovery disk to start the disaster recovery bluescreen mode.
3. Press F6 to add the QLogic QLA2310F PCI Fiber Channel adapter driver using the driver disk and the IBM Server RAID 5.10 adapter driver using the driver disk.
4. After Windows loads the drivers from the QLogic QLA2310F PCI Fiber Channel adapter driver disk and the IBM Server RAID 5.10 adapter driver disk, insert the machine-specific recovery disk again.

   Note: If you do not insert this disk after the F6 drivers are loaded, the original disk configuration is not restored.

5. After some time, the original partition layout of the computer appears. Select the disk and partition where Windows 2000 was installed and press Enter. Do not modify the displayed partition structure.

   The disaster recovery bluescreen mode completes and the computer boots to the Disaster Recovery Wizard.

6. Follow the Disaster Recovery Wizard instructions. The Disaster Recovery Wizard installs the network, and configures and formats the drives. The system may reboot a few times during this process.

7. When prompted by the Disaster Recovery Wizard, start the data restoration process.

8. When the disaster recovery process finishes, boot back to your original system.

9. Start the Tape Engine in all of the distributed servers.

Scenario 4: Bootable Tape Disaster Recovery for an HP tc3100

The following scenario uses the bootable tape method for recovering a local Windows 2000 computer.

Server Specifications

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

- System: HP tc3100 with 1 CPU and 1 GB RAM
- Network Adapter: Intel 82557x-based PCI Ethernet Adapter (10/100)
- Bootable Tape Device: HP Ultium-1 SCSI tape device, Model C7370-00150 connected to an Adaptec 29160 SCSI Controller
- Storage
  - Five disks/17 GB connected HP NetRAID RAID controller
  - Five logical disks of 17 GB each configured RAID0

- Partitions
  - Contains HP EISA partition on disk0
  - Drive C — 4 GB — disk0 — Windows/Boot (NTFS)
  - Drive E — 13 GB — disk0 — data volume (NTFS)
  - Drive F — 17 GB — disk1 — data volume (NTFS)
  - Drive G — 10 GB — disk2 — data volume (NTFS)
  - Drive H — 7 GB — disk3 — data volume (NTFS)
  - Drive I — 17 GB — disk4 — data volume (NTFS)
- Software Environment
  - Microsoft Windows 2000 Server with integrated Service Pack 2
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option

Prepare for Disaster During Local Server Setup

Planning for a successful disaster recovery begins when you set up your server. Perform the following procedure when you install CA ARCserve Backup and the Disaster Recovery Option on your server (HP tc3100):

1. The tape device must be bootable. When you reboot your system, enter the SCSI Utility (in this scenario, the Adaptec SCSI Utility). Select Advanced Configuration, and ensure that you enable BIOS support for bootable CDs.
2. Note the hardware RAID configuration and EISA partition in your system. In this scenario we note:
   - Five disks/17 GB connected HP NetRAID RAID controller
   - HP EISA partition on disk0 (first volume)

   Note: The option does not recreate the hardware RAID settings and does not restore the EISA partitions. You must manually recreate the hardware RAID configuration and EISA partitions before starting disaster recovery.
3. Add the CD provided by the hardware vendor used to create the RAID volumes and the EISA partition to the disaster recovery kit for this server. In this scenario, we add the HP Netserver Navigator Support CD, to create the RAID volumes and the EISA partition.
4. Save the custom hardware diskettes that you installed, using F6, when you initially set up your Windows 2000 server. Add these diskettes to the disaster recovery kit for this computer. You must provide these drivers again during disaster recovery. In this scenario, we save the HP NetRAID 2M driver diskette.

5. Create a CA Bootable Tape image, using the Boot Kit Wizard. For more information, see the section Recover from Disaster Using the Bootable Tape Method in the in the "Disaster Recovery on Windows 2000" chapter of this guide." chapter of this guide. This creates an image called *tober.iso*.
6. Format the media using the Device Manager or Device Wizard. This copies the image created in the previous step to the tape.
7. Start CA ARCserve Backup and take a local, full backup using the tape created in the previous step.
8. Add the disaster recovery bootable tape to the disaster recovery kit for this computer.

Disaster Recovery Prerequisites

You must have the following items before you can start the disaster recovery process:

- A bootable tape device
- The media containing the CA Bootable Tape image and a full backup of your computer on the CA ARCserve Backup server
- HP Netserver Navigator M.04.06 Support CD
- HP NetRAID 2M RAID controller driver diskette
- The original hardware RAID configuration

Recover From Disaster Using HP Setup CDs

To recover from a disaster using the HP Setup CD

1. Start the server (HP tc3100) using the HP Netserver Navigator M.04.06 Support CD.
2. Follow the HP guidelines and your original configuration for recreating the hardware RAID configuration.
3. Using the HP Netserver M.04.06 Support CD, install the EISA partition as it was in the original configuration.

Set Up Disaster Recovery Bootable Tapes

To set up a bootable tape

1. Remove all media from the diskette and CD drive.
2. Shut down the server and the tape drive.
3. Start the tape drive in boot mode. In this scenario, press and hold the eject button and power button simultaneously for 10 seconds. The Ready light should flash on and off.
4. Insert the bootable tape backup media.

5. Start the server to enter disaster recovery mode.
6. Answer Y to start the disaster recovery bluescreen mode.
7. Press F6 to add the HP NetRAID 2M RAID controller driver. Windows loads the driver from the HP NetRAID 2M RAID controller driver diskette.
8. After a few moments, the original partition layout of the computer appears. Select the disk and partition in which Windows 2000 was installed and press Enter. Do not modify the partition structure in any way.

   The disaster recovery bluescreen mode completes the process and the computer boots into the Disaster Recovery Wizard.
9. Follow the instructions displayed on the Disaster Recovery Wizard screens. The wizard formats drives. Your computer may reboot several times during the process.
10. Start the data restore process when prompted by the wizard.
11. Restart your computer when restoration is complete.

Scenario 5: Local Disaster Recovery for a Fujitsu Primergy TX200

The following scenario uses the bootable CD disaster recovery method to recover a local CA ARCserve Backup server on Windows 2000.

