BrightStor® ARCserve® Backup for UNIX and Linux

Disaster Recovery Option Guide

r11.1

Computer Associates®

C00610-1E

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2004 Computer Associates International, Inc.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

Chapter 1: Introducing the Option

Understanding the Option 1-2
Distinctive Features 1-2
Functionality 1-3
Disaster Recovery Methods 1-3

Chapter 2: Installing the Option

Prerequisites 2-1
Installation Checklist 2-1
Installing the Option 2-2
Alternate Location for Disaster Recovery Information 2-2

Chapter 3: Preparing for Disaster

Creating a Disaster Recovery Plan 3-1
Preparing for Disaster on Linux 3-2
Preparing for Disaster on Sun Solaris 3-2
- Floppy-Based Method 3-3
- Tape Method 3-3
- Creating Emergency Data Disks 3-3
- Storing Disaster Recovery Information on a Remote Server 3-4
- Verifying Disaster Recovery Information 3-4

Chapter 4: Recovering Linux Systems

Restoring Data 4-1
- Automatic Data Restoration 4-2
- Interactive Data Restoration 4-2

Recovery Options 4-3
Disaster Recovery 4-3
Special Considerations for Database Restores 4-5
Troubleshooting 4-5

Chapter 5: Recovering Sun Solaris Systems

Restoring Data 5-1
Automatic Data Restoration 5-2
Interactive Data Restoration 5-2
Recovering from a Disaster 5-3
Using the Floppy-Based Method 5-3
Using the Tape Method 5-4
Special Considerations for Database Restores 5-5

Chapter 1

Introducing the Option

BrightStor® 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.

Among the options BrightStor ARCserve Backup offers is the BrightStor® ARCserve® Backup Disaster Recovery Option. This option allows you to protect the data on your Linux and Sun Solaris servers from disaster, and to restore your data after a disaster occurs.

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 fails, only one thing matters—time. Each tick of the clock means business lost, opportunities squandered, efforts wasted. You need to get your system back online quickly, accurately, and safely. The BrightStor ARCserve Backup Disaster Recovery Option does this for you.

The option allows you to quickly and easily restore a Sun Solaris or Linux server without requiring you to reinstall the operating system. In addition, there are many time-consuming tasks—including installing the base operating systems and setting up the server—that would usually have to be manually performed after a disaster. The option enables you to restore your server with minimal effort and reliable recovery. It lets you make more efficient use of time by taking you from boot media, to backup media, to online, faster than other solutions. The option enables users with minimal server configuration experience to recover sophisticated configurations.

Understanding the Option

Disaster recovery works by collecting and saving machine-specific information before a disaster strikes. Whenever a full backup job is submitted, BrightStor ARCserve Backup automatically generates and saves emergency data information for the server locally, on the backup server, on backup media, and, if configured on Sun Solaris systems only, on a remote computer. If disaster strikes, the BrightStor ARCserve Backup Disaster Recovery Option can recover the server to the last full backup state. Recovery depends on the availability of emergency data and a full backup.

Note: The option generates or updates emergency data information for disaster recovery only when performing a full backup of the server.

Using a bootstrap recovery process, the option takes you from floppy disk or CD, to tape, to an operational state, quickly and reliably. By booting from the boot media and following a simple, user-friendly interface, even novice users can have their servers back online in record time.

The option is a complete solution to recover Sun Solaris and Linux servers after disasters. Typically, everything is accomplished by a hands-off procedure, although, for more complex scenarios, user involvement may be required.

Distinctive Features

The BrightStor ARCserve Backup Disaster Recovery Option is a flexible, easy-to-use, enterprise-wide solution to protect your data on Sun Solaris and Linux computers. The option provides you with the following features:

- Protects your local BrightStor ARCserve Backup server.
- Allows you to put an unusable system back online quickly, saving you substantial time compared to recovering your system by reinstalling and reconfiguring the operating system. Using the option, there is no need to reconfigure the system before it is usable.
- Works with minimal user input and can support any system that BrightStor ARCserve Backup supports. The option both protects the server on which BrightStor ARCserve Backup and other important applications are running and, after a disaster, effectively restores the server if the recommended measures were performed before the disaster occurred.

