BrightStor® ARCserve® Backup for Linux

Disaster Recovery Option Guide

r11.5

D01217-2E

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, and, if configured with the mount point, on a remote NFS location. If disaster strikes, the Disaster Recovery Option can recover the server to the last full backup state. Recovery depends on the availability of both the 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 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. The option supports:

- Multiple sessions and spanned tapes
- Multiple tape drives and host adapters
- Use of drives in tape libraries
- CD-based recovery
- Multiplexed backup sessions
- Multistreamed backup sessions
- Multiple file system types (for example, ext2, ext3, reiserfs, vfat, jfs, and xfs)
- Disk Staging Option using file system devices (B2D2T)
- Triple DES3 encrypted sessions
- BrightStor ARCserve Backup tape format

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

Disaster Recovery Method

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 CD-based method to store emergency data to be used in the event of a disaster. This method requires the full backup tape set, the Emergency Disk, and the recovery CD. The Emergency Disk must be created before the disaster.

Note: You can specify an NFS mount point during configuration to store emergency data there. The same location is required during disaster recovery.

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

The Disaster Recovery Option requires the following hardware:

- Intel x86 system
- One of the following:
  - 3.5" Floppy drive
  - NFS mount point
  - Removable media (for example, USB flash memory drive or Compact Flash and Secure digital cards)
- Linux-compatible CD-ROM drive
- SCSI tape drive

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

- Verify that your system meets the minimum requirements to install the option. For a complete 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.
- Verify that you have a functional floppy drive, a configured NFS mount point, or an available removable media mount point and a bootable CD-ROM.

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.

Alternate Location for Disaster Recovery Information

During configuration of the option, you are asked if you want to configure the Emergency Data Alternate Directory, an alternate location in which to save disaster recovery information. This is an NFS mount point to which emergency data is written after a full local server backup has written emergency data to the local server.

If the BrightStor ARCserve Backup server fails, machine-specific disaster recovery information can also be lost. To avoid this type of data loss, 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 cadro_setup configuration script, located in the $BAB_HOME/DR directory.

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 Linux server from potential disaster and bring it back online quickly by having all necessary disaster recovery components, the Emergency Disk or machine-specific information stored at an alternate location, a full backup on tape, and the Disaster Recovery bootable CD, available.

Ensure that the Disaster Recovery Option is installed on the BrightStor ARCserve Backup server 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.

Prepare for Disaster on Linux

To prepare for a disaster, perform the following steps:

1. Run the installation script and install the Disaster Recovery Option.
2. Perform a full node backup to tape on the machine on which the Disaster Recovery Option is installed.
3. Run DRmkdisk from the $BAB_HOME/DR/ directory. If you configured an NFS mount point during setup, you can also launch DRmkdisk from there. 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.

   If your server has no floppy drive, be sure to create an alternate location in which to save emergency data, using an NFS mount point. Alternatively, you can save emergency data to additional removable media (such as USB flash memory devices or Compact Flash and Secure digital cards) using DRmkdisk.

   Note: If you keep emergency data for several systems on the same disk, do not format the disk.

   It is a good practice to run this script when you change your computer hardware configuration and every time you run a full backup to ensure that the tape name and session information for the backup on the Emergency Disk are up-to-date.
4. Create the recovery CD. The Disaster Recovery Option CD ISO image can be downloaded from the Customer Support website and burned to a blank CD using CD creation software to create the bootable CD. This CD ISO image can be used to recover servers running any Linux distribution supported by the Disaster Recovery Option.

   Note: Your computer must be able to boot from the IDE or SCSI CD-ROM.

Verify Disaster Recovery Information

On Linux 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.

Chapter 4: Recovering Your System After a Disaster

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 successful full backup of the entire node for the failed system
- The Disaster Recovery bootable CD
- Emergency Disk for the failed system or access to the remote NFS location you specified during setup if you configured an alternate location for disaster recovery information.