Server Specifications

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

- System: Fujitsu Primergy TX200 with 1.8 GHz CPU and 512 MB RAM connected to a StorageTek L20 Tape Library
- Network Adapter: Broadcom NetXtreme Gigabit Ethernet Adapter
- Storage
  - Three disks/8.6 GB connected to Mylex AcceleRAID 352 RAID controller
  - Three physical drives configured as RAID level 1
  - Two logical disks (8.6 GB each)
  - One hot spare (8.6 GB)

- Partitions
  - Contains Fujitsu EISA partition on logical drive 1
  - Drive C - 8.2 GB - logical disk 0 - Windows/Boot volume (NTFS)
  - Drive E - 4.3 GB - logical disk 1- data volume (NTFS)
  - Drive F - 4.3 GB - logical disk 1- data volume (NTFS)
- Software Environment
  - Microsoft Windows 2000 Server with Service Pack 4
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option
  - CA ARCserve Backup Tape Library Option

Prepare for Disaster During Local Server Setup

Planning for a successful disaster recovery begins when you set up your server. Perform the following procedure when you install CA ARCserve Backup and the Disaster Recovery Option on your server (Fujitsu Primergy TX200):

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

   - Three disks of 8.6 GB connected to Mylex AcceleRAID 352 RAID controller
   - Three logical disks configured as RAID level 1
   - One drive as hot spare and two drives configured as two logical drives
   - Fujitsu Primergy EISA partition on logical disk 0

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

2. Add the CD provided by the hardware vendor (to create the RAID volumes and the EISA partition) to the disaster recovery kit for this server. In this scenario, we add the Fujitsu Primergy ServerStart CD version 5.307 to create the RAID volumes and the EISA partition.

3. Save the extra hardware drivers you installed (by pressing F6) when you set up your Windows 2000 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 Mylex AcceleRAID 352 RAID controller floppy disk.

   Note: If you do not know the devices installed on the Windows server, look in the Device Manager. If your system has failed, open the CardDesc.txt file on the machine-specific recovery disk to view a summary of the devices and drivers.

4. Configure an alternate location if you did not perform this task when the option was installed. For more information, about the Install and Configure the Option see chapter “Installing the Option."

5. Start CA ARCserve Backup and perform a full backup.

6. Create a disaster recovery bootable CD using the Boot Kit Wizard. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.

7. Create a machine-specific recovery disk. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.

8. Add the disaster recovery bootable CD and the machine-specific recovery disk to the disaster recovery kit for this system.

Disaster Recovery Prerequisites

You must have performed a full backup of your computer on the CA ARCserve Backup server before you can start the disaster recovery process. In addition, you must have the following items before you begin disaster recovery:

- The disaster recovery bootable CD. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.
- The machine-specific recovery disk. For more information about Machine-specific Recovery Disks for the Bootable CD Method, see chapter "Disaster Recovery on Windows 2000.”
- Fujitsu Primergy ServerStart Version 5.307 CD
- Mylex AcceleRAID 352 RAID controller driver floppy disk.
- The original hardware RAID configuration.

Recover from Disaster Using Fujitsu Primergy ServerStart CDs

To recover from a disaster using the Fujitsu Primergy ServerStart version 5.307 CD

1. Boot the server (Fujitsu Primergy TX200) using the Fujitsu Primergy ServerStart version 5.307 CD.

2. Follow the Fujitsu guidelines and your original configuration to recreate the hardware RAID configuration and install the EISA partition.

Perform Disaster Recovery Using the Bootable CD

To begin the disaster recovery process using the bootable CD

1. Start the server using the Disaster Recovery Boot CD and follow the on-screen instructions. For more information, see the section Bootable CD Method in the “Disaster Recovery on Windows 2000” chapter of this guide.
2. Insert the machine-specific recovery disk to start the disaster recovery bluescreen mode.
3. Press F6 to add the Mylex AcceleRAID 352 RAID controller drivers using the Mylex AcceleRAID 352 RAID controller driver disk.
4. When Windows has loaded the drivers from the Mylex AcceleRAID 352 RAID controller driver disk, insert the machine-specific recovery disk again. The original system disk configuration is read from the machine-specific recovery disk.

   Note: If you do not insert this disk after the F6 drivers are loaded, the original disk configuration is not restored.
5. After a period of time, the original partition layout of the computer appears. Select the C partition and press Enter. Do not modify the displayed partition structure. The disaster recovery bluescreen mode finishes, and the computer boots to the Disaster Recovery Wizard.
6. Follow the steps in the Disaster Recovery Wizard. The wizard installs the network, and configures and formats the drives. The system may reboot several times during this process.
7. When prompted, start the data restoration process.
8. When the disaster recovery process finishes, you can boot back to your previous system configuration.

Disaster Recovery Scenarios on Windows 2003

The following scenario 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 following scenario uses the ASR-based (Automated System Recovery) disaster recovery process to recover a CA 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
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option
  - CA ARCserve Backup Tape Library Option
  - CA 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 CA 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 CA ARCserve Backup and perform a full backup.

Disaster Recovery Prerequisites

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

- CA ARCserve Backup machine-specific recovery disk. For more information, see the section "Disaster Recovery Methods on Windows Server 2003 and Windows XP" of this guide.
- 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
- CA ARCserve Backup for Windows distribution CD
- Emulex LP9000 PCI Fibre Channel HBA driver disk
- HP Smart Array 642 Controller driver disk

Recover from Disaster

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 the section "Disaster Recovery Methods on Windows Server 2003 and Windows XP."
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 CA 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 CA ARCserve Backup files and services and connects to the CA 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 following scenario uses the ASR-based (Automated System Recovery) advanced disaster recovery process to recover a CA 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
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option
  - CA ARCserve Backup Tape Library Option
  - CA ARCserve Backup SAN Option

Prepare for Disaster During Primary Server Setup

A successful disaster recovery begins when you set up your primary server. Perform the following procedure when you install CA 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 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.

   Start CA ARCserve Backup and perform a full backup.

Disaster Recovery Prerequisites

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

- CA ARCserve Backup machine-specific recovery disk
- 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
- CA 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 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 CA 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 CA ARCserve Backup files and services and connects to the CA 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 following scenario 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 following scenario uses the Automated System Recovery (ASR)-based disaster recovery process to recover a CA 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
  - CA 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
  - Microsoft Windows 2000 Advanced Server with integrated Service Pack 4
  - CA ARCserve Backup
  - CA ARCserve Backup Disaster Recovery Option
  - CA ARCserve Backup Agent for Open Files
  - CA 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 CA ARCserve Backup server and perform a full backup.

Disaster Recovery Prerequisites

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

- CA ARCserve Backup machine-specific recovery disk. For more information see the section "Disaster Recovery Methods on Windows Server 2003 and Windows XP" of this guide.
- A full backup of the 1600SC client
- Windows XP distribution CD
- Dell Server Assistant version 7.5 Bootable CD
- The original hardware RAID configuration
- CA 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:

1. Boot the client computer (Dell PowerEdge 1600SC) using the Dell Server Assistant version 7.5 Bootable CD.
2. Follow the Dell guidelines to recreate the hardware RAID configuration.
3. Boot the client computer using the Windows XP distribution CD and follow the on-screen ASR instructions. For more information on Disaster Recovery, see the section "Disaster Recovery Methods on Windows Server 2003 and Windows XP" of this guide.
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 CA ARCserve Backup machine-specific recovery disk and press Enter.
7. 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. 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.
8. After Windows loads the driver, 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. 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.

