

IRIS FailSafe™ 2.0
DMF Administrator's Guide

Document Number 007-4249-001

CONTRIBUTORS

Written by Anita Manders
Illustrated by Dany Galgani
Edited by Rick Thompson
Production by Susan Gorski
Engineering contributions by Dave Caliguire, Paddy Sreenivasan

© 2000, Silicon Graphics, Inc.— All Rights Reserved

The contents of this document may not be copied or duplicated in any form, in whole or in part, without the prior written permission of Silicon Graphics, Inc.

LIMITED AND RESTRICTED RIGHTS LEGEND

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in the Rights in Data clause at FAR 52.227-14 and/or in similar or successor clauses in the FAR, or in the DOD, DOE, or NASA FAR Supplements. Unpublished rights reserved under the Copyright Laws of the United States.

Contractor/manufacturer is SGI, 1600 Amphitheatre Pkwy., Mountain View, CA 94043-1351.

Silicon Graphics, IRIS, and IRIX are registered trademarks and IRIS FailSafe, SGI, and the SGI logo are trademarks of Silicon Graphics, Inc.

ACSLs and STK are trademarks of Storage Technology Corporation. INFORMIX is a trademark of Informix Software, Inc. Netscape is a trademark of Netscape Communications Corporation. NFS is a trademark of Sun Microsystems, Inc. Oracle is a trademark of Oracle Corporation. Windows is a trademark of Microsoft Corporation.

Contents

List of Figures v

List of Tables vii

List of Examples ix

About This Guide xi

Audience xi

Structure of This Document xi

Related Documentation xii

Conventions Used in This Guide xiii

Reader Comments xiv

1. **IRIS FailSafe DMF Overview** 1
 - IRIS FailSafe DMF Monitoring 1
 - Overview of Configuring IRIS FailSafe for DMF 4
2. **Configuring IRIS FailSafe for DMF** 5
 - Required Software 5
 - Planning DMF Configuration 6
 - Tape Hardware Configuration 6
 - Tape Software Configuration 7
 - DMF Installation and Failover 10
 - Adding DMF Resource Information to the Configuration Database (CDB) 11
 - Creating a DMF Resource Type 11
 - Configuring a DMF Resource 14
 - Creating a Failover Policy for a DMF Resource Group 15
 - Creating a DMF Resource Group 15
 - Testing the DMF Resource 17
 - Testing Resource Group Failovers 18

List of Figures

Figure 1-1 Message Paths in IRIS FailSafe 3

List of Tables

Table i	IRIS FailSafe Release Notes	xiii
Table 2-1	DMF Configuration Parameters	11

List of Examples

Example 2-1	DMF Option Installation Process	11
Example 2-2	DMF Resource Type Installation	12
Example 2-3	Creating a DMF Resource Using <i>cmgr</i>	14
Example 2-4	Defining the Failover Policy	15
Example 2-5	Creating the Resource Group <i>dmf_group</i> of Type DMF	16

About This Guide

This guide provides information about how to configure IRIS FailSafe 2.0 systems with the IRIS FailSafe 2.0 Data Migration Facility (DMF) option. This option enables DMF and its resources to be failed over from one node to another when a FailSafe failover occurs. This guide is intended as a supplement to the information about configuring IRIS FailSafe that is described in the *IRIS FailSafe 2.0 Administrator's Guide*.

This guide was prepared in conjunction with the initial release of the IRIS FailSafe 2.0 DMF option and the IRIS FailSafe 1.2 release. It describes the IRIS FailSafe DMF software for DMF release 2.6.1 and higher.

Audience

This guide is written for system administrators who are responsible for configuring and administering an IRIS FailSafe system with the optional IRIS FailSafe DMF software. These system administrators must be able to customize several shell scripts and must be familiar with DMF configuration and DMF startup and shutdown procedures.