Data Restoration

When you back up the entire node of a 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:

- Recovery Server Name
- Emergency Floppy Date
- Tape Name
- Tape ID
- Sequence Number
- Tape Barcode

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 **Express Mode**. Alternatively, you can perform a custom recovery using **Advanced Mode**, allowing you to create a customized partition table and a customized session list before data restoration. This recovery method should be used only by advanced Linux system administrators.

Express Mode

When using Express mode to restore your data, 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 (Emergency Disk or NFS mount point and tapes) needed to perform a recovery. If all the media are found, the recovery proceeds automatically.

The main advantage of Express mode 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: Express mode is the recommended method.

Advanced Mode

When using Advanced mode, you can restore data to a customized disk layout. This allows you to expand partition sizes if the current hard disks are larger than the disks used for the backup operation. To create a new disk layout manually, perform the following steps:

1. Clear the Partition Hard Disks check box.
2. Click the Console button to open a terminal window.
3. Use fdisk or parted to create the partitions.
4. Enter Exit and press Enter to close the terminal window.
5. Click Next to continue the recovery process.

You can also customize recovery session lists, allowing you to restore sessions from multiple tapes, depending upon the needs of your system.

Recover from Disaster

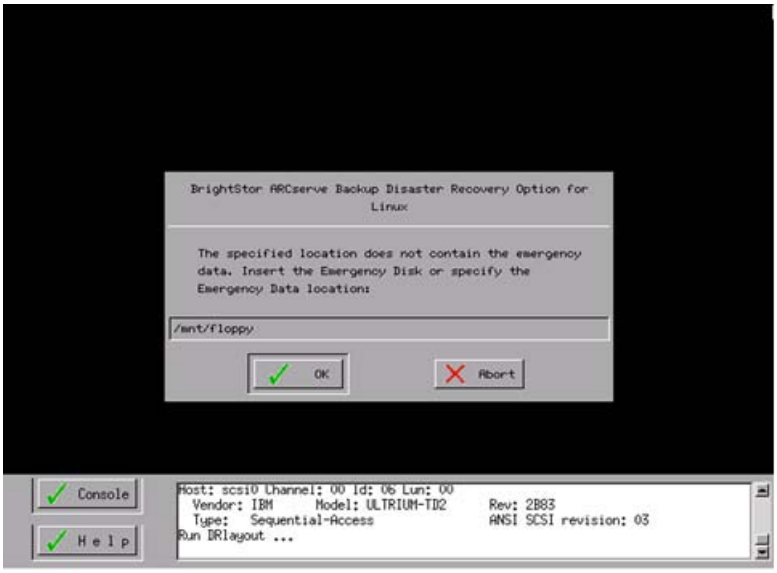
If disaster strikes your system, use the following procedure to perform a disaster recovery operation:

1. Ensure that the tape device is properly connected and turned on. Turn on the computer.
2. Insert the bootable Disaster Recovery CD.
3. At the boot prompt, press Enter.
4. Choose a keyboard map.
5. Select the language to use during the disaster recovery process.

6. If tape devices could not be found, perform one of the following:
   - If the SCSI card driver was not loaded at boot time, click Console to open a console and execute the modprobe command.
   - If the SCSI devices were powered on after the machine was started, click Console to open a console and execute the DRrescanscsibus utility to probe and provide information to the system.
   - If the SCSI connection failed, check the SCSI card and tape drive connections.
7. Insert the Emergency Floppy Disk and load the tape containing the full backup to be restored.

   If the server does not have a floppy drive, or if the disk is not available but the emergency data is stored in an alternate location or on additional removable media, you are prompted to specify the mount point.