10. The Windows Install screen appears and 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 CA ARCserve Backup files and services and connects to the CA 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.

Disaster Recovery Scenarios on Windows 2008

The following scenario 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 2008 system.

Scenario 1: Primary Server Disaster Recovery

The following scenario 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 CA 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 CA ARCserve Backup and perform a full backup.

Disaster Recovery Prerequisites

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

- CA ARCserve Backup machine specific recovery disk
- A full backup of the primary server
- Windows Server 2008 installation media
- CA ARCserve Backup installation media
- 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 CA 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 distributed 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 appears.

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: 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 distributed SAN servers in Windows 2000 and 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 distributed SAN servers. The option can recover any SAN server, as long as a full computer backup was performed using CA 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 distributed SAN servers, the option can determine if the current server is a primary server or distributed server.

- If the current server is a primary SAN server, the option connects to the SAN and uses the devices on the SAN directly.
- If the current server is a distributed SAN server, the option first contacts the primary SAN server. The option then communicates with the primary SAN server to handle any device operations on the SAN.

Appendix B: Recovering Clusters

Disaster recovery in a Windows-based cluster environment is a complex task. Although CA 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 2000 Advanced Server or Windows 2003 Enterprise Server.

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 following scenarios 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 following sections detail the requirements for 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 2000 Advanced Server or Microsoft Windows 2003 Enterprise Server 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.
- CA 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 2000 Advanced Server or Windows 2003 Enterprise Server.
- 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 2000 Advanced Server or 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, Disk Management.

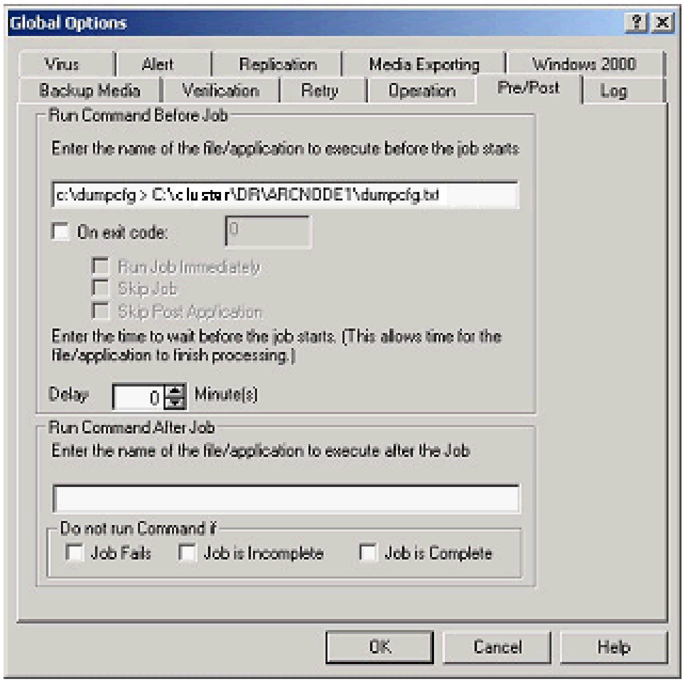
- Run the dumpcfg.exe utility (available on the Windows 2000 or Windows 2003 Resource Kit) to save the cluster quorum disk signature. It is good practice to preserve the important hard disk signatures if this information is not often used.

  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:

  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
     ```



Enter the name of the file/application to execute before the job starts: c:\dumpcfg > C:\cluster\DR\ARCNODE1\dumpcfg.txt

□ On exit code: 0

□ Run Job Immediately
□ Skip Job
□ Skip Post Application

Enter the time to wait before the job starts. (This allows time for the file/application to finish processing.)

Delay 0 Minute(s)

Enter the name of the file/application to execute after the Job:

Do not run Command if: □ Job Fails □ Job is Incomplete □ Job is Complete

- 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.

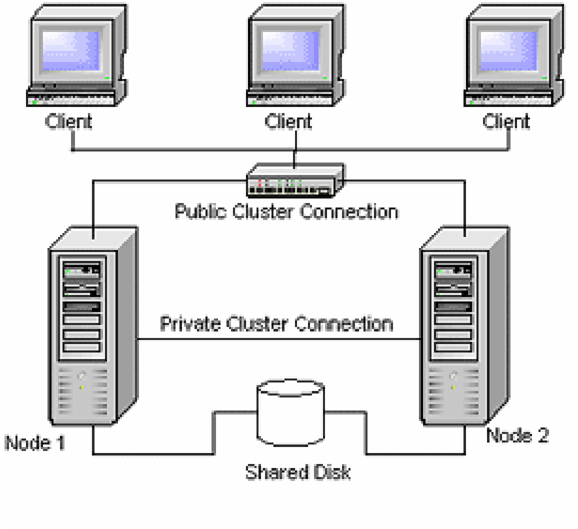
Non-quorum Disk

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 dumpcfg.exe)
- 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 following cases 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 following cases. 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.
   d. Use the dumpcfg.exe utility to restore the original disk signature for the shared disk. See the output file created by the dumpcfg.exe utility during the backup.
   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 CA 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

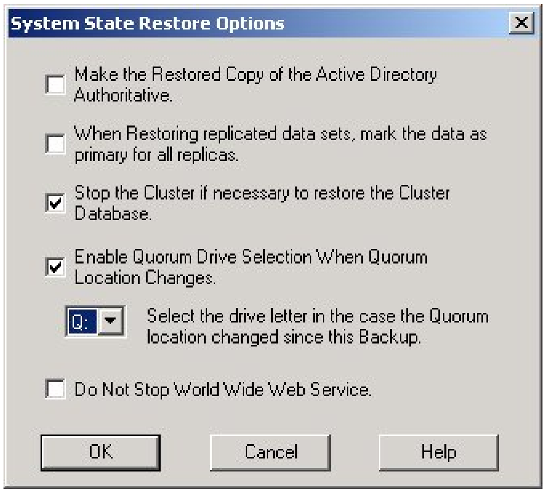
To recover cluster quorum disks with no node failures

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. Shut down the primary node.

6. If the cluster quorum disks are physically damaged, replace the cluster quorum shared disk with new disks.
7. Start the primary node.

   Note: Have the Cluster Disaster Recovery Requirements readily available for reference.
8. Use the dumpcfg.exe utility to restore the original disk signature for the shared disk. See the output file created by the dumpcfg.exe utility during the backup.
9. Recreate and reformat the partitions on the non-quorum shared disk.
10. From the Device Manager View menu, select Show Hidden Devices and enable the Cluster Disk Driver setting.
11. Restore the system state backup. In CA ARCserve Backup, select System State session and right-click to select the local option.

    The System State Restore Options dialog opens.



System State Restore Options

☐ Make the Restored Copy of the Active Directory Authoritative.

☐ When Restoring replicated data sets, mark the data as primary for all replicas.