Functionality

The BrightStor ARCserve Backup Disaster Recovery Option works with regular tape backups. On Sun Solaris computers, you can recreate hard disk slices and file systems, scan sessions, and perform restores. On Linux computers, wizards help create recovery boot disks, partition and format hard drives, scan sessions, and begin restores.

The option supports:

- Multiple sessions and spanned tapes
- Multiple tape drives and host adapter
- Use of tape drives in autochangers
- Floppy-based recovery on Linux and floppy-based and tape-based recovery on Sun Solaris
- Multiplexed backup sessions
- Triple DES3 encrypted sessions

The option can only restore full sessions; individual files cannot be restored.

Disaster Recovery Methods

The most critical information required to recreate your system after a disaster is the disaster recovery information generated each time you run a full backup. The option provides different approaches to access the data to be used for disaster recovery, based on platform.

On Sun Solaris, the option provides the following methods:

- **Floppy-based method**—Use this method if the BrightStor ARCserve Backup server to be recovered has a floppy disk drive and you have emergency disks. The emergency disks must be created before the disaster or, if an alternate location has been configured to store disaster recovery information, you can log in to the alternate location after the disaster to create an emergency disk.

- **Tape**—Use this method if you do not have emergency disks or a floppy drive. To use the tape-based method to perform recovery, you must configure an alternate location in which to store disaster recovery information. The information generated in the alternate location provides the necessary disaster recovery information on the tape.

On Linux, the option provides one method, the floppy-based method, to store emergency data to be used in the event of a disaster. Use this method if the BrightStor ARCserve Backup server to be recovered has a floppy disk drive and you have emergency disks. Emergency disks must be created before the disaster.

Chapter 2

Installing the Option

This chapter discusses information you must have available when you install the option and information to help you fine-tune the option after it is installed.

Prerequisites

Verify that you have installed, or will be installing, the BrightStor ARCserve Backup server and manager packages before you install the option. The option has no other prerequisites.

Before installing the BrightStor ARCserve Backup Disaster Recovery Option, verify that you have root user privileges or the proper authority to install software on the servers where you plan to install the BrightStor ARCserve Backup Disaster Recovery Option.

Note: Contact your BrightStor ARCserve Backup administrator to obtain the proper rights if you do not have them.

Installation Checklist

Use the following checklist to ensure that you have met all of the prerequisites and have all of the information that you need to complete the installation.

✓	Prerequisites
	Verify that your system meets the minimum requirements to install the option. For a list of system requirements, see the readme file.
	Verify that you have root user privileges or the proper authority to install software on the server on which you are installing the option.
	On Linux, verify that you have a functional floppy drive and bootable CD-ROM.

Installing the Option

You must install BrightStor ARCserve Backup server and manager packages for UNIX and Linux before you install the option.

You can install the option during or after the installation of the BrightStor ARCserve Backup base product. During the installation, you are presented with a list of available packages.

To install the BrightStor ARCserve Backup Disaster Recovery Option, perform the following procedure:

1. Log on to the BrightStor ARCserve Backup server. You must have root user privileges to install the option.
2. From the command line, enter the following command to start the installation script:

   ```
   # ./install
   ```

   or

   ```
   path/install
   ```

   where *path* is the location of the installation script.
3. Respond to all prompts as appropriate for your system configuration.

For the complete installation procedure, see the *BrightStor ARCserve Backup for UNIX and Linux Getting Started* guide.

Select the BrightStor ARCserve Backup Disaster Recovery Option from the component list when you are prompted to select the components you want to install. The option is automatically installed in the $BAB_HOME directory. No additional installation steps are required to install the option.

Alternate Location for Disaster Recovery Information

During configuration of the option on Sun Solaris servers, you are asked if you want to configure an alternate location in which to save disaster recovery information.

When you back up a BrightStor ARCserve Backup client computer with the option installed, the computer-specific information required to perform disaster recovery tasks is saved on the BrightStor ARCserve Backup server.