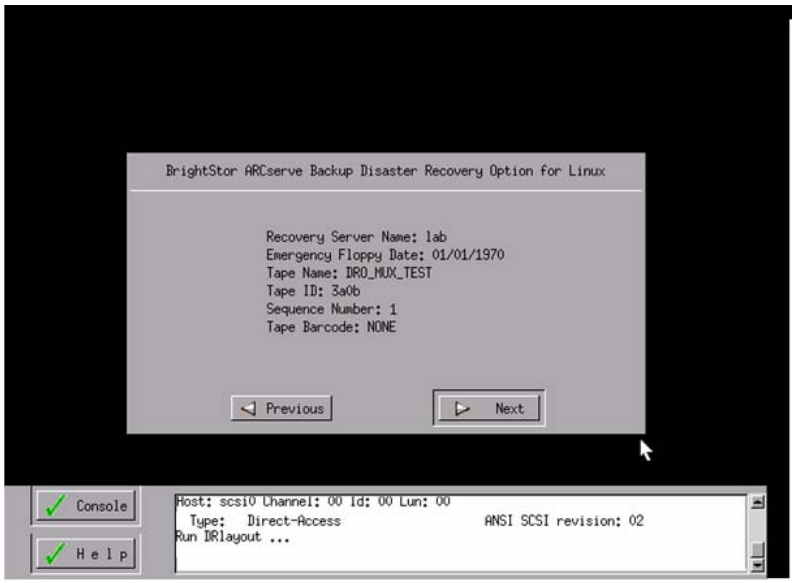
   Note: If no IP address has been assigned and you want to configure an NFS mount point to the location of the emergency data, see the General Usability section of the Frequently Asked Questions appendix in this guide for more information.



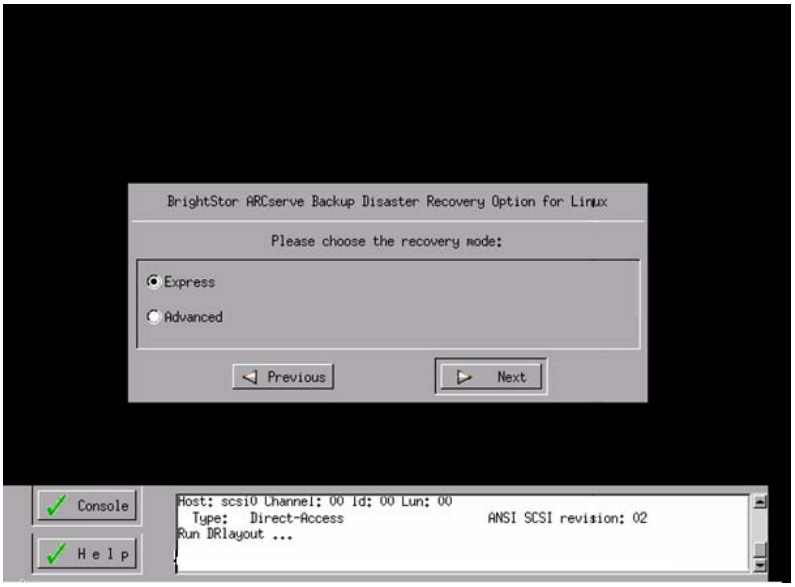
   The disaster recovery process begins.

8. If the Emergency Disk contains machine-specific information for multiple machines, you must select the machine for which you are performing disaster recovery.

9. Verify the server, Emergency Disk, and tape information and click Next.



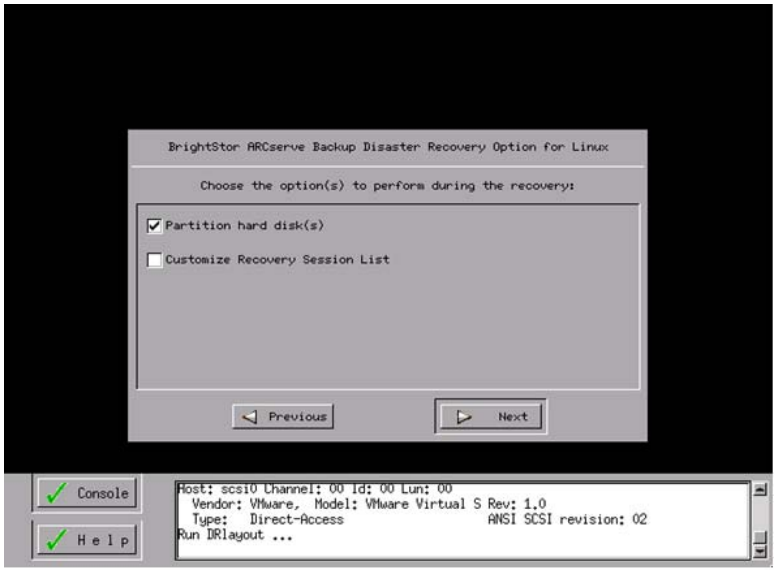
10. When prompted, choose either the Express mode or the Advanced mode for the recovery process.