Structure of This Document

This guide contains the following chapters:

- Chapter 1, “IRIS FailSafe DMF Overview,” describes the IRIS FailSafe components that are included in the IRIS FailSafe DMF option. It also provides an overview of the steps that are required to add DMF as a highly available service to an IRIS FailSafe cluster.
- Chapter 2, “Configuring IRIS FailSafe for DMF,” explains the procedure for adding DMF as a highly available service.

Related Documentation

For DMF installation information, see the *DMF Administrator's Guide for IRIX Systems* and the *DMF Release and Installation Guide for IRIX Systems*.

Besides this guide, other documentation for the IRIS FailSafe system includes

- *IRIS FailSafe 2.0 Administrator's Guide*
- *IRIS FailSafe 2.0 Programmer's Guide*
- *IRIS FailSafe 2.0 INFORMIX Administrator's Guide*
- *IRIS FailSafe 2.0 Netscape Server Administrator's Guide*
- *IRIS FailSafe 2.0 NFS Administrator's Guide*
- *IRIS FailSafe 2.0 Oracle Administrator's Guide*
- *IRIS FailSafe 2.0 Samba Administrator's Guide*

The IRIS FailSafe reference pages are as follows:

- cmond(1M)
- crsd(1M)
- failsafe(7M)
- ha_cilog(1M)
- ha_cmsd(1M)
- ha_exec2(1M)
- ha_filelock(1M)
- ha_fileunlock(1M)
- ha_fsadm(1M)
- ha_fsd(1M)
- ha_gcd(1M)
- ha_http_ping2(1M) (IRIS FailSafe Web)
- ha_ifdadmin(1M)
- ha_ifd(1M)
- ha_ifmx2(1M) (IRIS FailSafe INFORMIX option)

- `ha_macconfig2(1M)`
- `ha_srmd(1M)`
- `ha_statd2(1M)`

Release notes are included with each IRIS FailSafe product. The names of the release notes are as follows:

Table i IRIS FailSafe Release Notes

Release Note	Product
<i>failsafe2</i>	IRIS FailSafe 2.0
<i>failsafe2_dmf</i>	IRIS FailSafe 2.0 DMF
<i>failsafe2_informix</i>	IRIS FailSafe 2.0 INFORMIX
<i>failsafe2_nfs</i>	IRIS FailSafe 2.0 NFS
<i>failsafe2_oracle</i>	IRIS FailSafe 2.0 Oracle
<i>failsafe2_samba</i>	IRIS FailSafe 2.0 Samba
<i>failsafe2_web</i>	IRIS FailSafe 2.0 Netscape

Conventions Used in This Guide

These type conventions and symbols are used in this guide:

Italics New terms, manual/book titles, command names and command line arguments, file names, directory names, resource types, variable command line arguments, and variables to be supplied by the user in examples, code, and syntax statements

Fixed-width type
Examples of command output and code

Bold fixed-width type
Commands and text that you are to type literally in response to shell and command prompts

IRIS shell prompt for the super user (*root*)

Reader Comments

If you have comments about the technical accuracy, content, or organization of this document, please tell us. Be sure to include the title and document number of the manual with your comments. (Online, the document number is located in the front matter of the manual. In printed manuals, the document number can be found on the back cover.)

You can contact us in any of the following ways:

- Send e-mail to the following address:
techpubs@sgi.com
- Use the Feedback option on the Technical Publications Library World Wide Web page:
<http://techpubs.sgi.com>
- Contact your customer service representative and ask that an incident be filled in the SGI incident tracking system.
- Send mail to the following address:
Technical Publications
SGI
1600 Amphitheatre Pkwy., M/S 535
Mountain View, California 94043-1351
- Send a fax to the attention of Technical Publications at:
+1 650 932 0801

We value your comments and will respond to them promptly.

IRIS FailSafe DMF Overview

This chapter provides information about the components that are added to the base IRIS FailSafe 2.0 product by the IRIS FailSafe 2.0 DMF option. It assumes that you are familiar with the basic components of IRIS FailSafe described in Chapter 1 of the *IRIS FailSafe 2.0 Administrator's Guide*. This chapter also lists the steps you must take to add DMF to the highly available services that are failed over on an IRIS FailSafe cluster.

