

IRIS FailSafe™ Version 2  
DMF Administrator's Guide

Document Number 007-4249-002

---

#### CONTRIBUTORS

Written by Anita Manders, Steven Levine

Illustrated by Dany Galgani

Edited by Rick Thompson

Production by Bryan Perkins

Engineering contributions by Dave Caliguire, Kevan Rehm, Paddy Sreenivasan

---

#### COPYRIGHT

© 2000, 2001 Silicon Graphics, Inc. All rights reserved; provided portions may be copyright in third parties, as indicated elsewhere herein. No permission is granted to copy, distribute, or create derivative works from the contents of this electronic documentation in any manner, in whole or in part, without the prior written permission of Silicon Graphics, Inc.

#### LIMITED RIGHTS LEGEND

The electronic (software) version of this document was developed at private expense; if acquired under an agreement with the USA government or any contractor thereto, it is acquired as "commercial computer software" subject to the provisions of its applicable license agreement, as specified in (a) 48 CFR 12.212 of the FAR; or, if acquired for Department of Defense units, (b) 48 CFR 227-7202 of the DoD FAR Supplement; or sections succeeding thereto. Contractor/manufacturer is Silicon Graphics, Inc., 1600 Amphitheatre Pkwy 2E, Mountain View, CA 94043-1351.

---

#### TRADEMARKS AND ATTRIBUTIONS

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

INFORMIX is a trademark of Informix Software, Inc. Netscape is a trademark of Netscape Communications Corporation. Oracle is a trademark of Oracle Corporation. Windows is a trademark of Microsoft Corporation.

---

## New Features in This Guide

This version of the *IRIS FailSafe Version 2 DMF Administrator's Guide* supports the IRIS FailSafe 2.1 release. There are major operational differences between the FailSafe DMF agent for FailSafe 2.0 and the FailSafe DMF agent for FailSafe 2.1; this manual has been reworked to account for those changes.



---

## Record of Revision

<b>Version</b>	<b>Description</b>
001	January 2000 Incorporates information for the IRIS FailSafe 2.0 release.
002	August 2001 Incorporates information for the IRIS FailSafe 2.1 release.



---

# Contents

<b>Figures</b> . . . . .	ix
<b>Tables</b> . . . . .	xi
<b>Examples</b> . . . . .	.xiii
<b>About This Guide.</b> . . . . .	xv
Audience . . . . .	xv
Structure of This Document . . . . .	xv
Related Documentation . . . . .	.xvi
Obtaining Publications . . . . .	xviii
Conventions Used in This Guide . . . . .	xviii
Reader Comments . . . . .	xviii
<b>1. IRIS FailSafe DMF Overview</b> . . . . .	1
IRIS FailSafe DMF Monitoring . . . . .	1
Overview of Configuring IRIS FailSafe for DMF . . . . .	3
<b>2. Configuring IRIS FailSafe for DMF</b> . . . . .	5
Required Software. . . . .	5
FailSafe 2.1 DMF Configuration . . . . .	6
The DMF Configuration Flag . . . . .	6
The DMF Administrative Filesystems and Directories . . . . .	7
Configuring the DMF Administrative Filesystems as Shared XLV Filesystems . . . . .	8
Configuring the DMF Administrative Filesystems as CXFS filesystems . . . . .	9
The DMF-Managed User Filesystems . . . . .	9
FailSafe TMF Resource Configuration . . . . .	11

- Adding DMF Resource Information to the Configuration Database (CDB) . . . . . 11
  - Creating a DMF Resource Type . . . . . 11
  - Configuring a DMF Resource . . . . . 13
  - Creating a Failover Policy for a DMF Resource Group . . . . . 14
  - Creating a DMF Resource Group . . . . . 15
- DMF Action Scripts . . . . . 17
- Testing the DMF Resource . . . . . 17
- Index.** . . . . . 19



---

## Figures

<b>Figure 1-1</b>	Message Paths in IRIS FailSafe in a two-node cluster . . . . .	2
-------------------	--	---