The Express mode requires little user interaction except when backed up sessions are protected by passwords or when a media is spanned. If the full backup session is password protected, you must enter the session password to continue the recovery. If the full backup is spanned over multiple media, you must insert the correct media when prompted. Data is read from the tape and restored to your system.

In the Advanced mode, you can configure the following options:

- **Partition Hard Disks**: If the size, number, or configuration of the disks has changed, you can manually partition the disks and file systems and restore your data to the new custom partition table. You can clear the Partition Hard Disks check box, open a console, and use fdisk to create a custom file system layout.
- **Customize Recovery Session Lists**: Depending upon your circumstances, you can remove sessions and restore data from different tapes. To customize the session list, click the check box.



11. Verify the server, Emergency Disk, tape, and session information and click Next.
12. 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.
13. When the disaster recovery process finishes, press Enter to restart your computer.

    Note: Remove the disaster recovery CD after your machine has shut down and before it reboots.

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 Agent for Oracle
- BrightStor® ARCserve® Backup Agent for Apache Web Server
- BrightStor® ARCserve® Backup Agent for MySQL
- BrightStor® ARCserve® Backup 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.

Disaster Recovery Utilities

The 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.

Note: These utilities can be executed in a terminal window. To access a terminal window, click the Console button during the disaster recovery process.

Appendix A: Disaster Recovery Scenarios

This chapter provides information about recovering server class systems using the Disaster Recovery Option. The scenarios provide detailed information for recovery of Red Hat Linux, SuSE Linux, Miracle Linux, and Red Flag Linux systems. Each scenario describes the specific hardware and software being recovered and provides a procedure to recover that system.

Red Hat Linux Scenarios

The following scenario provides system-specific information and procedures to recover a typical Red Hat Linux system.

Scenario 1: Recover a Dell PowerEdge 1600SC Machine

The following scenario uses the Disaster Recovery Option to recover a Red Hat Linux system after a disaster.

Server Specifications

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

- System: DELL PowerEdge 1600SC with a dual-processor Xeon 2.00GHz CPU and 1.99GHz, 1GB RAM, connected to a EXABYTE Mammoth2 tape drive through a Symbios logic SCSI adapter.
- Network Adapter: Intel 82540EM based PCI Ethernet Adapter (10/100/1000)
- Storage: 3 discs of 34.6GB configured as one logical volume
- Partitions:
  - /dev/sda1- ext2 – 1GB - /boot (boot file system)
  - /dev/sda2 – ext3 - 44GB - / (root file system)
  - /dev/sda3 - SWAP – 5GB

- Software Environment:
  - Red Hat Linux Enterprise Server 3.0
  - GNOME Desktop Environment
  - BrightStor ARCserve Backup server and manager components
    - BrightStor® ARCserve® Backup Client Agent for Linux
    - Disaster Recovery Option

Prepare for Disaster During Machine Setup

Planning for a successful disaster recovery starts when you set up your DELL PowerEdge 1600SC. Perform the following procedure when you install BrightStor ARCserve Backup for Linux and the Disaster Recovery Option on your machine:

1. Save any extra hardware drivers you installed manually when you initially set up your Red Hat Linux Enterprise Server 3.0 machine. You may need to provide these drivers again during the disaster recovery process.

   In this scenario, we did not add any drivers manually.

   Note: Check the Hardware Browser if you do not know the devices installed on your Linux machine.