The major sections in this chapter are as follows:

- “IRIS FailSafe DMF Monitoring” on page 1
- “Overview of Configuring IRIS FailSafe for DMF” on page 4

IRIS FailSafe DMF Monitoring

The IRIS FailSafe DMF option adds DMF daemon monitoring support to the IRIS FailSafe base software. The DMF monitor script monitors the DMF daemon (*dmdaemon*). The script periodically makes status requests to the daemon to verify that it is up and running. If the monitor script detects a failure, it reports a local monitoring failure to FailSafe, which logs the failure and sends a message to the system console. A failure of the DMF subsystem does **not** cause a failover to occur. If the host that is running FailSafe DMF crashes, DMF fails over to another host along with its filesystems.

There are several scripts that IRIS FailSafe uses to start, stop, and monitor DMF. These scripts are as follows:

<i>start</i>	Starts the DMF daemon
<i>stop</i>	Stops DMF on this node
<i>probe</i>	Tests to see if DMF can be started on this node
<i>monitor</i>	Extended test to see if DMF is running on this node
<i>exclusive</i>	Tests to see if DMF is already running on this node
<i>restart</i>	Determines if the DMF daemon should be restarted

If the monitor script detects a failure, it will report a local monitoring failure to FailSafe, and FailSafe will take the appropriate action. Figure 1-1 shows an example of the message paths in IRIS FailSafe and the appropriate action. Figure 1-1 also shows the interaction between the resource action scripts and the FailSafe agents (ha_ifd, ha_ifmx2). The DMF resource action scripts do not interact with any FailSafe agent directly, except for the ha_srmd process.