☑ Stop the Cluster if necessary to restore the Cluster Database.

☑ Enable Quorum Drive Selection When Quorum Location Changes.

Q: Select the drive letter in the case the Quorum location changed since this Backup.

☐ Do Not Stop World Wide Web Service.

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.

12. Restart the primary node.
13. 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 ARCserve Home directory.

    ```
    caclurst /s c:\%SystemRoot%\clusbkup /q Q:
    ```

    If this is a remote disaster recovery, copy the caclurst.exe file to the Client Agent for Windows directory.

14. Reboot the primary node.
15. Connect the shared disks to the secondary node.
16. 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 the section Recover Cluster Quorum Disks with No Node Failures in this chapter.

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 C: Recovering NEC Clusters

Disaster recovery in a Windows-based cluster environment is a complex task. Although CA 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 or Windows 2000 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

The following sections provide 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 CA ARCserve Backup as a CLUSTERPRO/ExpressCluster-aware application:

- Install CA 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 CA ARCserve Backup components on all nodes. You must configure each of these components in the same way.

- Use the same CA ARCserve Backup Device Group Name for the same devices in the CA ARCserve Backup configuration on each node of the cluster. To ensure this, use the default Device Group Names assigned by CA ARCserve Backup when you use Device Configuration.
- Use the same CA ARCserve Backup system accounts for all CA 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 CA 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 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.

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

The following sections provide 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.

CA ARCserve Backup Installed Outside NEC CLUSTERPRO/ExpressCluster SE Cluster

The following sections provide procedures to resolve cluster failures when CA 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:

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 CA 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. If the NEC StoragePathSavior 2.0 Standard for Windows 2000 (UFS202-0120) is used, see the section 2.5.5 X-Call Disk Settings in the NEC document *NEC ExpressCluster System Construction Guide/ Cluster Installation and Configuration Guide (Shared Disk)*.

   h. Reboot the server.

   i. Confirm that the drive letter is identical to the one you set in the previous step using the operating system's disk administrator.

   j. 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.

   k. 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

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.

CA ARCserve Backup Installed on the NEC CLUSTERPRO/ExpressCluster SE Cluster

Performing disaster recovery with CA 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 CA 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

The following sections provide the procedures to follow to recover your data if your shared disk fails.

Recover Data with CA ARCserve Backup Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disks

To recover the data residing on the shared disks, if the CA ARCserve Backup was installed on the shared disk, perform the following procedure:

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 CA 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. If the NEC StoragePathSavior 2.0 Standard for Windows 2000 (UFS202-0120) is used, see the section 2.5.5 X-Call Disk Settings in the NEC document *NEC ExpressCluster System Construction Guide/ Cluster Installation and Configuration Guide (Shared Disk)*.

   e. Reboot the server.

   f. From the NEC ExpressCluster Disk Administrator, verify that the cluster letters on the CLUSTER disk partition are the same as the original letters.

   g. 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 CA 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:

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 CA 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. If the NEC StoragePathSavior 2.0 Standard for Windows 2000 (UFS202-0120) is used, see the section 2.5.5 X-Call Disk Settings in the NEC document *NEC ExpressCluster System Construction Guide/ Cluster Installation and Configuration Guide (Shared Disk)*.

h. Reboot the server.

i. Confirm that the drive letter is identical to the one you set in the previous step using the operating system's disk administrator.

j. 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.

k. 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

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 the section Recover Data with CA ARCserve Backup Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disk in this document.
5. To recover all other cluster nodes one by one, perform the procedure provided in the section Recover One Failed NEC CLUSTERPRO/ExpressCluster SE Cluster Node in this document.

   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 the section Recover Data with CA ARCserve Backup Not Installed on NEC CLUSTERPRO/ExpressCluster SE Shared Disk in this document.

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 following scenarios 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.

CA ARCserve Backup Installed Outside NEC CLUSTERPRO/ExpressCluster LE Cluster

The following sections provide procedures to help you recover your data if CA 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:

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 CA 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:

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 CA 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. 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 provided in the following sections, depending upon whether CA ARCserve Backup is installed on the mirrored disk.

Recover Data with CA 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 CA 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 CA ARCserve Backup installation is restored.

   Note: See the special considerations in the section Active/Passive Configuration in this document.

4. From the Start menu, select Shut Down to reboot all servers.

CA ARCserve Backup Not Installed on Mirrored Disks

If any disk in a mirrored set becomes damaged, but the cluster nodes are undamaged, and CA ARCserve Backup is not installed on the mirrored disk, 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 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

To recover an entire cluster

1. To recover the primary node, perform the procedure provided in the section Recover Data with CA ARCserve Backup Installed on Mirrored Disk in this document.
2. To recover the secondary nodes, perform the procedure provided in the section Recover One Failed Cluster Node in Active/Passive Configuration in this document.
3. Return all nodes to the cluster. To do so, see the NEC documentation for more information.

Appendix D: Staging Using File System Devices

The Disaster Recovery Option integrates fully with the Disk Staging Option using file system devices. If you migrate backup data from one place to another 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

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 E: 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 CA ARCserve Backup StorageTek ACSLS Option
- You must have installed the StorageTek LibAttach Service
- The machine must be running on a supported Windows 2003 platform

This section contains the following topics:

Disaster Preparation

For a typical Windows 2003 disaster recovery operation, you must create or obtain the following media:

- Microsoft Windows 2003 CD. You must use the same version and edition you installed on your machine.
- The CA ARCserve Backup CD
- 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! CA has signed an agreement with STK that stipulates that you, as a CA 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

To perform disaster recovery of the local backup server using a StorageTek ACSLS library

1. Boot from the Microsoft Windows 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 CA ARCserve Backup CD and the machine-specific recovery disk.
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 F: 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)

CA ARCserve Backup Requirements

In addition to the CA ARCserve Backup base, the following options are required to back up Windows Small Business Server 2003 data correctly:

- CA ARCserve Backup Agent for Open Files for Windows
- Disaster Recovery Option
- CA 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 CA 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 CA 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. The following sections provide procedures to recover the databases.

For information about recovering Windows 2003 machines, see the section "Disaster Recovery on Windows 2003 and Windows XP" in this guide.

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 the following sections, see the appropriate CA 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.

The following sections provide information and procedures relating to each step in the process.

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:

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 the section Delete the Microsoft SharePoint Website and Uninstall Microsoft SharePoint in this guide 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 appears.

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:

1. Using the CA 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. Enter the appropriate information in the required fields and click OK.

4. 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 G: Restoring Data Using the DRScanSession Utility

The Disaster Recovery Option provides a special purpose utility, DRScanSession, that allows you to perform the following:

- Restore a system from a tape for which you do not have the latest disaster recovery machine specific disk.
- Specify the backup from which a system should be restored. It may be necessary to specify this information if, for example, you want to restore a system from a previous full backup, not the last full backup. Additionally, this feature can help if, for example, you have misplaced the latest disaster recovery information. You can use this utility to specifically select the latest session from a tape as the session to restore the system.