2. Start the BrightStor ARCserve Backup server and perform a full machine backup.

3. Create a disaster recovery bootable CD. You can download the ISO image from the Customer Support website.

4. Execute the DRmkdisk script, located in the $BAB_HOME/DR directory, to create an Emergency Disk.

Disaster Recovery Prerequisites

You must have performed a full backup of your machine using BrightStor ARCserve Backup, and have the following items before you can start the disaster recovery process:

- The Emergency Disk containing the backed up data to be restored
- The disaster recovery CD
- Media containing the full backup to be restored
- Any drivers you installed manually during initial system setup

Recover from Disaster

To perform a disaster recovery on your DELL PowerEdge 160SC system, perform the following steps:

1. Boot the machine using the disaster recovery bootable CD.
2. At the boot prompt, press Enter.
3. Choose a keyboard map.
4. Select a language to use during the disaster recovery process.
5. Insert the Emergency Disk and load the tape containing the full backup to restore.
6. Verify the server, Emergency Disk, and tape information and click Next.
7. When prompted, select Express as the recovery mode.

   Your hard disks are partitioned, the file system layout is created, and the restore process begins.
8. When the disaster recovery process finishes, press Enter to boot back to your previous system configuration.

   Note: Remove the disaster recovery CD after your machine has shut down and before it reboots.

SuSE Linux Scenarios

The following scenario provides system-specific information and procedures to recover a typical SuSE Linux system.

Scenario 1: Recover an HP ProLiant G3 ML330 Machine

The following scenario uses the Disaster Recovery Option to recover a SuSE Linux system after a disaster.

Server Specifications

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

- System: HP ProLiant G3 ML330 with a processor Intel R XEON CPU 2.80GHz, 1GB RAM, connected to a StorageTek L20 tape library through a Adaptec AHA-2940 SCSI adapter
- Network Adapter: Compaq NC7760 GB Server Adapter
- Storage: Three discs of 34.6GB; Disk 0 not configured; Disks 1 and 2 configured as MegaRAID-LD0 RAID1
- A USB flash memory drive

- Partitions
  - /dev/cciss/c0d0p1 -ext2 - 128M - /boot (boot file system)
  - /dev/cciss/c0d0p2 – SWAP-2G - SWAP
  - /dev/cciss/c0d0p3 -vfat - 1G - /vfat
  - /dev/cciss/c0d0p4 –ext3 - 10G - /(root file system)
- Software Environment
  - SuSE Linux Enterprise Edition v9.0
  - KDE Desktop Environment
  - BrightStor ARCserve Backup server and manager components
    - Client Agent for Linux
    - Disaster Recovery Option

Prepare for Disaster During Machine Setup

Planning for a successful disaster recovery starts when you set up your HP ProLiant G3 ML330 system. Perform the following procedure when you install BrightStor ARCserve Backup for Linux and the Disaster Recovery Option on your machine:

1. Save any extra hardware drivers you installed manually when you initially set up your SuSE Linux machine. You may need to provide these drivers again during the disaster recovery process.

   In this scenario, a cciss driver was needed. This driver is included on the disaster recovery ISO CD image.

2. Start the BrightStor ARCserve Backup server and perform a full machine backup. Sessions 1-8 are created.

3. Run a second full machine backup. Sessions 9-16 are created.

4. Create a disaster recovery bootable CD. You can download the ISO image from the Customer Support website.

5. Execute the DRmkdisk script, located in the $BAB_HOME/DR directory, to write the emergency data to the USB flash memory drive.

Disaster Recovery Prerequisites

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

- The flash memory drive containing the backed up data to be restored.
- The disaster recovery CD
- Media containing the full backup to be restored
- Any drivers you installed manually during initial system setup.

Recover from Disaster

To perform a disaster recovery on your HP ProLiant G3 ML330 system, perform the following steps:

1. Start the machine using the disaster recovery bootable CD.
2. At the boot prompt, press Enter.
3. Choose a keyboard map.
4. Select a language to use during the disaster recovery process.
5. Insert the flash memory drive and load the full backup to be restored.
6. Click Console and manually configure the flash memory drive mount point.
7. Specify the mount point for the flash memory drive.
8. Verify the server and tape information and click Next.
9. When prompted, select Advanced as the recovery method.
10. Select the Customize Recovery Session List option and click Next.