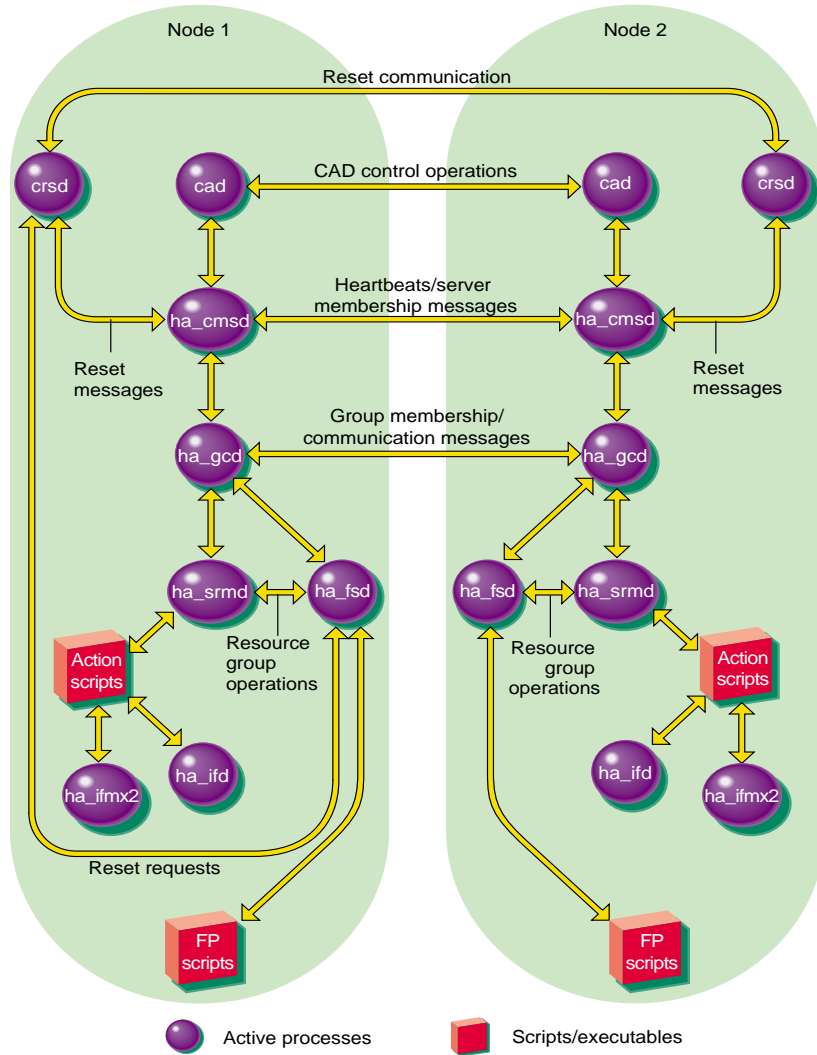


Figure 1-1 Message Paths in IRIS FailSafe

Overview of Configuring IRIS FailSafe for DMF

To configure an IRIS FailSafe cluster for failover of DMF, follow these steps:

1. Install, configure, and test the base IRIS FailSafe software as described in the *IRIS FailSafe 2.0 Administrator's Guide*.
2. Install the latest IRIS FailSafe 2.0 rollup patch software. To install the IRIS FailSafe 2.0 patch in the cluster, please read the patch release notes.
3. Install the FailSafe 2.0 DMF option for IRIX software on each host that will run the option in the cluster and any additional software if required. See the section "Required Software" in Chapter 2.
4. Install DMF on each host in the cluster that is to run the option. See the *DMF Release and Installation Guide for IRIX Systems*.
5. If migrating data to tape, install TMF on each host that is to run the FailSafe 2.0 DMF option.
6. If migrating to tape, configure the tape hardware and the FailSafe 2.0 DMF tape software. See the sections "Tape Hardware Configuration" and "Tape Software Configuration" in Chapter 2.
7. Add the DMF resource type, resource attribute, and resource information to the configuration database (CDB) file. See the section "Adding DMF Resource Information to the Configuration Database (CDB)" in Chapter 2.
8. Determine how to configure the DMF filesystems. See the section "Planning DMF Configuration" in Chapter 2.
9. Test the DMF failover. See the section "Testing the DMF Resource" in Chapter 2.

Configuring IRIS FailSafe for DMF

This chapter provides information about configuring the IRIS FailSafe DMF option for use on an IRIS FailSafe system. The major sections in this chapter are as follows:

- “Required Software” on page 5
- “Planning DMF Configuration” on page 6
- “Tape Hardware Configuration” on page 6
- “Tape Software Configuration” on page 6
- “DMF Installation and Failover” on page 10
- “Adding DMF Resource Information to the Configuration Database (CDB)” on page 10
- “Testing the DMF Resource” on page 17

Required Software

The required software for IRIS FailSafe 2.0 DMF failover is as follows:

- DMF software, release 2.6.1 or higher
See the *DMF Administrator's Guide for IRIX Systems* for more information about DMF.
- Base IRIS FailSafe 2.0 software and the latest IRIS FailSafe 2.0 rollup patch
See the section “Installing the IRIS FailSafe Software” in Chapter 2 of the *IRIS FailSafe 2.0 Administrator's Guide* for a complete list of the required base software.
- IRIS FailSafe DMF software, as follows:
 - The *IRIS FailSafe 2.0 DMF Administrator's Guide* subsystem is *failsafe2_dmf.books.book_AG*.
 - The IRIS FailSafe 2.0 DMF release notes subsystem is *failsafe2_dmf.man.relnotes*.
 - The base software subsystem is *failsafe2_dmf.sw.base*.

- If the offline storage media for migrated data is tape, the IRIX Tape Management Facility (TMF) must be installed on each host that runs the IRIS FailSafe 2.0 DMF option. You must also create a tape configuration file on each host that runs the option. For more information, see the section “Tape Software Configuration.”

Planning DMF Configuration

The DMF databases, log files, journal files, and user filesystems that are managed by DMF must be XFS filesystems or XLV logical volumes and they must exist on a shared disk within the cluster. The user filesystems must be mounted using the *dmi* mount option. The user filesystems are normally created as NFS filesystems so that they can be mounted and accessed remotely.