If the BrightStor ARCserve Backup server fails, computer-specific disaster recovery information can also be lost. To avoid this type of data loss on Sun Solaris servers, we recommend that you configure an alternate location for disaster recovery information. If the server fails, you can access the alternate location to obtain the information you need in the event of a disaster.

You can configure this feature while configuring the option after installation or at a later time, by running the csetup command. For more information about configuring an alternate location for disaster recovery information, see the section Storing Disaster Recovery Information on a Remote Server in the "Preparing for Disaster" chapter of this guide.

Chapter 3

Preparing for Disaster

The most important thing you can do to guard against data loss is to maintain current backups of all your servers and workstations. If you do not maintain regular backups, BrightStor ARCserve Backup is limited in its ability to recover your data after a disaster. Be sure to create a media rotation policy and a schedule to maintain current full backups.

If disaster does strike, the BrightStor ARCserve Backup Disaster Recovery Option provides you with the ability to recover your system quickly, efficiently, and completely. The option restores your system to its state at the time of the last backup and allows you to avoid fully reinstalling and reconfiguring your operating system and other installed software packages.

We strongly recommend that you perform regular full backups of your system, and keep the information about the media containing the last full backup in a convenient location for easy access in the event of a disaster.

Creating a Disaster Recovery Plan

Disaster recovery is a two-step process: preparation and recovering. As part of your disaster recovery preparations, you should develop a Disaster Recovery plan and create a set of disaster preparation materials to be kept off site. Be sure you know where these disaster preparation materials are located. Follow the instructions in this guide to create the disaster preparation materials you need.

To test your plan, perform the following steps:

1. Set up a test server with a similar configuration to your original server.
2. Simulate a recovery on your test server by following the instructions in the chapter of this guide that applies to your operating system.

Preparing for Disaster on Linux

You can protect your Linux server from potential disaster and bring it back online quickly by having all necessary disaster recovery components, an emergency disk, a full backup, and the BrightStor ARCserve Backup Disaster Recovery bootable CD, available.

Note: The BrightStor ARCserve Backup Disaster Recovery Option CD image can be downloaded from the Computer Associates Technical Support web site and burned to a blank CD, using CD creation software, to create the bootable CD.

Ensure that the BrightStor ARCserve Backup Disaster Recovery Option is installed on the BrightStor ARCserve Backup server that is to be protected from disaster. On Linux systems, the option is installed in the $BAB_HOME/DR/ directory. To protect your BrightStor ARCserve Backup server, you must back up the entire computer. To prepare for a disaster, perform the following steps:

1. Run the installation script and install the BrightStor ARCserve Backup Disaster Recovery Option.
2. Back up the entire node on the computer on which the BrightStor ARCserve Backup Disaster Recovery Option is installed.

   Your computer must be able to boot from the IDE or SCSI CD-ROM.
3. Run DRmkdisk from the $BAB_HOME/DR/ directory. This script copies emergency data specific to your computer to a disk, which is required during the recovery process. One disk can hold emergency data for several systems.

   Note: You must update this disk whenever the computer hardware configuration changes.

   Important! *If you keep emergency data for several systems on the same disk, do not format the disk.*

   Tip: It is a good practice to run this script every time you run a full backup to update the tape name and session information for the backup on the emergency disk.

Preparing for Disaster on Sun Solaris

You can protect your local Sun Solaris computer from a potential disaster by creating emergency disks or storing emergency data information remotely. If you have configured an alternate location in which to store disaster recovery information, you can create emergency disks at any time, even after the workstation has failed.

Note: You should provide an alternate location for storing emergency data so that emergency disks can be created even after a BrightStor ARCserve Backup server has crashed.

Ensure that the BrightStor ARCserve Backup Disaster Recovery Option is installed on the BrightStor ARCserve Backup server to be protected. To protect your BrightStor ARCserve Backup server, you must back up the entire computer.

Floppy-Based Method

This method uses two emergency disks containing configuration information for a specific computer. This method allows you to recover a particular server, even one with an unformatted hard drive, and fully restore the system using the latest backup tape. The Sun Solaris installation CD-ROM is required during the recovery process.