    Note: The Partition hard disks option should remain selected.
11. Clear the selection of session 11, the session created for the /vfat file system during the second full backup. Ensure that session 11 is not selected.
12. Click Add sessions.
13. Select the tape containing the two full backups (sessions 1-16) and click Next.
14. Select session 3, the session created for the /vfat file system during the first full backup, and click Next.

15. Ensure that session 3 is to be restored to /vfat, not session 11, and click Next.

    Your hard disks are partitioned, the file system layout is created, and the restore process begins.

16. When the disaster recovery process finishes, press Enter to boot back to your previous system configuration.

    Note: Remove the disaster recovery CD after your machine has shut down and before it reboots.

Miracle Linux Scenarios

The following scenario provides system specific information and procedures to recover a typical Miracle Linux system.

Scenario 1: Recover a Dell Precision Workstation 350 MT Machine

The following scenario uses the Disaster Recovery Option to recover a Miracle Linux system after a disaster.

Server Specifications

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

- System: Dell Precision Workstation 350 MT with a processor Intel XEON CPU 1.80GHz, 512MB RAM, connected to a HP C5683A tape drive through a Adaptec AHA-2940U2W SCSI adapter.
- Network Adapter: Dell 3c905c-TX/TX-M[Tornado]
- Storage: Three discs of 34.6GB configured as MegaRAID-LD0 RAID5
- Partitions
  - /dev/sda1 -ext2 - 296M - /boot (boot file system)
  - /dev/sda2 -ext2 - 20G - / (root file system)
  - /dev/sda3 -ext2 - 1G - swap
  - /dev/sda5 -ext2 - 40G - /data

- Software Environment
  - Miracle Linux Standard Edition v3.0
  - GNOME Desktop Environment
  - BrightStor ARCserve Backup server and manager components
  - Client Agent for Linux
  - Disaster Recovery Option

Prepare for Disaster During Machine Setup

Planning for a successful disaster recovery starts when you set up your DELL Precision Workstation 350 MT system. Perform the following procedure when you install BrightStor ARCserve Backup for Linux and the Disaster Recovery Option on your machine:

1. Save any extra hardware drivers you installed manually when you initially set up your Miracle Linux machine. You may need to provide these drivers again during the disaster recovery process.

   In this example, no drivers needed to be added manually.

2. Start the BrightStor ARCserve Backup server and perform a full machine backup.

3. Create a disaster recovery bootable CD. You can download the ISO image from the Customer Support website.

4. Execute the DRmkdisk script, located in the $BAB_HOME/DR directory, to create an Emergency Disk.

Disaster Recovery Prerequisites

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

- The Emergency Disk containing the backed up data to be restored.
- The disaster recovery CD
- Media containing the full backup to be restored
- Any drivers you installed manually during initial system setup.

Recover from Disaster

To perform a disaster recovery on your DELL Precision Workstation 350 MT system, perform the following steps:

1. Start the machine using the disaster recovery bootable CD.
2. At the boot prompt, press Enter.
3. Choose a keyboard map.
4. Select a language to use during the disaster recovery process.
5. Insert the Emergency Disk and load the full backup to be restored.
6. Verify the server, Emergency Disk, and tape information and click Next.
7. When prompted, select Express as the recovery method.

   Your hard disks are partitioned, the file system layout is created, and the restore process begins.
8. When the disaster recovery process finishes, press Enter to boot back to your previous system configuration.

   Note: Remove the disaster recovery CD after your machine has shut down and before it reboots.

Red Flag Linux Scenarios

The following scenario provides system specific information and procedures to recover a typical Red Flag Linux system.

Scenario 1: Recover a Dell GX260 Machine

The following scenario uses the Disaster Recovery Option to recover a Red Flag Linux system after a disaster.