The filesystems that contain DMF databases, log files, journal files, and user filesystems and that are managed by DMF must be defined as filesystem and volume resources. For more information, see Chapter 2 and Chapter 5 in the *IRIS FailSafe 2.0 Administrator's Guide*.

Tape Hardware Configuration

The FailSafe 2.0 DMF option runs only with Storage Technology Corporation (STK) libraries that are managed by the Automated Cartridge System Library Software (ACSLs). Each host in the cluster that runs the FailSafe 2.0 DMF option is connected to a separate set of drives of the same type within a common STK library. This configuration implies that each drive has access to the same tapes within the library.

Tape Software Configuration

The FailSafe 2.0 DMF option works in conjunction with the IRIX Tape Management Facility (TMF). DMF and TMF must be installed on each node that runs the FailSafe 2.0 DMF option. TMF is used as the mounting service for tapes used by DMF and must be included along with DMF.

You must create a tape configuration file */etc/config/ha_dismnt.config* that defines the tape library and drives attached to hosts within the cluster. This file identifies the tape drives from which FailSafe DMF will eject tapes before starting DMF.

For example, if DMF was running on host A and was using the tape drives with vendor addresses of 0001 and 0002 at the time of the failover, you must ensure that the tapes in those drives were ejected before you restart DMF on another host. If DMF was failed over from host A to host B, host B should eject the tapes in drives 0001 and 0002 before you start DMF, so DMF has access to the migrated data on those tapes. You can also have host B eject the tapes from the tape drives to which it is attached before you start DMF. This action ensures that the tape drives that DMF will use from host B are available before DMF is started.

The tape configuration file must exist on each host that runs FailSafe 2.0 DMF with TMF. The configuration file contains the name of the network server associated with the library, and a list of tape drive vendor addresses.

The syntax for the configuration file is the name of the server followed by a list of drive vendor addresses as follows:

```
<tape library server name>
<vendor address for drive 1>
<vendor address for drive 2>
.
.
.
```

The entries in the tape configuration file `/etc/config/ha_dismnt.config` are derived from information in the TMF configuration file for a host. The following example shows the loader and device definitions from TMF configuration files for hosts A and B. It then gives the associated FailSafe DMF tape configuration file that would be created on each host defining the server and vendor addresses for each drive, as follows:

HOST A TMF configuration file -

```
LOADER
    name = wolfy ,
    type = STKACS ,
    status = DOWN ,
    mode = ATTENDED ,
    message_path_to_loader = NETWORK ,
    server = wolfcreek ,
    scratch_volume_label_type = NONE ,
```

```
queue_time = 15 ,  
verify_non_label_vsn = NO ,  
message_route_masks = (IRIX) ,  
loader_ring_status = IGNORE
```

DEVICE

```
name = t3 ,  
device_group_name = CART ,  
file = /hw/tape/tps7d5 ,  
status = DOWN ,  
loader = wolfy ,  
vendor_address = (0,0,1,2)
```

DEVICE

```
name = t4 ,  
device_group_name = CART ,  
file = /hw/tape/tps7d3 ,  
status = DOWN ,  
loader = wolfy ,  
vendor_address = (0,0,1,3)
```

HOST B TMF configuration file -

LOADER

```
name = wolfy ,  
type = STKACS ,  
status = DOWN ,  
mode = ATTENDED ,  
message_path_to_loader = NETWORK ,  
server = wolfcreek ,  
scratch_volume_label_type = NONE ,  
queue_time = 15 ,  
verify_non_label_vsn = NO ,
```

```
message_route_masks = (IRIX) ,  
loader_ring_status = IGNORE
```

DEVICE

```
name      = t5 ,  
device_group_name = CART ,  
file      = /hw/tape/tps5d5 ,  
status    = DOWN ,  
loader    = wolfy ,  
vendor_address = (0,0,1,5)
```

DEVICE

```
name      = t6 ,  
device_group_name = CART ,  
file      = /hw/tape/tps5d6 ,  
status    = DOWN ,  
loader    = wolfy ,  
vendor_address = (0,0,1,6)
```

In the previous example, the loader named *wolfy* has server *wolfcreek* associated with it. There are two tape drives in the library attached to each host. The vendor addresses for the drives are 0012, 0013, 0015, and 0016.

