Chapter 1

Planning a Backup Strategy

As a site administrator, you must make sure there are backups of the files at your site. Users depend on you to recover files that have been accidentally erased, or lost due to hardware problems.

This chapter contains the following sections:

- "Types of Backup Media" on page 3
- "Choosing a Backup Tool" on page 4
- "Backup Strategies" on page 6

When you are familiar with backup and have addressed the needs of your site, refer to Chapter 2 for detailed information on the backup utilities that you plan to use.

Types of Backup Media

Some of the common types of backup media supported on Silicon Graphics, Inc., systems include:

- 1/4" cartridge tape, 4-track
- 8 mm cartridge
- DAT
- DLT

In addition to backup devices attached to any particular system, backup devices of various types and capacities may be accessible through network connections. Refer to your owner's guide for information on locally accessible devices, and the appropriate vendor documentation for network-accessible device information.

Certain limitations or conditions described in this chapter might not apply to your specific media. For example, if you back up a 350 MB filesystem with an 8 mm cartridge

drive (which can hold up to 1.2 GB), you probably don't have to worry about using more than one tape. (For more information on tape capacities, see "IRIX Admin: Peripheral Devices.")

Choosing a Backup Tool

The IRIX system provides a variety of backup tools, and you should use whichever ones work best for you. If many users at your site are already familiar with one backup program, you may wish to use that program consistently. If there are workstations at your site from other manufacturers, you may wish to use a backup utility that is common to all the workstations.

IRIX provides the following utilities for backing up your data:

- System Manager
- bru(1M)
- Backup(1M) and Restore(1M), which use *bru*
- dump(1M) and restore(1M)
- xfsdump(1M) and xfsrestore(1M) for XFS™ filesystems
- tar(1M)
- cpio(1M)
- dd(1M)

Optional products for Silicon Graphics systems are also available. IRIS NetWorker™ is a scalable, full-featured data management tool for data backup and recovery. You can use IRIS NetWorker to back up data on high-end servers, or centrally manage backups for all your network workstations and file servers. See your Silicon Graphics sales representative for optional backup solutions.

Backup tools can be viewed as filesystem-oriented programs, like *bru*, *Backup*, and *dump,* or as file- and directory-oriented programs, like *tar* and *cpio.* While these utilities are not actually limited to one or the other, they are generally more convenient when used in this way. In addition, you can use dd(1) to read images exactly as they are written, with or without conversions. The *dd* command is useful to read data that is written in a format incompatible with the other backup utilities, but you would not normally use *dd* to create backups.

Table 1-1 summarizes the backup utilities available with IRIX.

Table 1-1 Backup Utilities Summary

Utility	Summary Description	Reference
System Manager	Graphical interface to *bru* utility. Most convenient and probably best tool if you are backing up only your own IRIX host.	*Personal System Administration Guide*
bru	Automatic file compression, space estimates, integrity checking. Prompts for additional media. May not be available on all hosts in a heterogeneous environment.	bru(1) reference page and "bru" on page 19
Backup and *Restore*	A command line "front end" to the *bru* utility.	Backup(1) and Restore(1) reference pages and "Backup and Restore" on page 23
dump and *restore*	Supports incremental backups and interactive restores. Standard UNIX backup utilities good in heterogeneous environments (but cannot back up XFS filesystems).	dump(1M) and restore(1M) reference pages and "dump and restore" on page 26
xfsdump and *xfsrestore*	Supports incremental backups, interactive restores, and interrupt recovery. Use instead of *dump* and *restore* on XFS filesystems.	xfsdump(1M) and xfsrestore(1M) reference pages and "xfsdump and xfsrestore" on page 30
tar	Most common UNIX backup utility historically and in current distribution, making it portable and thus widely used in very heterogeneous computer environments.	tar(1) reference page and "tar" on page 62
cpio	Flexible and standard UNIX command generally combined in command line pipes with other commands.	cpio(1) reference page and "cpio" on page 65
dd	Standard UNIX command to read input and write output with optional conversions.	dd(1M) reference page and "dd" on page 67

Backup Strategies

You should develop a regimen for backing up the system or systems at your site and follow it closely. That way, you can accurately assess which data you can and cannot recover in the event of a mishap.

Exactly how you perform backups depends upon your workstation configuration and other factors. Regardless of the strategy you choose, though, you should always keep at least two full sets of reasonably current backups. You should also encourage users to make their own backups, particularly of critical, rapidly changing files. Users' needs can change overnight, and they know best the value of their data.

Workstation users can back up important files using the System Manager, found in the "System" toolchest on your screen. The System Manager is described in detail in the *Personal System Administration Guide*. Make sure users have access to an adequate supply of media (for example, cartridge tapes), whether new or used.

If your media can handle your largest filesystem with a single volume, you don't have to use an incremental backup scheme, though such a system reduces the amount of time you spend making backups. However, if you must regularly use multiple volumes to back up your filesystems, then an incremental backup system reduces the number of tapes you use.

The following sections discuss the different aspects of backing up data.

When to Back Up Data and What to Back Up

How often you back up your data depends upon how busy a system is and how critical the data is. A simple rule of thumb is to back up any data on the system that is irreplaceable or that someone does not want to reenter.

Root Filesystems

On most systems, the root filesystem is fairly static. You do not need to back it up as frequently as the */usr* filesystem.

Changes may occur when you add software, reconfigure hardware, change the site-networking (and the system is a server or network information service [NIS] master workstation), or change some aspect of the workstation configuration. In some cases, you

can maintain backups only of the individual files that change, for example, */unix*, */etc/passwd*, and so forth.