---

## Tables

<b>Table i</b>	IRIS FailSafe Release Notes . . . . .	xvii
<b>Table 2-1</b>	DMF Administrative Filesystems and Directories . . . . .	7



---

## Examples

<b>Example 2-1</b>	DMF Resource Type Installation . . . . .	12
<b>Example 2-2</b>	Creating a DMF Resource Using <code>cmgr</code> . . . . .	13
<b>Example 2-3</b>	Defining the Failover Policy . . . . .	14
<b>Example 2-4</b>	Creating the Resource Group <code>dmfcxfs</code> of Type DMF . . . . .	15



---

## About This Guide

This guide provides information about how to configure IRIS FailSafe 2.1 systems with the IRIS FailSafe 2.1 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 Version 2 Administrator's Guide*.

This guide was prepared in conjunction with Release 2.1 of the IRIS FailSafe DMF option and the IRIS FailSafe 2.1 release. It describes the IRIS FailSafe DMF software for DMF release 2.6.3.3 and higher. This guide uses *FailSafe* as an abbreviation for *IRIS FailSafe*.

## 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 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*.

For CXFS installation information, see the *CXFS Software Installation and Administration Guide*.

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

- *IRIS FailSafe Version 2 Administrator's Guide*
- *IRIS FailSafe Version 2 Programmer's Guide*
- *IRIS FailSafe 2.0 INFORMIX Administrator's Guide*
- *IRIS FailSafe 2.0 Netscape Server Administrator's Guide*
- *IRIS FailSafe Version 2 NFS Administrator's Guide*
- *IRIS FailSafe 2.0 Oracle Administrator's Guide*
- *IRIS FailSafe Version 2 Samba Administrator's Guide*
- *IRIS FailSafe Version 2 TMF Administrator's Guide*

The IRIS FailSafe man pages are as follows:

- `cdbBackup(1M)`
- `cdbRestore(1M)`
- `cluster_mgr(1M)`
- `crsd(1M)`
- `failsafe(7M)`
- `fs2d(1M)`
- `ha_cilog(1M)`
- `ha_cmds(1M)`
- `ha_exec2(1M)`
- `ha_fsadm(1M)`
- `ha_fsd(1M)`
- `ha_gcd(1M)`



- `ha_http_ping2(1M)` (IRIS FailSafe Netscape Web option)
- `ha_ifd(1M)`
- `ha_ifdadmin(1M)`
- `ha_ifmx2(1M)` (IRIS FailSafe INFORMIX option)
- `ha_macconfig2(1M)`
- `ha_srmd(1M)`
- `ha_statd2(1M)`
- `haStatus(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

<b>Release Note</b>	<b>Product</b>
<code>cluster_admin</code>	Cluster administration services
<code>cluster_control</code>	Cluster node control services
<code>cluster_services</code>	Cluster services
<code>failsafe2</code>	IRIS FailSafe 2.1 release
<code>failsafe2_dmf</code>	FailSafe/DMF
<code>failsafe2_informix</code>	FailSafe/INFORMIX
<code>failsafe2_nfs</code>	FailSafe/NFS
<code>failsafe2_oracle</code>	FailSafe/Oracle
<code>failsafe2_samba</code>	FailSafe/Samba
<code>failsafe2_tmf</code>	FailSafe/TMF
<code>failsafe2_web</code>	FailSafe/Netscape web
<i>patch_number</i>	FailSafe patch release

## Obtaining Publications

To obtain SGI documentation, go to the SGI Technical Publications Library at:

<http://techpubs.sgi.com>

## Conventions Used in This Guide

These type conventions and symbols are used in this guide:

<i>Italics</i>	New terms, manual/book titles, variable command line arguments, and variables to be supplied by the user in examples, code, and syntax statements
Fixed-width type	Command names and command line arguments, file names, directory names, resource types, and examples of command output and code
<b>Bold fixed-width type</b>	Commands and text that you are to type literally in response to shell and command prompts
#	IRIX shell prompt for the super user ( <i>root</i> )

## 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](mailto: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 2.1 product by the IRIS FailSafe 2.1 DMF option. It assumes that you are familiar with the basic components of IRIS FailSafe described in Chapter 1 of the *IRIS FailSafe Version 2 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 3

### 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 and FailSafe will take the appropriate action. If the host that is running FailSafe DMF crashes, DMF fails over to another host along with its filesystems.