The tape configuration file */etc/config/ha_dismnt.config* on each host appears as follows:

```
wolfcreek  
0 0 1 2  
0 0 1 3  
0 0 1 5  
0 0 1 6
```

DMF Installation and Failover

DMF will be installed on each host in the cluster that runs the FailSafe 2.0 DMF option, and if you are migrating files to tape, TMF will also be installed. DMF only runs on one host within the cluster at a time. TMF runs on each host that has the FailSafe 2.0 DMF option.

The DMF databases, logfiles, journal files, and user filesystems are all created on storage media that is shared between all of the hosts that run the FailSafe 2.0 DMF option within the cluster.

As indicated before, the failure of DMF itself will **not** cause a failover to occur. The failover of DMF and its resources should only occur in the case of catastrophic system failure on the host.

When DMF and its resources failover to another host, the FailSafe DMF option verifies that the database, logfile, and journal filesystems are available to DMF before it starts DMF. The option also checks to see if there is a tape configuration file present. If there is, the option requests ACSLS to unload all tape drives that may have been in use by DMF at the time of the failover, and all tape drives that DMF may need after restarting. The DMF daemon is then started on new host.

Adding DMF Resource Information to the Configuration Database (CDB)

This section describes procedures that show you how to create a DMF resource type, resource, resource group, and configuration database that includes DMF configuration information, how to create a failover policy for a DMF resource group, and how to test the DMF resource. These procedures assume that a CDB that does not include DMF has already been created, installed, and tested as described in the *IRIS FailSafe 2.0 Administrator's Guide*.

Creating a DMF Resource Type

This subsection assumes that you are already familiar with the concepts of resource types. The DMF resource type defines the following resource attributes. See Table 2-1 for the DMF resource name and configuration parameter.

Table 2-1 DMF Configuration Parameters

Resource Parameters	Comments
<i>resource-name</i>	Defines the name of the DMF resource; for example <i>dmf</i> .
resource attribute	
<i>daemon-path</i>	The location of the DMF daemon binary; for example, <i>/etc/dmf/daemon/etc/dmdaemon</i> .

The DMF resource type is automatically created at cluster creation time. If this automatic resource creation fails, the administrator must create the resource type before a DMF resource is created. The DMF resource type must be installed if you want to add a DMF resource to a cluster that was created before the DMF software was installed.

Example 2-1 DMF Option Installation Process

```

Inst> 1 *
View: distribution
Status: N=new, U=upgrade, S=same, D=downgrade
Selection: i=install, r=remove, k=keep

Subsystem Types [bdrpc]: b=reBoot needed, d=Default, r=Required,
p=patch, c=Client only

i U failsafe2_dmf.books.book_AG [d] 0 FailSafe DMF Plugin 2.0
Administrator's Guide
i U failsafe2_dmf.man.relnotes 0 FailSafe DMF Plugin 2.0 release notes
i U failsafe2_dmf.sw.base [d] 0 FailSafe DMF Plugin 2.0 base software

Disk space summary (Kbytes):
           /      /DMF_cm1      /apps
Current free space          2272380      4422412      5656968
- Selections net change           0           0           0
- Temporary inst overhead       1296+           0           0
= Minimum free during install   2271084      4422412      5656968
    
```

```
Final projected free space          2272380    4422412    5656968
```

```
Inst> g
Pre-installation check ..    8%
Checking space requirements .. 16%
Installing/removing files .. 16%
Upgrading selected failsafe2_dmf.books subsystems
Installing/removing files .. 65%
Upgrading selected failsafe2_dmf.man subsystems
Installing/removing files .. 72%
Upgrading selected failsafe2_dmf.sw subsystems
Installing/removing files .. 94%
Running exit-commands .. 99%
Checking dependencies .. 100% Done.
Installations and removals were successful.
You may continue with installations or quit now.
```

```
Inst> quit
```

You can use one of the following methods to create the DMF resource type:

- Run cluster manager (*cmgr*) and manually create the resource type. For more information, see the *IRIS FailSafe 2.0 Administrator's Guide*.
- Run cluster manager (*cmgr*) and install the resource type, as shown in the following example.