This process of backing up single files is not always simple. Even a minor system change such as adding a user affects files all over the system, and if you use the graphical System Manager, you may tend to forget all the files that may have changed. Also, if you are not the only administrator at the site, you may not be aware of changes made by your coworkers. Using complete filesystem backup utilities, such as the System Manager or *bru*, on a regular schedule avoids these problems.

A reasonable approach is to back up the root partition once a month. In addition to regular backups, here are some specific times to back up a root filesystem:

- whenever you add users to the system, especially if the workstation is an NIS master workstation
- just before installing new software
- after installing new software and when you are certain the software is working properly

If your system is very active, or if you are not the only administrator, back up the root filesystem regularly.

User Filesystems

The */usr* filesystem, which often contains both system programs (such as in */usr/bin*) and user accounts, is usually more active than a root filesystem. Therefore, you should back it up more frequently.

At a typical multiuser installation, backing up once per day, using an incremental scheme, should be sufficient.

Treat the */var* filesystem similarly—it contains data such as the contents of users' mailboxes.

Incremental Backups

Incremental backups can use fewer tapes to provide the same level of protection as repeatedly backing up the entire filesystem. They are also faster than backing up every file on the system.

An incremental scheme for a particular filesystem looks something like this:

1. On the first day, back up the entire filesystem. This is a monthly backup.
2. On the second through seventh days, back up only the files that changed from the previous day. These are daily backups.
3. On the eighth day, back up all the files that changed the previous week. This is a weekly backup.
4. Repeat steps 2 and 3 for four weeks (about one month).
5. After four weeks (about a month), start over, repeating steps 1 through 4.

You can recycle daily tapes every month, or whenever you feel safe about doing so. You can keep the weekly tapes for a few months. You should keep the monthly tapes for about one year before recycling them.

Backing Up Files Across a Network

If you are managing a site with many networked workstations, you may wish to save backups on a device located on a central workstation.

To back up across a network, use the same basic backup commands, but with a slight change. Enter:

system_name`:/dev/tape`

If required, specify an account on the remote device:

user`@`*system_name*`:/dev/tape`

Users can use a central tape drive from their workstations with this method. Note that if you are backing up to a remote tape drive on a workstation that is not made by Silicon Graphics, the device name */dev/tape* may not be the correct name for the tape drive. Always learn the pathname of the tape device before executing the backup commands.

For example:

```
tar cvf guest@alice:/dev/tape ./bus.schedule
```

or

```
echo "./bus.schedule" | cpio -ovcO guest@alice:/dev/tape
```

Automatic Backups

You can use the *cron* utility to automatically back up filesystems at predetermined times. The backup media must be already mounted in the drive, and, if you want this to be truly automatic, it should have enough capacity to store all the data being backed up on a single piece of media. If all the data doesn't fit, then someone must manually change backup media.

Here is an example *cron* command to back up the */usr/src* hierarchy to */dev/tape* (tape drive) every morning at 03:00 using *bru*:

```
0 3 * * * /usr/sbin/bru -c -f /dev/tape /usr/src
```

Place this line in a *crontabs* file, such as */var/spool/cron/crontabs/root*.

This sort of command is useful as a safety net, but you should not rely on automatic backups. There is no substitute for having a person monitor the backup process from start to finish and properly archive and label the media when the backup is finished. For more information on using *cron* to perform jobs automatically, see "IRIX Admin: System Configuration and Operation."

Storing Backups

Store your backup tapes carefully. Even if you create backups on more durable media, such as optical disks, take care not to abuse them. Set the write protect switch on tapes you plan to store as soon as a tape is written, but remember to unset it when you are ready to overwrite a previously-used tape.

Do not subject backups to extremes of temperature and humidity, and keep tapes away from strong electromagnetic fields. If there are a large number of workstations at your site, you may wish to devote a special room to storing backups.

Store magnetic tapes, including 1/4 in. and 8 mm cartridges, upright. Do not store tapes on their sides, as this can deform the tape material and cause the tapes to read incorrectly.

Make sure the media is clearly labeled and, if applicable, write-protected. Choose a label-color scheme to identify such aspects of the backup as what system it is from, what level of backup (complete versus partial), what filesystem, and so forth.

To minimize the impact of a disaster at your site, such as a fire, you may want to store main copies of backups in a different building from the actual workstations. You have to balance this practice, though, with the need to have backups handy for recovering files.

If backups contain sensitive data, take the appropriate security precautions, such as placing them in a locked, secure room. Anyone can read a backup tape on a system that has the appropriate utilities.

How Long to Keep Backups

You can keep backups as long as you think you need to. In practice, few sites keep system backup tapes longer than about a year before recycling the tape for new backups. Usually, data for specific purposes and projects is backed up at specific project milestones (for example, when a project is started or finished). As site administrator, you should consult with your users to determine how long to keep filesystem backups.

With magnetic tapes, however, there are certain physical limitations. Tape gradually loses its flux (magnetism) over time. After about two years, tape can start to lose data.

For long-term storage, re-copy magnetic tapes every year to year-and-a-half to prevent data loss through deterioration. When possible, use checksum programs, such as the sum(1) utility, to make sure data hasn't deteriorated or altered in the copying process. If you want to reliably store data for several years, consider using optical disk.

Reusing Tapes

You can reuse tapes, but with wear, the quality of a tape degrades. The more important the data, the more precautions you should take, including using new tapes.

If a tape goes bad, mark it as "bad" and discard it. Write "bad" on the tape case before you throw it out so that someone doesn't accidentally try to use it. Never try to reuse an obviously bad tape. The cost of a new tape is minimal compared to the value of the data you are storing on it.