Note: We recommend that you use the DRScanSession Utility for local disaster recovery only.

To use the DRScanSession Utility, ensure that you have the following:

- A machine-specific recovery disk for the system you want to recover. It need not be the most recent one, but it should meet the following criteria:
  - The disk layout must be compatible in that, for each partition, the new volume should be larger than the old one.
  - The system configuration must be unchanged. For example, devices must not have been moved from one group to another and group names must be unchanged. In addition, no additional devices should be attached, and no new CA ARCserve Backup options added.

  Note: Disaster recovery information is updated each time you run a full backup.
- The tape and the tape session number of the disaster recovery session you want to restore.

Note: The Disaster Recovery DRScanSession Utility is supported for the Windows 2000 local disaster recovery process. It should not be used when recovering a system using the Bootable Tape method (OBDR).

For Windows XP and Windows Server 2003, you must use the Scan and Replace Session function from the Disaster Recovery Option.

This section contains the following topics:

DRScanSession and Windows 2000 Disaster Recovery

The following sections provide information about using the DRScanSession utility during the Windows 2000 disaster recovery process.

Prepare to Use the DRScanSession Utility

Before you start the DRScanSession Utility, perform the following steps:

1. Insert the tape containing the disaster recovery session you want to restore into the tape drive or changer.

   Have the CA ARCserve Backup CD ready so you can copy the DRScanSession.exe, DRESTORE.dll, and the DRScanSessionres.dll files from the \BOOTDISK directory.
2. Note the approximate date, time, or session number of the disaster recovery backup you want to restore and the name of the computer you want to restore.

3. Obtain the disaster recovery bootable disk for the computer you want to recover.
4. Prepare a blank disk. This disk becomes the new machine-specific recovery disk.

Use the DRScanSession Utility

To use the DRScanSession Utility

1. Start a normal disaster recovery of your system using the machine-specific recovery disk.
2. When the bluescreen mode finishes, the computer reboots to the Disaster Recovery Wizard. Press Ctrl+Shift and double-click the image in the Disaster Recovery Wizard to display the disaster recovery Command Prompt.
3. To change the %windir%\system32\DR directory, enter CD DR in the command line.
4. Copy the DRScanSession.exe and the DRESTORE.dll binary file and the DRScanSessionres.dll file from the \BOOTDISK directory on the CA ARCserve Backup CD to the disaster recovery directory.

   Note: See the section Prepare to Use the DRScanSession Utility in this chapter for more information about copying these files.
5. Run the DRScanSession Utility.
6. The DRScanSession Utility prompts you for the computer name and the machine-specific recovery disk. A message may appear, stating that the disk is not the correct one.

   To verify that the disk contains information corresponding to the correct computer, enter the following at the command prompt:

   ```
   dir a:
   ```

   where A is your diskette drive. The directory should contain the file [MachineName].drf.
7. The Tape Engine starts. This may take some time, especially if you have a changer.
8. A list of tape devices and changers attached to your computer appears, with the details of the tapes inside of them. Select the tape you want to use for disaster recovery. If you do not see the devices you expected, verify that the option's configuration was not changed after you created the recovery disks.

9. The system prompts you to enter the session number of the session you want to restore, or to scan the entire tape for all disaster recovery sessions.

   The quickest method is to enter the session number. However, if you do not know the session number, you must scan the tape. If you enter the session number, the system verifies that it is a disaster recovery session. If you scan the tape, a list of disaster recovery sessions found in the tape appears. Select a session from the list.

10. The option performs a temporary restore of the disaster recovery session. When prompted, insert a blank disk that will become the new machine-specific recovery disk. If you perform a disaster recovery using this disk, the selected session is restored.

Use DRScanSession for Remote Disaster Recovery

Use the DRScanSession utility to create a new machine-specific disk to perform remote disaster recovery on client machines to the point at which a full backup is available.

To create machine specific disk to perform remote disaster recovery on client machine

1. Log on to the CA ARCserve Backup server machine that contains the backup media.

2. Copy the DRScanSession.exe, DRESTORE.dll, and the DRScanSessionRes.dll files from the \BootDisk directory of the CA ARCserve Backup CD to the home directory of the CA ARCserve Backup installation.

3. Run the following command and follow the prompts on screen:

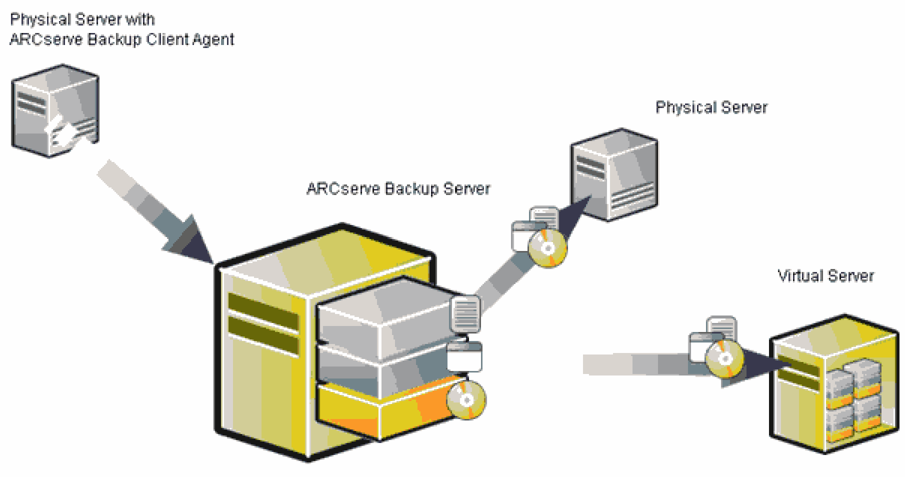
   ```
   Drscansession -noreg
   ```

Disaster Recovery Log File

If an error occurs, the DRScanSession Utility creates a DRSS.LOG file in the DR directory. Open this log file to view the error.

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 CA 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.

This section contains the following topics:

Prerequisites

You must have knowledge on CA ARCserve Backup Disaster Recovery Option, Microsoft ASR, network configuration utility netsh, and the usage of VMware ESX server.

Operating Systems

This feature is supported in the following operating systems:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows 2003
- Microsoft Windows XP Professional

Virtual Infrastructures

This feature is supported on VMware ESX Server 2.5 and higher virtual infrastructures from VMWare.

Software Requirements

The following information provides some information about the software requirements:

- CA ARCserve Backup Base r11.5 with SP3 or later versions
- CA ARCserve Backup Disaster Recovery Option
- CA 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. The following sections provide best practices for the following scenarios:

- Local Backup and Local Restore
- Remote Backup and Remote Restore
- Local Backup and Remote Restore

Note: CA 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.

