BrightStor® ARCserve® Backup for UNIX

Disaster Recovery Option Guide

r11.5

Computer Associates®

Contents

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 servers from disaster, and to get your machine back on line quickly and reliably and 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 Disaster Recovery Option does this for you.

The option allows you to quickly and easily restore servers 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.

How the Option Works

Disaster recovery works by collecting and saving machine-specific information before a disaster strikes. If the Disaster Recovery Option is installed, 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 a remote computer. If disaster strikes, the 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 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 Disaster Recovery Option is a flexible, easy-to-use, enterprise-wide solution to protect your data. 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 Disaster Recovery Option works with regular tape backups. You can recreate hard disk slices and file systems, scan sessions, and perform restores.

The option supports:

- Multiple sessions and spanned tapes
- Multiple tape drives and host adapters
- Use of tape drives in autochangers
- Floppy-based and Tape-based recovery
- Multiplexed backup sessions
- Triple DES3 encrypted sessions
- BrightStor ARCserve Backup tape format

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 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-based method:** 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.

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 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 Disaster Recovery Option.

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

Requirements

Ensure that you have met all of the prerequisites and have all of the information that you need to complete the installation before you begin:

- 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.

Install the Option

You must install BrightStor ARCserve Backup server and manager packages 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 from which to choose, including the Disaster Recovery Option.

The following installation guidelines assume that BrightStor ARCserve Backup is already installed and configured. For information about installing and configuring BrightStor ARCserve Backup, see the *Getting Started* guide.

To install the 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. You can obtain the installation script from the product CD.

3. The license agreement prompts you to accept or decline the terms of the license agreement. To continue with the installation, enter Y.

    Note: You must agree to the terms of the license to install the option.

4. Choose the appropriate selection for licensing.

5. Select the Disaster Recovery Option from the component list. The option is automatically installed in the $BAB_HOME directory.

6. Respond to all prompts as appropriate for your system configuration.

For the complete installation procedure, see the *Getting Started* guide.

No additional installation steps are required to install the option.

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 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 full 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.

Create a Disaster Recovery Plan

Disaster recovery is a two step process: preparation and recovery. 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 configuration similar to that on your original server.

2. Simulate a recovery on your test server by following the instructions in this guide.

Disaster Preparation

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: We recommend that you 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 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-based 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.

Create 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 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.

   Note: 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.

Store Disaster Recovery Information on Remote Servers

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 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

Verify 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, in this order:

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.

4. If you have created floppy disks for disaster recovery, the utility verifies that the files on the floppy disks are identical to the local files tested in the preceding checks..

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

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.

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 Store Disaster Recovery Information on Remote Servers in this guide.

Chapter 4: 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-based method, you must have access to disaster recovery information stored in an alternate location.

- Sun Solaris installation CD-ROM.

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

Data Restoration

When you back up the 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 during the disaster recovery process:

- 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 the **Automatic Recovery Mode**. Alternatively, you can perform a custom recovery and select the file systems to restore and the source from which to restore them. This recovery method is called the **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.

Recover from Disaster

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

Floppy-based Method Disaster Recovery

To use the Floppy-based method, you must ensure that you have the following items:

- Sun Solaris installation CD. You must ensure that the version is the same as the version that was previously installed.

- Two emergency disks containing configuration information for the specific computer to be recovered.

Recover from Disaster Using the Floppy-based Method

To recover from a disaster using the Floppy-based Method, perform the following steps:

1. Insert the tape containing your last full backup 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.

   Note: If you are running Solaris 10 on AMD64, to boot from the installation CD, you may be required to change the boot sequence to set CD-ROM as the first boot device.

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

   ```
   boot cdrom –s
   ```

   Note: If you are running Solaris 10 on AMD64, enter the following command when the prompt Select type of installation appears:

   ```
   boot -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.

On Solaris 10, enter the following command to mount the emergency disk:

```
mount -r /dev/diskette0 /mnt
```

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

Your BrightStor ARCserve Backup server has been recovered.

Tape-based Method Disaster Recovery

To use the Tape-based 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. You must ensure that 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.

   Note: 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*/

Recover from Disaster Using the Tape-based Method

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.

    Note: If you are running Solaris 10 on AMD64, to boot from the installation CD, you may be required to change the boot sequence to set CD-ROM as the first boot device.

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

    ```
    boot cdrom –s
    ```

    Note: If you are running Solaris 10 on AMD64, enter the following command when the prompt Select type of installation appears:

    ```
    boot -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.

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

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

    to the following:

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

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

Your BrightStor ARCserve Backup server has been recovered.

Special Considerations for Databases

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 Disaster Recovery Option. After you have restored the server using the Disaster Recovery Option, you can start BrightStor ARCserve Backup and restore your databases using a typical database recovery procedure.