IRIS FailSafe supports up to eight nodes in a cluster. Figure 1-1 shows an example of the message paths in IRIS FailSafe in a two-node cluster. 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.

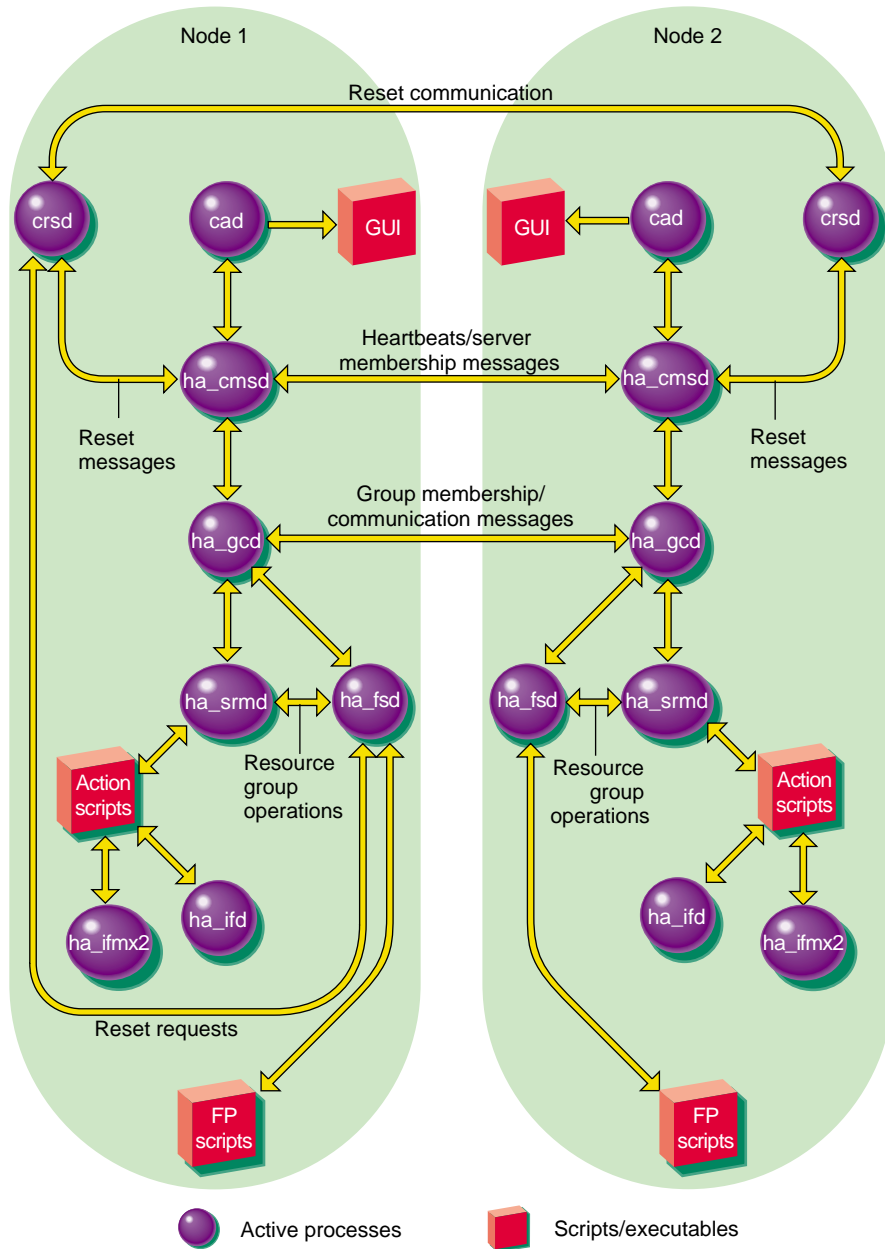


Figure 1-1 Message Paths in IRIS FailSafe in a two-node cluster

## 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 Version 2 Administrator's Guide*.
2. Install the FailSafe 2.1 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.
3. Install DMF on each host in the cluster that is to run the option. See the *DMF Release and Installation Guide for IRIX Systems*.
4. If files are being migrated to offline tape storage in a tape library and the tape management software being used to manage this tape storage is the IRIX Tape Management Facility (TMF), then follow these steps:
  - a. Install and configure TMF on each host that is to run the FailSafe 2.1 DMF option. See *IRIX TMF Release and Installation Guide*.
  - b. Install and configure the TMF 2.1 FailSafe option on each host that is to run the FailSafe 2.1 DMF option. See the *IRIS FailSafe Version 2 TMF Administrator's Guide*.
5. Configure DMF.
6. Add the DMF resource type, resource attributes, and resource information to the configuration database (CDB) file.
7. 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
- “FailSafe 2.1 DMF Configuration” on page 6
- “Adding DMF Resource Information to the Configuration Database (CDB)” on page 11
- “DMF Action Scripts” on page 17
- “Testing the DMF Resource” on page 17

### Required Software

The required software for IRIS FailSafe 2.1 DMF failover is as follows:

- DMF software, release 2.6.3.3 or higher  
See the *DMF Administrator’s Guide for IRIX Systems* for more information about DMF.
- Base IRIS FailSafe 2.1 software  
If you are going to configure the DMF administrative filesystems or DMF-managed filesystems as CXFS filesystems, you must be running IRIX 6.5.13f or later, or, alternately, you must be running IRIX 6.5.10f, 6.5.11f, or 6.5.12f with patch 4264.
- IRIS FailSafe DMF software, as follows:
  - The *IRIS FailSafe Version 2 DMF Administrator’s Guide* subsystem is `failsafe2_dmf.books.FailSafe2DMF_AG`.
  - The IRIS FailSafe 2.1 DMF release notes subsystem is `failsafe2_dmf.man.relnotes`.