Server Specifications

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

- System: DELL GX260 with a processor P4 2.00GHz CPU, 512MB RAM, connected to a HP C5683A tape drive through a Adaptec AHA-2940U2W SCSI adapter.
- Network Adapter: Intel PRO/1000 MT Network Connection
- Storage: WDC-WD400BB-75DEA0-Ultra ATA/100 43.7GB 100MB/s Disk drive

- Partitions
  - / - ext3 – 5.7GB
  - /opt – ext2 - 5.7GB
  - /usr - reiserfs– 5.7GB
  - /home – softraid on ext3 9.7 GB
  - hda5 – SWAP 1.0 GB
  - hda8 – vfat 5.7 GB
- Software Environment
  - Red Flag Linux DC 4.1
  - KDE Desktop Environment
  - BrightStor ARCserve Backup
  - Client Agent for Linux
  - Disaster Recovery Option

Prepare for Disaster During Machine Setup

Planning for a successful disaster recovery starts when you set up your DELL GX260 system. Perform the following procedure when you install BrightStor ARCserve Backup and the Disaster Recovery Option on your machine:

1. Save any extra hardware drivers you installed manually when you initially set up your Red Flag DC 4.1 machine. You may need to provide these drivers again during the disaster recovery process.

   In this scenario, we did not add any additional drivers manually.

2. Start the BrightStor ARCserve Backup server and perform a full machine backup.

3. Create a disaster recovery bootable CD. You can download the ISO image from the Customer Support website.

4. Execute the DRmkdisk script, located in the $BAB_HOME/DR directory, to create an Emergency Disk.

Disaster Recovery Prerequisites

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

- The Emergency Disk containing the backed up data to be restored
- The disaster recovery CD
- Media containing the full backup to be restored
- Any drivers you installed manually during initial system setup

Recover from Disaster

To perform a disaster recovery on your DELL GX260 system, perform the following steps:

1. Boot the machine using the disaster recovery bootable CD.
2. At the boot prompt, press Enter.
3. Choose a keyboard map.
4. Select a language to use during the disaster recovery process.
5. Insert the Emergency Disk and load the tape containing the full backup to be restored.
6. Verify the server, Emergency Disk, and tape information and click Next.
7. When prompted, select Express as the recovery mode.

   Your hard drive is partitioned, the file system layout is created, and the restore process begins.
8. When the disaster recovery process finishes, press Enter to boot back to your previous system configuration.

   Note: Remove the disaster recovery CD after your machine has shut down and before it reboots.

Appendix B: Frequently Asked Questions

This appendix provides answers to some frequently asked questions using the Disaster Recovery Option. To help you quickly find the answers to your questions, the information in this appendix is divided into the following categories:

- General Usability
- Hardware
- Utilities

General Usability

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

What constitutes a full backup for disaster recovery purposes?

If a machine is designated for a full backup, the selection box for the machine is solid green.

Note: To ensure that the entire server is backed up, we recommend that you do not use filters.

Is a floppy drive required to perform disaster recovery?

No, if you have configured the option to write emergency data to an NFS mount point. See the section Alternate Location for Disaster Recovery Information in this guide for more information.

Note: You can use DRmkdisk to write emergency data to alternate removable media (for example, USB flash memory drives or Compact Flash and Secure digital cards.

What file systems can I recover?

The option supports ext2, ext3, reiserfs, xfs, jfs, and vfat file systems.

Can I configure my network to transfer files to a remote location or set up an NFS mount point during the disaster recovery process?

During disaster recovery, you can configure your network to allow you to transfer files to a remote destination or to set up an NFS mount point. To configure your network, perform the following procedure:

1. Identify the driver required for your Network Interface Card (for example, 3c59x or e1000).
2. From a command line, enter the following to display the currently loaded modules:

   ```
   lsmod
   ```

3. If your driver does not appear in the list, use one of the following methods to load the correct driver:
   - Enter modprobe *driver name*, as in the following example:

     ```
     modprobe e1000
     ```

   - Enter DRload *driver name,* as in the following example:

     ```
     DRload 3c59x
     ```

4. Configure the IP address as in the following:

   ```
   ifconfig eth# xxx.xxx.xxx.xxx netmask yyy.yyy.yyy.yyy
   ```

   For example,

   ```
   ifconfig eth0 172.31.255.255 netmask 255.255.255
   ```

5. Execute the following command to start telnet and the ftp server:

   ```
   /etc/init.d/xinetd restart
   ```

How do I load a driver that is not contained on the Disaster Recovery CD?