Example 2-2 DMF Resource Type Installation

```
cmgr> show resource_types installed

NFS
template
Netscape_web
statd
Oracle_DB
MAC_address
IP_address
INFORMIX_DB
NFS
filesystem
volume

cmgr> install resource_type DMF in cluster eagan
```

```
cmgr> show resource_type DMF
```

```
Name: DMF
  Predefined: true
  Order: 100
  Restart mode: 0
  Restart count: 0

  Action name: probe
    Executable: /var/cluster/ha/resource_types/DMF/probe
    Maximum execution time: 50000ms
    Monitoring interval: 0ms
    Start monitoring time: 0ms
  Action name: stop
    Executable: /var/cluster/ha/resource_types/DMF/stop
    Maximum execution time: 40000ms
    Monitoring interval: 0ms
    Start monitoring time: 0ms
  Action name: exclusive
    Executable: /var/cluster/ha/resource_types/DMF/exclusive
    Maximum execution time: 50000ms
    Monitoring interval: 0ms
    Start monitoring time: 0ms
  Action name: start
    Executable: /var/cluster/ha/resource_types/DMF/start
    Maximum execution time: 40000ms
    Monitoring interval: 0ms
    Start monitoring time: 0ms
  Action name: restart
    Executable: /var/cluster/ha/resource_types/DMF/restart
    Maximum execution time: 40000ms
    Monitoring interval: 0ms
    Start monitoring time: 0ms
  Action name: monitor
    Executable: /var/cluster/ha/resource_types/DMF/monitor
    Maximum execution time: 40000ms
    Monitoring interval: 20000ms
    Start monitoring time: 50000ms

  Type specific attribute: daemon-path
    Data type: string
    Default value: /etc/dmf/dmbase/etc/dmdaemon

  No resource type dependencies
```

- Instead of using cluster manager (*cmgr*) to create the DMF resource type in cluster *eagan*, you can use the IRIS FailSafe 2.0 **Load Resource Type** GUI task to load the DMF resource type in the cluster *eagan*.

Configuring a DMF Resource

After you have defined the resource type, the administrator must define a DMF resource based on the resource type. A resource requires a unique resource name (for example, the DMF resource type is the *dmf* instance name). Then, the administrator must supply the resource parameters. To create the resource, either use the cluster manager (*cmgr*), the *cmgr* template scripts, or the GUI.

Example 2-3 Creating a DMF Resource Using *cmgr*

```
cm2> /usr/cluster/bin/cluster_mgr
Welcome to IRIS FailSafe Cluster Manager Command-Line Interface

cmgr> define resource dmf of resource_type DMF in cluster eagan
Enter commands, when finished enter either "done" or "cancel"

Type specific attributes to create with set command:

Type Specific Attributes - 1: daemon-path

No resource type dependencies to add

resource dmf ? done

cmgr>
```

Creating a Failover Policy for a DMF Resource Group

After you have defined a resource instance of resource type DMF, you can define the failover policy for the resource group that contains the resource. To create the failover policy, use the cluster manager (*cmgr*), the *cmgr* template scripts, or the GUI. The following example shows how to define the failover policy.

Example 2-4 Defining the Failover Policy

```
cmgr> define failover_policy manual
Enter commands, when finished enter either "done" or "cancel"
```

```
failover_policy manual ? set attribute to Auto_Failback
failover_policy manual ? set script to ordered
failover_policy manual ? set domain to cm1 cm2
failover_policy manual ? done
Successfully defined failover policy manual
```

Creating a DMF Resource Group

To create a resource group, you must first become familiar with the terms and concepts of FailSafe. A DMF resource group must include a resource instance of DMF along with filesystem and volume resource instances. The filesystem and volume resources have been previously created and are DMF database, spool, journal, and user filesystems. You must also indicate what the failover policy is at the time you create the group. To create the resource group, use the cluster manager (*cmgr*), the *cmgr* template scripts, or the GUI.