Tape Method

This method uses a BrightStor ARCserve Backup tape containing the emergency data required to restore the server. It lets you recover any server, even one with an unformatted hard drive, and fully restores the system using the latest backup tape. The Sun Solaris installation CD-ROM is required during the recovery process.

Note: When using this method, you must configure an alternate server to store emergency data.

Creating Emergency Data Disks

To prepare emergency data disks to be used with floppy-based media, perform the following steps:

1. Back up the entire node on the computer on which the BrightStor ARCserve Backup Disaster Recovery Option is installed.
2. Run DRmkdisk from the $BAB_HOME/DR/ directory. This script copies the emergency data specific to your computer to the disks required during recovery. You must update these disks whenever your computer hardware configuration changes.

   Tip: It is a good practice to run this script every time you run a full backup to update the tape name and session information for the last full backup on the emergency disks.

Storing Disaster Recovery Information on a Remote Server

You should configure a remote Sun Solaris server to store the emergency data required to perform disaster recovery. When you perform a backup of the BrightStor ARCserve Backup server on which the BrightStor ARCserve Backup Disaster Recovery Option is installed, the machine-specific information is created locally, on a remote computer, and on the tape.

If the BrightStor ARCserve Backup server fails, this remote computer can be used either to create an emergency disk (for the floppy-based method) or to collect the tape name and session information (for the tape method).

Note: We strongly recommend that you provide an alternate location for disaster recovery information on Sun Solaris computers.

To store the emergency data information on a remote server, perform the following steps:

1. On a remote Sun Solaris computer, ensure that you have a share directory with read and write permissions for the root (superuser) of the computer on which BrightStor ARCserve Backup is running.

   For example, if the remote computer containing emergency data is SUNHOST and BrightStor ARCserve Backup is running on BRIGHTSTORDR, execute the following command on SUNHOST:

   ```
   #share -orw,root=BRIGHTSTORDR /space
   ```

   Note: Only the superuser of SUNHOST can create this share. An entry for BRIGHTSTORDR might need to be created in /etc/hosts on SUNHOST. Ensure that nfsd and mountd are running.

2. Set the NFS directory to be used to store emergency data remotely using one of the following methods:

   - Run csetup
   - Run $BAB_HOME/DR/cadro_setup

Verifying Disaster Recovery Information

On Sun Solaris systems, you can use the DRcheck utility to verify that all of the data created during your disaster recovery process is correct. Run the DRcheck script after a full backup of your local server. The script verifies the following information:

1. Confirms that all disaster recovery-related files have been created and contain data.
2. Checks the local system's mounted file systems and verifies that an entry exists for each file system, according to the disaster recovery information.

3. Checks whether Remote (NFS) files have been created. If they have been created, the utility checks that they are identical to the local files tested in the previous two checks.

If the utility detects any problems, it generates a message in the console, identifying the problem.

Chapter 4

Recovering Linux Systems

Before you begin recovering your server after a disaster, make sure that you have the following items available:

- A tape set containing the last known good backup of the entire node for the failed system
- BrightStor ARCserve Backup Disaster Recovery bootable CD
- BrightStor ARCserve Backup emergency disk for the failed system

Restoring Data

When you back up an entire node of the BrightStor ARCserve Backup server on which the option is installed, session information for all file systems that have been backed up is stored as part of the emergency data. The following information is collected and displayed for each file system you backed up:

- File system name
- Tape name
- Tape random ID
- Beginning and ending tape sequence number
- Session number
- Beginning and ending slot number and beginning and ending bar code number (if applicable)

This information is displayed during the disaster recovery process before the actual restoration of data begins. We recommend that you use this information to recover the system automatically, using **Automatic Recovery Mode**. Alternatively, you can perform a custom recovery and select the file systems to restore and the location to which to restore them. This recovery method is called **Interactive Recovery Mode**.