When you boot with the Disaster Recovery CD, most hardware is auto-probed and the corresponding drivers are loaded. However, because new hardware is frequently introduced, it is possible that a required driver will not be contained on the Disaster Recovery CD. If the required driver is not on the Disaster Recovery CD, perform the following steps to load the driver:

1. Identify the driver required for your device (for example, aic7870).
2. Obtain the required driver and ensure that it is compatible with the kernel version on the Disaster Recovery CD. To determine the kernel version, run uname -r in the Disaster Recovery environment.
3. Mount the media containing the driver.

4. Load the driver using the command insmod, as in the following example:

   ```
   #insmod aic7870.ko
   ```

5. Verify that the driver is loaded. To do so, run lsmod, as in the following example:

   ```
   #lsmod|grep aic7870
   ```

Note: To load a driver successfully, the driver must be compatible with the version of the kernel on the Disaster Recovery CD. If you cannot find a driver version that is compatible, contact Customer Support for assistance.

Will the Disaster Recovery Option recover all of my file system attributes?

The option recovers most critical configurations such as ACLs, Block Size, Permissions, UID, and GID. However, if you have special manual configurations, we recommend that you check your configuration and, if necessary, reset these specifications once the server has been recovered and restarted.

How does the Disaster Recovery Option for Linux restore snapshot volumes that were included in the full backup used for disaster recovery?

The option restores the session containing the snapshot volume to the mount point to which the snapshot was mounted at the time of the backup operation.

We recommend that you do not include snapshot volume backups in disaster recovery backups to avoid having disk space run out when the original volume and the snapshot volume are both restored during disaster recovery.

Is the Disaster Recovery Option for Linux integrated with the BrightStor® ARCserve® Backup Storage Area Network (SAN) Option?

The Disaster Recovery Option for Linux is not integrated with the SAN Option. However, the option can be used to recover from SAN devices if you can ensure that no other SAN servers will use the shared devices during the disaster recovery operation.

Does the Disaster Recovery Option support LVM and SoftRAID configurations?

Yes.

I am experiencing problems during the startup of my X-Window environment during Disaster Recovery. What can I do to correct this?

BrightStor ARCserve Backup Disaster Recovery program runs in the X-Window environment with some default settings suitable for most Linux systems. If X-Window cannot be launched in your environment, you may need to manually set up the X-Window environment using the following procedure:

1. Press Ctl+Alt+Backspace to enter a console and run the commands identified in one of the following methods:

   Method 1:

   Enter the following commands:

   ```
   cd /etc/X11
   ```

   ```
   cp XF86Config.alt XF86Config
   ```

   Method 2:

   Enter the following command:

   ```
   xf86config
   ```

   You are prompted to make hardware selections. When you have made all of the necessary selections, you are prompted with the question “Shall I write it to /etc/X11/XF86Config?” Answer Y for yes.

2. To verify the setup of the X-Window environment, run the following command:

   ```
   xinit
   ```

3. If X-Window runs properly, press Ctl+Alt+Backspace to enter the console and run the following command to continue with the disaster recovery process:

   ```
   DRstart
   ```

Hardware

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

Can I back my system up to a tape library and then recover it from the tape library?

The option does not support recovery from auto-loaders, changers, or tape libraries. However, you can recover a system if the backup tape is loaded from the slot to the drive either manually or from the server using mtx. For more information, enter mtx help.

My Disaster Recovery CD will not boot. Why?

If you receive a Bus Error while booting from the Disaster Recovery CD, the image may not have been burned correctly. Create another Disaster Recovery CD and start the procedure again.

Utilities

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

How do I generate logs during the disaster recovery process?

In an alternate console or terminal window, run the DRtrace utility to generate a log file. To access an alternate console, press Ctrl+ Alt+F#. To access a terminal window from the Disaster Recovery interface, click the Console button.

What does the DRrescanscsibus utility do? When would I use it?

The DRrescanscsibus utility scans the attached SCSI devices that were not detected during system boot and provides this information to the kernel. Use this utility if, for example, after the system has booted, you power on a tape drive that uses a SCSI connection.