Network Interface Card (NIC) is Nonfunctional after a Local Restore

The Network Interface Card (NIC) does not function properly when the system restarts after a local restore.

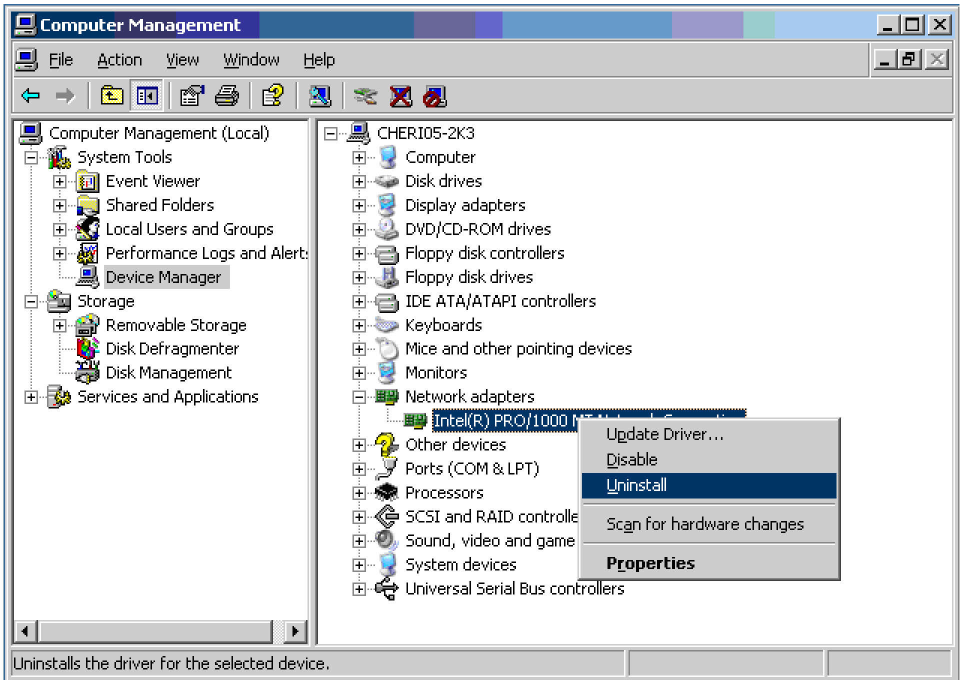
You can use one of the following solutions to solve this problem:

- 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:



Uninstalls the driver for the selected device.

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.

Unable to Establish a Connection with tape engine

The connection to the tape engine is not established when the Disaster Recovery restore begins. This issue is mostly encountered with a VMware ESX recovery.

To establish a connection with Tape Engine

1. Open command prompt from Restore Manager.
2. Execute the following command:

   ```
   ipconfig
   ```

   Note: You must configure the a new IP address when the available IP address is 169.254.159.XXX or there is no IP address assigned. CA 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

   ```
   C:\WINDOWS\system32\drivers\etc\hosts
   ```

   Microsoft Windows 2000

   ```
   C:\DRBOOT.TMP\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

   ```
   C:\WINDOWS\system32\DR
   ```

   Microsoft Windows 2000

   ```
   C:\DRBOOT.TMP\system32
   ```

   This establish 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.

See Network Interface Card (NIC) is Nonfunctional after a Local Restore (see page 159) for more information.

Local Backup and Remote Restore

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 Machine Specific Recovery Disk (MSD) floppy in Windows 2000:

1. Modify the following two files using registry edit tools :
   - **TEST-SERVER.DRF**

     Modify the record DRLOCALCOMPUTERNAME from TEST-SERVER to TEST-SERVER-REP.

     Note: CA ARCserve Backup server names and CA ARCserve Backup domain names cannot exceed 15 bytes. A name totaling 15 bytes equates to approximately 7 to 15 characters.
   - **w2ktcpip_drf**

     Modify the record IP address from 192.168.1.224 to 192.168.1.226. For more information on how to modify files see Modify a Registry File (see page 166).
2. Rename the following files:
   - TEST-SERVER_CA to TEST-SERVER-**REP**_CA
   - TEST-SERVER.DRF to TEST-SERVER-**REP.**DRF
   - TEST-SERVER_DLST to TEST-SERVER-**REP**_DLST
   - TEST-SERVER_DTBL to TEST-SERVER-**REP**_DTBL
   - TEST-SERVER_PRDS to TEST-SERVER-**REP**_PRD
3. Add an empty file BABDRE115.
4. Add a file w2karmt.dmp by following the steps given below:

   a. Copy the following file in the CA ARCserve Backup installation CD to the CA ARCserve Backup home directory on your machine.

   ```
   \Utilities\IntelNT\DRO\ENU\makermt.exe
   ```

b. Open the command prompt and go to the CA ARCserve Backup home directory and execute the following command:

```
makermt -BAB11_5 -alter -file w2karmt.dmp
```

c. You are prompted to input the server name, domain name, user name and the password. In this case enter TEST-SERVER for both server name and domain name. The w2karmt.dmp file is generated in the current directory.

d. Copy this file to the MSD floppy. Use this floppy and the bootable CD to restore the local backup data to the remote virtual machine.

To modify the MSD floppy for Window XP and Windows 2003

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.

To modify the MSD floppy in Windows 2000

1. Modify the **TEST-SERVER.DRF** file using registry edit tools.

   You can modify the record DRCOMPUTERNAME from **TEST-SERVER** to **DR-SERVER**.

   For more information on how to modify files, see Modify a Registry File (see page 166).
2. Add an empty file BABDRE115.

3. Add **w2karmt.dmp** file using the following steps:

   a. Copy the following file in the CA ARCserve Backup installation CD to the CA ARCserve Backup home directory on your machine.

   ```
   \Utilities\IntelNT\DRO\ENU\makermt.exe
   ```

   b. Open command prompt and go to the CA ARCserve Backup home directory and execute the following command:

   ```
   makermt -BAB11_5 -alter -file w2karmt.dmp
   ```

   c. Enter the server name, domain name, user name and the password. For this scenario, enter DR-SERVER for both server name and domain name. The **w2karmt.dmp** file is generated in the current directory.

   d. Copy this file to the MSD floppy. Use this floppy and the bootable CD to restore the local backup data to the remote virtual machine.

To modify the MSD floppy for Windows XP/Windows 2003

1. Modify the following 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

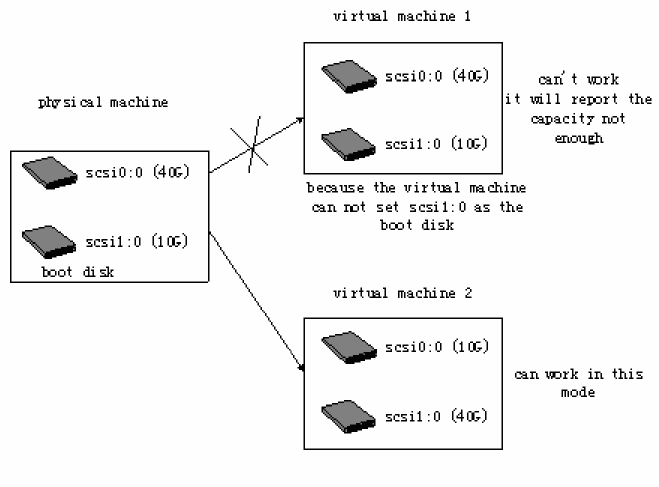
Unable to Load the SCSI Disk

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:



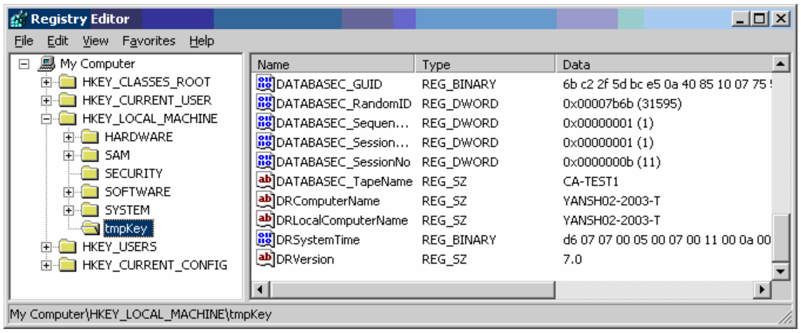
Note: Check with the specification of each disk.

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:



Name	Type	Data
DATABASEC_GUID	REG_BINARY	6b c2 2f 5d bc e5 0a 40 85 10 07 75 !
DATABASEC_RandomID	REG_DWORD	0x00007b6b (31595)
DATABASEC_Sequen...	REG_DWORD	0x00000001 (1)
DATABASEC_Session...	REG_DWORD	0x00000001 (1)
DATABASEC_SessionNo	REG_DWORD	0x0000000b (11)
DATABASEC_TapeName	REG_SZ	CA-TEST1
DRComputerName	REG_SZ	YANSH02-2003-T
DRLocalComputerName	REG_SZ	YANSH02-2003-T
DRSystemTime	REG_BINARY	d6 07 07 00 05 00 07 00 11 00 0a 00
DRVersion	REG_SZ	7.0

My Computer\HKEY_LOCAL_MACHINE\tmpKey

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 CA 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

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.

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.

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.
6. The Windows Settings dialog appears.
7. Select Remote Installation Service.
8. Double-click Choice Options from the right panel.

   The Choice Options property page appears.
9. Select the options as follows:

   Automatic Setup - Disabled

   Custom Setup - Disabled

   Restart Setup - Disabled

   Tools - Enabled
10. 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

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.

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:

- Change the following key-value pair:

  ```
  ImageType= Flat
  ```

  to

  ```
  ImageType = ASR
  ```

- 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.

- 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 CA 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 CA 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 CA ARCserve Backup Server on which Disaster Recovery Option is installed. You can find the BAB_HOME\drpatch.xp on the CA 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:

1. **Copy DR emergency data to OS image directory:** Locate the DR directory in the home directory of the CA 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 CA 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 IA64:

      ```
      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 IA64>%systemdrive%\dr_asr.log"

5=1,4000,1,"%SystemRoot%\syswow64\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 CA 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, and click Enter on keyboard.
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.Click C on your keyboard.
7. Wait for the CA ARCserve Backup Disaster Recovery wizard to appear. Once the wizard appears, the recovery proceeds.

Appendix J: 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

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

All Windows Platforms

The following information applies to all supported Windows platforms.

Error Messages Appear in the Windows Event Log that Relate to the ARCserve Database

Valid on Windows Server 2003 platforms.

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 CA ARCserve Backup for Windows.

System Configurations to Avoid

Symptom:

What system configurations should I avoid for disaster recovery?

Solution:

You should avoid the following configurations:

Windows 2000, 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.

Windows 2000 Disaster Recovery Methods

Symptom:

There are a number of methods of disaster recovery in Windows 2000. Which one do I use?

Solution:

We recommend using the bootable CD method to perform disaster recovery on a Windows 2000 computer. For more information, see the section Bootable CD Method in the "Disaster Recovery on Windows 2000" chapter of this guide.

Restore of Incremental and Differential Restores

Symptom:

I have backed up the CA 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:

Windows 2000, Windows 2003, and Windows XP

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.

Local DR using Remote FSD

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 2000, Windows 2003, and Windows XP

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.

Perform Incremental and Differential Backup

Valid on Windows 2000, 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.

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 CA 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 2000:

On the machine-specific recovery disk for client computers, the file labeled w2karmt.dmp contains the name of the CA ARCserve Backup server to which the disaster recovery process must connect for data restoration. By default, this is the server backing up the client computer. To restore from a different server, use the makermt utility found on the CA ARCserve Backup CD to create a new w2karmt.dmp file. Add this new file to the machine-specific recovery disk and start the disaster recovery process.

Note: In 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 CA 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 a Windows XP or Windows 2003 operating system, 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. Do not use the Disaster Recovery Wizard to create or delete 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 CA 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
```

Boot Disk Creation

Symptom:

The option is asking for the Windows 2000 boot disk. Where do I get these?

Solution:

Use one of the following methods to obtain the necessary boot disks:

Windows 2000:

Use the DISKCOPY command and copy your original Windows 2000 boot disks to a new set of three disks for the option to modify.

Windows 2000:

Run makebt32.exe in the BootDisk folder of your Windows 2000 installation CD.

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 CA 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.

Recovery with Different Sessions

Symptom:

I do not want to restore the last full backup sessions for a local disaster recovery in Windows 2000. What can I do?

Solution:

Use the DRScanSession utility to modify the machine-specific recovery disk, and perform a disaster recovery. See the appendix DRScanSession Utility for more information.

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 XP or 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-Enlgish 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 CA ARCserve Backup server?

Solution:

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

Hardware

The following section provides answers to frequently asked questions related to hardware.