The following example shows the creation of the resource group *dmf_group*. The filesystems */dmf_home*, */dmfjournals*, and */dmf1* are DMF filesystems. The */dmf_home* filesystem contains the DMF databases and spool directories. The */dmfjournals* filesystem contains the DMF journal files. The */dmf1* filesystem is a user filesystem that DMF manages.

Example 2-5 Creating the Resource Group *dmf_group* of Type DMF

```
cmgr> define resource_group dmf_group in cluster eagan
Enter commands, when finished enter either "done" or "cancel"

resource_group dmf_group ? set failover_policy to manual
resource_group dmf_group ? add resource dmf of resource_type DMF
resource_group dmf_group ? add resource /dmf1 of resource_type
filesystem
resource_group dmf_group ? add resource /dmfjournals of resource_type
filesystem
resource_group dmf_group ? add resource /dmf_home of resource_type
filesystem
resource_group dmf_group ? add resource dmfl of resource_type volume
resource_group dmf_group ? add resource dmfjournals of resource_type
volume
resource_group dmf_group ? add resource dmf_home of resource_type
volume
resource_group dmf_group ? done
Successfully defined resource group dmf_group

cmgr> show resource_group dmf_group

Resource Group: dmf_group
Cluster: eagan
Failover Policy: manual

Resources:
dmf      (type: DMF)
/dmf_home (type: filesystem)
/dmfjournals (type: filesystem)
/dmf1    (type: filesystem)
dmfl     (type: volume)
dmfjournals (type: volume)
dmf_home (type: volume)
```

Testing the DMF Resource

To ensure that the DMF resource has been correctly configured, you can test individual actions by executing the scripts. Each script, located at `/var/cluster/ha/resource_types/DMF`, requires two arguments, an input file and an output file. The contents of these files are the resource names. The scripts will display either a 0 if they are successfully executed, or display a positive integer that indicates the error type. For more information on error codes, see the *IRIS FailSafe 2.0 Programmer's Guide*. The script output is logged to the file `/var/cluster/ha/log/script_hostname`. This file should be checked after testing each script to verify that the script worked properly.

You can test each script by starting with the following commands:

```
$ cd /var/cluster/ha/resource_types/DMF
$ echo "dmf" > /tmp/ipfile
```

where *dmf* is the name of the resource instance of resource type DMF.

You can then execute each script with the following command:

```
$ ./script-name /tmp/ipfile /tmp/opfile
```

where *script-name* is one of the following names:

<i>start</i>	Starts the DMF daemon
<i>stop</i>	Stops DMF on this node
<i>probe</i>	Tests to see if DMF can be started on this node
<i>monitor</i>	Extended test to see if DMF is running on this node
<i>exclusive</i>	Tests to see if DMF is already running on this node
<i>restart</i>	Determines if the DMF daemon should be restarted

After executing each script, verify that it worked correctly by verifying the output it generates in the `/var/cluster/ha/log/script_hostname` file.

To view the individual script actions, you must edit the script and add `"set -x"` in the *action* function.

Testing Resource Group Failovers

You can test the failover policy by using either *cmgr* or the FailSafe GUI to move the resource group to another node in the cluster. To ensure that the resource group correctly failed over, use *cmgr* or the GUI to display the resource group states. The following example uses *cmgr* to test the failover policy for resource group *dmf_group* in cluster *eagan*:

```
cmgr> admin offline resource_group dmf_group in cluster eagan
cmgr>
cmgr> admin online resource_group dmf_group in cluster eagan
cmgr>
cmgr> admin move resource_group dmf_group to node cm2
cmgr>
```

After testing, move resource group *dmf_group* to another node, verify that the filesystems have been moved over and are mounted properly on the node, and verify that DMF is up and running on the node.