  - The base software subsystem is `failsafe2_dmf.sw.base`.

- If files are being migrated to offline tape storage in a tape library and the tape management software being used to manage this tape storage is the IRIS Tape Management Facility (TMF), then TMF release 1.3.2.0 or later must be installed on each host; see *IRIX TMF Release and Installation Guide*. The IRIS FailSafe TMF agent must also be installed and configured on each host that is running DMF/TMF; for more information on the installation and configuration of the IRIS FailSafe TMF agent, see the *IRIS FailSafe Version 2 TMF Administrator's Guide*.

When running TMF, you must be running IRIX 6.5.12 or later. Alternately, you can run the following releases of IRIX with the indicated patches:

IRIX 6.5.10m	patch 4210
IRIX 6.5.10f	patch 4211
IRIX 6.5.11m	patch 4187
IRIX 6.5.11f	patch 4209

## FailSafe 2.1 DMF Configuration

The IRIS FailSafe DMF agent requires that you configure the following:

- The DMF configuration flag
- The DMF administrative filesystems and directories
- The DMF-managed user filesystems

If you are using a DMF Tape MSP to migrate user files to tape, and if you will be using TMF as the tape mounting service, then you will also need to configure:

- FailSafe TMF resources

These topics are discussed in the following sections.

### The DMF Configuration Flag

In a FailSafe environment, DMF should be started by FailSafe itself and should not be started automatically during the boot process. After the DMF package has been installed on each node in the FailSafe cluster, execute the following command on each node to determine whether DMF has been configured to start automatically:

```
# /etc/chkconfig |grep dmf
          dmf                on
```

If the `dmf` value exists and is set to `on`, issue the following command to ensure that DMF is started only by FailSafe:

```
# /etc/chkconfig dmf off
```

## The DMF Administrative Filesystems and Directories

Running DMF requires a set of administrative filesystems and directories to be configured. DMF cannot start unless all of these filesystems and directories are first mounted and available. They are defined in the DMF configuration file. Table 2-1 lists the DMF administrative filesystems and directories:

**Table 2-1** DMF Administrative Filesystems and Directories

Filesystem	Attribute	Description
HOME_DIR	Mandatory	Used for DMF databases
JOURNAL_DIR	Mandatory	Used for DMF database journals
SPOOL_DIR	Mandatory	Used for DMF log files
MOVE_FS	Optional	Used for moving files between MSPs
CACHE_DIR	Optional	Used by a tape MSP as a cache for merging data from sparse tapes to new
FTP_DIRECTORY	Optional	Used by a FTP MSP to store files
STORE_DIRECTORY	Optional	Used by a disk MSP to store files

In the above table, a file noted as mandatory must be defined by all users of DMF. A file noted as optional is needed only by users of certain MSP types.

In addition, the working directory used by the `dmaudit` command must also be available when DMF starts. The directory is configured by running the `dmaudit` command and selecting the `<workdir>` item in the `<config>` menu.

You can configure the DMF administrative filesystems as XLV logical volumes or as CXFS filesystems. In either case, you must configure the DMF resource to be dependent

on the administrative filesystems, since the administrative filesystems must be present before DMF starts.

If you use XLV filesystems, you must define them as filesystem and volume resources and make them part of the resource group that contains the DMF resource. Failover of these resources is a fast and stable process; the filesystems are recovered quickly on a failover. The procedure for configuring the DMF administrative filesystems as XLV filesystems in a FailSafe environment is provided in “Configuring the DMF Administrative Filesystems as Shared XLV Filesystems” on page 8.

If you use CXFS filesystems, you must create a CXFS resource for each of the filesystems and add each CXFS resource to the resource group that contains the DMF resource. On failover, CXFS must recover the administrative filesystems before they are accessible. If there are many other CXFS filesystems, recovery could take many minutes. There is no way to predict or set the order of recovery and the DMF filesystems may be some of the last filesystems to be recovered. The procedure for configuring the DMF administrative filesystems as CXFS filesystems in a FailSafe environment is provided in “Configuring the DMF Administrative Filesystems as CXFS filesystems” on page 9.

### **Configuring the DMF Administrative Filesystems as Shared XLV Filesystems**

To configure the DMF administrative filesystems as XLV filesystems, follow these steps:

1. Ensure that the DMF configuration is identical on all hosts.
2. Create the DMF administrative filesystems on shared disks as XLV filesystems.
3. Create the `filesystem` and `volume` FailSafe resources for each of those filesystems.
4. Add a dependency in each `filesystem` resource on the `volume` resource corresponding to that filesystem. This guarantees that FailSafe will not try to mount the filesystems until the volume labels have first been updated by the volume resource.
5. Create a DMF resource and create dependencies in the DMF resource on each of the filesystem resources that you created. This ensures that DMF will not start until they are all mounted.
6. Create the DMF resource group. For information on what a DMF resource group must include, see “Creating a DMF Resource Group” on page 15.

See “Adding DMF Resource Information to the Configuration Database (CDB)” on page 11 for more detailed information on creating a DMF resource type, a DMF resource, a DMF resource group, and a failover policy for a DMF resource group.

### Configuring the DMF Administrative Filesystems as CXFS filesystems

As indicated previously, DMF cannot start until the DMF administrative filesystems are available. If they are CXFS filesystems, CXFS must recover them before they are accessible.

To configure DMF filesystems as CXFS filesystems, follow these steps:

1. Ensure that the DMF configuration is identical on all hosts.
2. Create the DMF administrative filesystems as CXFS filesystems.
3. Create a CXFS resource for each filesystem. When you create a CXFS resource for a DMF administrative filesystem, be sure to configure the `relocate-mds` attribute to `off`, since DMF does not require the metadata server to fail over with the filesystem.
4. Create a DMF resource, and create dependencies in the DMF resource on each of the CXFS resources. This ensures that DMF will not start until these CXFS resources (filesystems) have been recovered and are available for DMF.
5. Create the DMF resource group. For information on what a DMF resource group must include, see “Creating a DMF Resource Group” on page 15.