Automatic Data Restoration

When using the Automatic Recovery Mode to restore your data automatically, all file systems are restored using the information recorded during the last full backup. Before starting the restore process, you must provide all the media needed to perform a recovery. If all the media are found, the recovery proceeds automatically. If any media are missing, you must either provide the media or change to the Interactive Recovery Mode.

The main advantage of the Automatic Recovery Mode method is that it does not require any user input, other than loading a spanned sequence in the tape drive or supplying a password when an encrypted session is recovered.

Note: Automatic Recovery Mode is the recommended method.

Interactive Data Restoration

When using the Interactive Recovery Mode to restore data, you must confirm the restoration of each file system before the option can restore it. In addition, you must perform the following actions for each file system:

- Choose a tape device from the list of available devices.
- Provide media and confirm its use.
- Provide a session number from which to restore the file system. You can scan the tape to determine which file systems were backed up on the tape, and then provide the session number.

The advantage of this method is that you have control over the file systems to be restored and the media to use.

Recovery Options

During the recovery process you are presented with the following options:

- **Interactive**: Fully Interactive: You are prompted with the results of the restore process at different stages during recovery. If something is incorrect (for example, the emergency disk is not in the floppy disk drive) you can take corrective action. This option is enabled by default.
- **Manual Part**: Change Partition Size: If you restore data with a larger hard disk than was used for the backup operation, you can expand the partition size. Only advanced Linux systems administrators should use this option.
- **Bad Block:** Bad Block Testing: Produces a report documenting the results of performing a bad block test on your hard disks.

  Note: This option can be time consuming.
- **Verbose**: This option enables the generation of detailed messages.

Disaster Recovery

If disaster strikes your Linux system, use the following procedures to perform a disaster recovery operation:

1. Ensure that the tape device is properly connected and turned on. Turn on the computer.
2. Insert the bootable BrightStor ARCserve Backup disaster recovery CD.

   Note: If you receive a Bus Error during this step, the disaster recovery CD may not have been burned correctly. Recreate the image and start the procedure again.
3. At the boot prompt, press Enter.
4. Enter DRstart to start the disaster recovery process. The help dialog opens.

   Note: If no tape devices are found during this step, perform the following:

   - If the SCSI card driver was not loaded during boot up time, execute modprobe.
   - If the SCSI devices were powered on after the Linux machine was started, execute the DRscanscsibus utility to probe and provide information to the system.
   - If the SCSI connection failed, check the SCSI card and tape drive connections.

5. Follow the prompts until you are asked to insert the emergency disk. This disk reads system-specific data and creates an infrastructure for restoring your system.

   The session information from the last successful full backup of this computer appears.

6. When prompted, choose either the Automatic Recovery Mode or the Interactive Recovery Mode for the recovery process.

   - The Automatic Recovery Mode does not require user interaction except when backed up sessions are protected by passwords. If the full backup session is password protected, enter the session password to continue the recovery. Data is read from the tape and restored to your system.
   - In the Interactive Recovery Mode, you are prompted to insert the specific tape and verify the tape name, sequence, and random ID for every session you backed up.
   - If you are recovering a system using a multiplexed backup that spans multiple tapes, you are prompted to insert the highest sequence tape into the tape device to allow the device to read necessary information before recovering any of the sessions.

   Note: In Automatic Recovery Mode, you are prompted to ensure that all tapes are in the tape devices. If the necessary tapes are not in the tape devices, the recovery mode changes to the Interactive Recovery Mode, even if you have specified the Automatic Recovery Mode.

   If you have multiple devices, you are prompted to choose a device to recover the current session.

7. Disaster recovery, by default, restores your system from the tape session number recorded when the emergency disk was created. The default session number is the session number at the start of the last full backup of the system. To restore the system from another full backup, enter the beginning session number for that backup directly. Alternatively, you can scan the tape to determine the session number to specify.

8. If the full backup session is protected by a password, enter the session password to continue the recovery. Data is read from the tape and restored to your system.

9. Follow the prompts until the process ends.

10. Restart your computer.

11. After you restart your computer, execute the DRingres command to recover the Advantage™ Ingres® database.

Your BrightStor ARCserve Backup server has been recovered.