Windows 2000, Windows 2003, and Windows XP

The following information applies to Windows 2000, 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
```

Operating Systems

The following section provides answers to frequently asked questions related to operating systems.

All Windows Platforms

The following information 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 2000:

Always choose the first partition, typically C.

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 2000:

To open a command prompt during the disaster recovery mode, press and hold Ctrl+Shift while double-clicking the image on the Disaster Recovery wizard dialog.

Windows XP and Windows 2003:

To open a command prompt, in the Advanced Disaster Recovery GUI, click Troubleshooting and click Command Line Console option.

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 protocal 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 2000**

     The network configuration file is named “w2ktcpip_drf”, it is available on MSD floppy. You can use DRNetConfig.exe utility to modify MAC address of specified network adapter. This utility is available in the CA ARCserve Backup installation CD/DVD, in Utilities directory.

   - **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 CA 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 CA ARCserve Backup server user name or password since the last full backup.

   b. Verify the Windows workstation and server services are running on the CA 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 CA 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 XP or 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

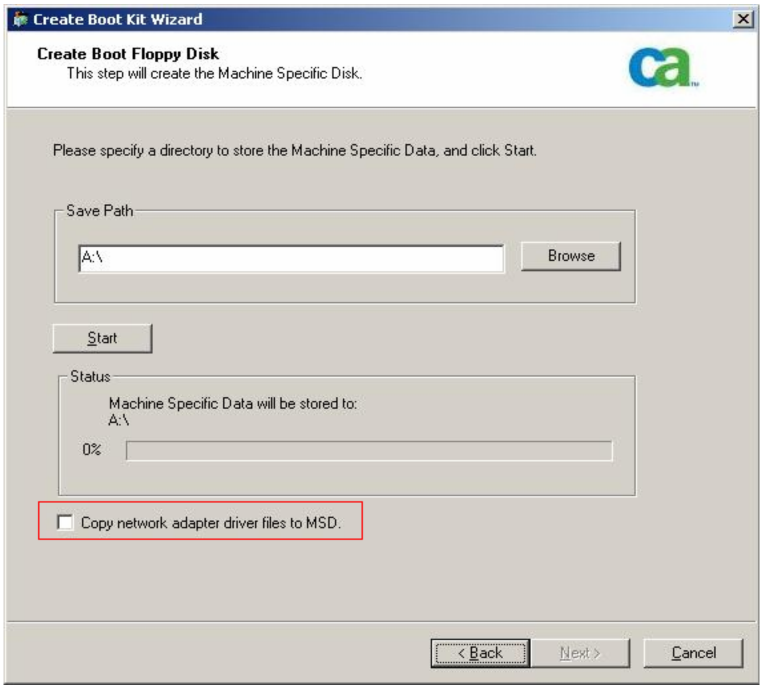
Symptom:

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:



Create Boot Kit Wizard

Create Boot Floppy Disk

This step will create the Machine Specific Disk.

Please specify a directory to store the Machine Specific Data, and click Start.

Save Path: A:\

Status

Machine Specific Data will be stored to:
A:\

0%

□ Copy network adapter driver files to MSD.

Server Admin error when creating MSD using Floppy Disk

Valid on Windows Server 2008 (x64/IA64)

Symptom:

When creating Machine Specific Disk for 64-bit (x64/IA64) 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.

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 CA 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 CA ARCserve Backup CD 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 2000

Symptom:

When recovering a Windows 2000 machine, I received errors such as "Failed to restore file…" toward the end of the restore process. I checked my system volume (C:) and noticed that the system volume is running out of free space. Why?

Solution:

For Windows 2000 disaster recovery, the process first installs a temporary working operating system and then restores the files from the backup media. The size of the temporary working operating system is approximately 300 MB. This temporary operating system can, potentially, take away the disk space needed for file restoration. To avoid the problem, ensure that the C drive always has at least 300 MB of free space available during the backup.

Windows 2000 Disaster Recovery Operating Systems FAQs

The following information applies only to Windows 2000 platforms.

Cannot See Original Partitions

Symptom:

During a CD-based disaster recovery, I did not see the original partition recreated while in the bluescreen mode. Why?

Solution:

If you add any drivers during the bluescreen mode of the disaster recovery process by pressing F6, you must put the disaster recovery machine-specific recovery disk back in the drive after the last driver is added. Disaster recovery reads the original disk configuration from the machine-specific recovery disk; if it is not in the drive, disaster recovery cannot recreate the original disk configuration.

The following procedure outlines the steps to take to add drivers:

1. Press F6 to add extra drivers.
2. Insert the manufacturer's driver disk when prompted.
3. Select the installed devices.
4. Repeat the preceding steps as necessary for additional drivers.
5. You are prompted to press Enter to continue Windows setup. Remove any disk in the drive and insert the disaster recovery disk before you press Enter.

Cannot Boot From Bootable CD

Symptom:

After creating the bootable CD image for a Windows 2000 disaster recovery, the computer to be recovered could not boot from the bootable CD. Why?

Solution:

The following are some common causes for this problem:

- The CD drive is not bootable.
- The CD media itself is corrupted.
- The system boots from the hard drive or diskette drive first. If this happens, you must change the boot order.
- The disaster recovery bootable CD image file**,** cdboot.iso, was copied improperly onto the CD media. Use CD copying software to expand the image and replicate that image onto a blank CD as the bootable CD image. Do not try to merely copy the image file onto a blank CD.

File Overwriting

Symptom:

In the Disaster Recovery Wizard mode, I see a Confirm File Replace prompt with the message “The target file exists and is newer than the source. Overwrite the newer file?” Should I choose Yes or No?

Solution:

You should **not** overwrite the newer file. Select No.

Utilities

The following section provides answers to frequently asked questions related to utilities.

DRScanSession Utility

Symptom:

What does the DRScanSession utility do? Where do I use it?

Solution:

The DRScanSession utility is supported on Windows 2000.

The MACHINENAME.DRF file on the machine-specific recovery disk contains information about the backup sessions that comprise the latest full backup of the computer. The DRScanSession utility allows you to specify the disaster recovery backup from which the system should be restored, rather than using the last full backup by default.

The DRScanSession utility scans inserted tapes to find a disaster recovery backup session from which to restore. The DRScanSession utility can only be used in the disaster recovery environment and only works when performing a local disaster recovery. The utility is in the utilities directory of the CA ARCserve Backup CD.

Note: For more information about the DRScanSession utility, see the appendix "Restoring Data Using the DRScanSession Utility" in this guide.

Symptom:

How do I use the tapetest utility to diagnose common local disaster recovery problems?

Solution:

The tapetest utility is supported on Windows 2000.

To use the tapetest utility, open the DOS prompt console and change the disaster recovery directory and run the tapetest utility.

The following are useful functions of the tapetest utility:

- To display a list of devices on the screen, to determine the devices to use with other tapetest options, or to identify the devices that CA ARCserve Backup detects are attached to the computer, enter the following at the prompt:

  ```
  tapetest –y
  ```

- To test that CA ARCserve Backup can successfully communicate with a device, enter the following:

  ```
  tapetest -d# -ping
  ```

  where d# is the device number.

- To send a list of all media available on the CA ARCserve Backup servers specified in the infile, to the outfile, enter the following:

  ```
  tapetest -mediainfo infile outfile
  ```

- To display information on the media in any attached tape drives (standalone tape drives only) on the screen, enter the following:

  ```
  tapetest -ym
  ```

Applications

The following 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*.