See “Adding DMF Resource Information to the Configuration Database (CDB)” on page 11 for more detailed information on creating a DMF resource type, a DMF resource, a DMF resource group, and a failover policy for a DMF resource group.

### The DMF-Managed User Filesystems

As for the DMF administrative filesystems, you can configure the DMF-managed user filesystems as XLV volumes or as CXFS filesystems in a FailSafe environment. Note that for DMF-managed user filesystems, it is not necessary to create dependencies from the DMF resource to the filesystem resource since it is permissible for DMF to start before these filesystems are mounted.

To configure the DMF-managed user filesystems as XLV filesystems, follow these steps:

1. Create the `filesystem` and `volume` FailSafe resources for each of the filesystems.
2. Add a dependency in each filesystem resource on the volume resource corresponding to that filesystem. Remember to include the `dmi mount` option when you create each of the filesystem resources.
3. Add each of these resources to the resource group that contains the DMF resource.

To configure the DMF-managed user filesystems as CXFS filesystems, follow these steps:

1. When you create these filesystems in your CXFS cluster, make sure that you include the `dmi` option as a mount option for each filesystem.
2. Create a CXFS resource for each of these filesystems.

When you create a CXFS resource for DMF-managed user filesystem, be sure to configure the `relocate-mds` attribute to `on`. This differs from the configuration of DMF administrative CXFS filesystems, since in this case it is imperative that the metadata server fails over along with the filesystem.

3. Add each of these resources to the resource group that contains the DMF resource.

Whenever a CXFS FailSafe resource with the `relocate-mds` attribute set to `on` is started on a new node, it first checks to see if its filesystem is already mounted and if the CXFS metadata server for the filesystem is already running on this node. If both are true, then the filesystem is ready to use, and the CXFS resource does not have to do anything.

If either of these are not true, the CXFS resource will instigate the following actions:

1. The filesystem is unmounted across all nodes.
2. The filesystem is mounted locally on the new node, making it the new metaserver.
3. The filesystem is then mounted on the remaining nodes.

This sequence of actions will cause any user program which has files open within the unmounting filesystem to be killed, and the filesystem will be unavailable for a period of time until it can be remounted across all nodes.

A FailSafe administrator is free to define any type of failover policy. However, in order to minimize user disruptions an administrator may wish to define the DMF resource group failover policy in a fashion that increases the likelihood that the new FailSafe node will also be the new CXFS metaserver node, so that the above unmount/remount sequence is not necessary.

If a node on which a CXFS metadata server is running should crash, the metaserver will always move to the first available node listed in the filesystem's `mnttab` entry `server_list` parameter. This behavior matches the behavior of a FailSafe ordered failover policy with the attributes `Controlled_Failback` and `InPlace_Recovery` selected.

To minimize user disruptions in the face of server crashes, the administrator may therefore wish to define the DMF resource group to use an ordered failover policy with `Controlled_Failback` and `InPlace_Recovery` selected and enter the names of the failover domain nodes in the same order that they appear in the filesystem's `server_list` parameter.

## FailSafe TMF Resource Configuration

If you intend to use a DMF Tape MSP to migrate user files to tape, and if you will be using TMF as the tape mounting service, then you will need to configure the following:

1. Define one FailSafe 2.1 TMF Agent resource for each TMF Device Group in use by DMF. For more information on the IRIS FailSafe TMF agent, see the *IRIS FailSafe Version 2 TMF Administrator's Guide*.
2. Include the TMF resources as part of the DMF resource group. This ensures that the TMF Device Group fails over along with the rest of the DMF resource group.

## Adding DMF Resource Information to the Configuration Database (CDB)

This section describes how to create a DMF resource type, how to create a DMF resource, and how to create a DMF resource group. It also shows how to create a failover policy for a DMF resource group. These procedures assume that a CDB that does not include DMF has already been created, installed, and tested as described in the *IRIS FailSafe Version 2 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 is not automatically created at cluster creation time. The DMF resource type must be installed if you want to add a DMF resource to a cluster.

Use `inst` to install the DMF option.