Special Considerations for Database Restores

BrightStor ARCserve Backup has special agents available to back up databases. These agents are:

- BrightStor® ARCserve® Backup for Linux Agent for Oracle
- BrightStor® ARCserve® Backup for Linux Agent for Apache Web Server
- BrightStor® ARCserve® Backup for Linux Agent for MySQL
- BrightStor® ARCserve® Backup for Linux Agent for Advantage Ingres

If you have backed up any of these databases using BrightStor ARCserve Backup, you cannot restore the database using the BrightStor ARCserve Backup Disaster Recovery Option. After you have restored the server using the BrightStor ARCserve Backup Disaster Recovery Option, you can start BrightStor ARCserve Backup and restore your databases using a typical database recovery procedure.

Troubleshooting

The BrightStor ARCserve Backup Disaster Recovery Option includes the following utilities to provide additional information if you encounter problems:

- **DRtrace**: This utility creates a log file with all the necessary information for debugging, if an error occurs. This log file can be sent to Computer Associates to assist in diagnosing the problem.
- **DRrescanscsibus**: This utility scans attached SCSI devices that have not been detected during system boot (for example, if the device was powered off) and provides this information to the system kernel.

Chapter 5

Recovering Sun Solaris Systems

Before you begin recovering your server after a disaster, ensure that you have the following items available:

- Tape containing the last known backup of the entire node for the crashed system.
- If you are using the floppy-based method, you must have two BrightStor ARCserve Backup emergency disks for the failed system. If you had previously configured emergency data to be stored in an alternate location and you do not have the emergency disks, or if they have not been updated, you can run DRmkdisk on the alternate location computer to create the disks.
- If you are using the tape method, you must have access to disaster recovery information stored in an alternate location.
- Sun Solaris installation CD-ROM.

  Note: Be sure the version is the same as the version that was previously installed.

Restoring Data

When you back up an entire node of the BrightStor ARCserve Backup server on which the option is installed, session information for all of the file systems that are backed up is stored as part of the emergency data. The following information is collected and displayed for each file system that was backed up:

- File system name
- Tape name
- Tape random ID
- Beginning and ending tape sequence number
- Session number
- Beginning and ending slot number and beginning and ending bar code number (if applicable)

This information is displayed during the disaster recovery process before the actual restoration of data begins. We recommend that you use this information to recover the system automatically, using **Automatic Recovery Mode**. Alternatively, you can perform a custom recovery and select the file systems to restore and where to restore them from. This recovery method is called **Interactive Recovery Mode**.

Automatic Data Restoration

When using the Automatic Recovery Mode to restore your data automatically, all file systems are restored using the information recorded during the last full backup. Before starting the restore process, you must provide all the media needed to perform a recovery. If all the media are found, the recovery proceeds automatically. If any media are missing, you must either provide the media or change to the Interactive Recovery Mode.

The main advantage of the Automatic Recovery Mode method is that it does not require any user input, other than loading a spanned sequence in the tape drive or supplying a password when an encrypted session is recovered.

Note: Automatic Recovery Mode is the recommended method.

Interactive Data Restoration

When using the Interactive Recovery Mode to restore data, you must confirm the restoration of each file system before the option can restore it. In addition, you must perform the following actions for each file system:

- Choose a tape device from the list of available devices.
- Provide media and confirm its use.
- Provide a session number from which to restore the file system. You can scan the tape to determine which file systems were backed up on the tape, and then provide the session number.

The advantage of this method is that you have control over the file systems to be restored and the media to use.

Recovering from a Disaster

If disaster strikes your system, use one of the following procedures to perform the disaster recovery operation.

Using the Floppy-Based Method

To recover from a disaster, perform the following steps:

1. Insert the tape containing your emergency data into the tape drive.

   Note: If you are not sure which tapes to use, you are prompted later in the process with the tape details (tape name, tape sequence, tape random ID) so that you can find and insert the correct tapes. For tape libraries, you are prompted to mount a particular tape using the bar code and slot number information (if applicable).

2. Ensure that the tape device is properly connected and turned on. Turn on the computer.

3. Insert the first BrightStor ARCserve Backup emergency disk into the disk drive.

   Note: You are prompted to insert the second emergency disk at the appropriate time during the disaster recovery process.

4. Insert the Sun Solaris installation CD into the CD drive.

5. Enter the following command to start your computer using the Sun Solaris CD:

   ```
   boot cdrom -s
   ```

6. When the computer starts, enter the following commands to mount the emergency disk:

   ```
   #mount /dev/diskette0 /mnt
   #cd /mnt/DR
   #./DRgmain
   ```

   The recovery process starts.

7. Follow the prompts to complete the disaster recovery process.

8. When you restart the computer for the first time after performing the disaster recovery procedure, execute the $BAB_HOME/sbin/DRingres script to recover your Advantage™ Ingres® databases.

Your BrightStor ARCserve Backup server has been recovered.

Using the Tape Method

To use the tape method, you must have configured an alternate location on a remote computer to store the emergency data.

Before you begin recovering your server after a disaster, ensure that you have the following items:

- Sun Solaris installation CD.

  Note: Be sure the version is the same as the version that was previously installed.

- Tape containing the emergency data and the last known backup of the entire node for the failed system.
- The tape name, sequence, session number, and random ID of the tape containing the emergency data for the system. This information is contained in the DRTapeSessionInfo file on the remote computer that was configured to store BrightStor ARCserve Backup emergency data.

Tip: If you have configured /export/drshare as the NFS share to store your disaster recovery information, this file is located in -/export/drshare/DR/data/*hostname*/

To recover from a disaster, perform the following steps:

1. Insert the tape containing your last known good backup into the tape drive.
2. Ensure that the tape device is properly connected and turned on, and that the computer is turned on.
3. Insert the Sun Solaris installation CD into the CD drive.
4. Enter the following command to start your computer using the Sun Solaris CD:

   ```
   boot cdrom -s
   ```

5. Enter the following commands:

   ```
   #cd /
   #mt -t TapeDevice:/dev/rmt/0n rewind
   #mt -t TapeDevice:/dev/rmt/0n fsf <sessionNumber>
   #dd if=TapeDevice:/dev/rmt/0n bs=512 | tar -xvf -
   #mt -t TapeDevice:/dev/rmt/0n rewind
   #cd tmp/CADRO
   #./DRgmain
   ```

   where *TapeDevice* is the tape device file corresponding to the tape device you want to use.

   The recovery process begins.

Note: If the full backup tape is a multiplexing tape, you must change the following line:

```
#dd if=TapeDevice:/dev/rmt/0 bs=512 | tar -xvf -
```

to the following:

```
#dd if=TapeDevice:/dev/rmt/0 bs=512 skip=1 | tar -xvf -
```

6. Follow the prompts to complete the disaster recovery process.
7. When you restart the computer for the first time after performing the disaster recovery procedure, execute the $BAB_HOME/sbin/DRingres script to recover your Advantage Ingres databases.

Your BrightStor ARCserve Backup server has been recovered.

Special Considerations for Database Restores

BrightStor ARCserve Backup has special agents available to back up databases. These agents are:

- BrightStor® ARCserve® Backup for UNIX Agent for Oracle
- BrightStor® ARCserve® Backup for UNIX Agent for Lotus Domino
- BrightStor® ARCserve® Backup for UNIX Agent for Sybase
- BrightStor® ARCserve® Backup for UNIX Agent for Informix
- BrightStor® ARCserve® Backup for UNIX Agent for SAP R/3 for Oracle
- BrightStor® ARCserve® Backup for UNIX Agent for DB2 UDB
- BrightStor® ARCserve® Backup for UNIX Agent for Advantage Ingres

If you have backed up any of these databases using BrightStor ARCserve Backup, you cannot restore the database using the BrightStor ARCserve Backup Disaster Recovery Option. After you have restored the server using the BrightStor ARCserve Backup Disaster Recovery Option, you can start BrightStor ARCserve Backup and restore your databases using a typical database recovery procedure.