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 Version 2 Administrator's Guide*.
- Run cluster manager (`cmgr`) and install the resource type.
- Instead of using the cluster manager (`cmgr`) to create the DMF resource type, you can use the IRIS FailSafe 2.1 GUI. Go to the "Resources & Resource Types" task page and select the "Load a Resource" task to load the DMF resource type.

The following example installs the a DMF resource type using cluster manager (`cmgr`).

**Example 2-1** DMF Resource Type Installation

```
cmgr> show clusters

eagan

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 in cluster eagan

Name: DMF
Predefined: false
Order: 101
```



```

Restart mode: 1
Restart count: 1

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: 40000ms
  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: 180000ms
  Start monitoring time: 0ms

No resource type dependencies

```

## Configuring a DMF Resource

After you have defined the resource type, 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 in the example below). To create the resource use the cluster manager (`cmgr`), the `cmgr` template scripts, or the GUI.

### Example 2-2 Creating a DMF Resource Using `cmgr`

```

# /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"

No type specific attributes to create with set command

No resource type dependencies to add

resource dmf ? done
Successfully defined resource dmf

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 will contain the resource. You can define any available failover policy for the resource group; however, if you are using CXFS filesystems, a failover policy of `ordered` with the hostnames in the failover domain defined in the same order as they are defined in the CXFS membership will result in the least impact on a user's jobs. For more information on defining a failover policy when using CXFS filesystems, see "The DMF-Managed User Filesystems" on page 9.

To determine the order of CXFS membership, execute the `/etc/mount` command. This will yield a list of the mounted filesystems. Check the `server_list` parameter of a CXFS filesystem entry to see a list of the CXFS membership in the order in which the nodes of the cluster see the membership.

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 2-3 Defining the Failover Policy

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

failover_policy dmfadmin ? set attribute to Controlled_Failback
failover_policy dmfadmin ? set script to ordered
failover_policy dmfadmin ? set domain to guinness dublin
failover_policy dmfadmin ? done
```

```
Successfully defined failover policy dmffadmin
```

## 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 should include at least the following:

- A DMF resource
- Resources for the DMF administrative filesystems. If these are CXFS filesystems, there must be a CXFS resource defined for each of them with the `relocate-mds` attribute defined as `false`. If these are XLV filesystems, there must be a filesystem and volume resource defined for each of them.
- A resource for each DMF-managed user filesystem. If the DMF-managed user filesystems are XLV filesystems, there must be a filesystem and volume resource for each filesystem. If the DMF-managed user filesystems are CXFS filesystems, there must be a CXFS resource defined for each filesystem with the `relocate-mds` attribute defined as `true`.
- If files are being migrated to offline tape storage in a tape library and the tape management software being used to manage this tape storage is the IRIX Tape Management Facility (TMF), then a resource should be defined for each TMF Device Group which is used by a DMF `dmatmsp` MSP process.

Set dependencies in the DMF resource for the DMF administrative filesystem resources but not for the DMF-managed user filesystems.

You must indicate what the failover policy is at the time you create the group.

The following example shows the creation of the DMF resource group `dmfcxfs` in cluster `eagan`. The DMF filesystems in this resource group are all CXFS filesystems. A CXFS resource is added to the resource group for each filesystem.

### Example 2-4 Creating the Resource Group `dmfcxfs` of Type DMF

```
cmgr>
Welcome to SGI Cluster Manager Command-Line Interface

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

```
resource_group dmfcxfs ? set failover_policy to dmfadmin
resource_group dmfcxfs ? add resource dmf of resource_type DMF
resource_group dmfcxfs ? add resource /cdmfhome of resource_type CXFS
resource_group dmfcxfs ? add resource /cdmfjournals of resource_type
CXFS
resource_group dmfcxfs ? add resource /cdmfspool of resource_type CXFS
resource_group dmfcxfs ? add resource /dmf_user1 of resource_type CXFS
resource_group dmfcxfs ? add resource /dmf_user2 of resource_type CXFS
resource_group dmfcxfs ? add resource /dmf_user3 of resource_type CXFS
resource_group dmfcxfs ? add resource tmf of resource_type TMF

resource_group dmfcxfs ? done
Successfully defined resource group dmfcxfs

cmgr> show resource_group dmfcxfs

Resource Group: dmfcxfs
Cluster: eagan
Failover Policy: dmfadmin

Resources:
dmf (type: DMF)
/dmf_user1 (type: CXFS)
/dmf_user2 (type: CXFS)
/dmf_user3 (type: CXFS)
/cdmfhome (type: CXFS)
/cdmfjournals (type: CXFS)
/cdmfspool (type: CXFS)
tmf (type: TMF)

cmgr> show failover_policy dmfadmin
Failover Policy: dmfadmin
Version: 1
Script: ordered
Attributes: Controlled_Failback InPlace_Recovery
Initial AFD: guinness dublin

cmgr> show resource dmf of resource_type DMF

Resource dependencies
CXFS /cdmfhome
CXFS /cdmfjournals
CXFS /cdmfspool

cmgr> show resource /dmfuser_1 of resource_type CXFS
```

```
relocate-mds: true

No resource dependencies

cmgr> show resource /cdmfhome of resource_type CXFS

relocate-mds: false

No resource dependencies

cmgr>
```

## DMF Action Scripts

There are several scripts that FailSafe uses to start, stop, and monitor DMF. These scripts are found in the `/var/cluster/ha/resource_types/DMF` directory and are as follows:

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

## 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 the input file is the resource name. The output file is empty. 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 Version 2 Programmer's Guide*. The output file should be checked after testing each script to verify that the script worked properly.

For example, you can test the DMF resource `dmf` that was previously created by executing the following commands as root:

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

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:

<code>start</code>	Starts the DMF daemon
<code>stop</code>	Stops DMF on this node
<code>monitor</code>	Extended test to see if DMF is running on this node
<code>exclusive</code>	Tests to see if DMF is already running on this node
<code>restart</code>	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 where *hostname* is the name of the host on which FailSafe is running.

---

# Index

## A

action scripts, FailSafe, 17  
administrative filesystems, DMF, 7

## C

CACHE\_DIR, 7  
configuration database (CDB), 11  
configuration flag, DMF, 6  
CXFS  
  membership, 14  
CXFS filesystems  
  as DMF administrative filesystems, 8, 15  
  as DMF-managed user filesystems, 10, 15  
  configuration, 9

## D

database journals, DMF, 7  
databases, DMF, 7  
dmaudit command, 7  
dmdaemon, 1  
DMF  
  administrative filesystems, 7  
  configuration flag, 6  
  daemon, 1  
  database journals, 7  
  databases, 7

log files, 7  
monitor script, 1  
resource configuration, 13  
resource group configuration, 15  
resource type creation, 11  
testing, 17  
user filesystems, 9

## F

failover domain, 11  
failover policy, 10, 14, 15  
FailSafe  
  action scripts, 17  
  agents, 1  
  man pages, xvi  
  message paths, 1  
  release notes, xvii  
  TMF agent, 6  
FTP\_DIRECTORY, 7

## H

HOME\_DIR, 7

## J

JOURNAL\_DIR, 7

- L**
  - log files, DMF, 7
  
- M**
  - man pages, xvi
  - mnttab, 11
  - monitor script, DMF, 1
  - MOVE\_FS, 7
  - MSP, 7
  
- R**
  - release notes, xvii
  - relocate-mds CXFS attribute, 10
  - resource configuration, 13
  - resource group configuration, 15
  
- S**
  - server\_list parameter of mnttab, 11
  - SPOOL\_DIR, 7
  - STORE\_DIRECTORY, 7
  
- T**
  - Tape Management Facility (TMF), 3, 6
    - agent, 6
    - configuration, 11
    - device group, 15
    - FailSafe option, 3
    - resource, 15
  - testing DMF, 17
  - TMF, See Tape Management Facility
  
- X**
  - XLV filesystems
    - as DMF administrative filesystems, 8, 15
    - as DMF-managed user filesystems, 9, 15
    - configuration, 8