

AlphaServer Intelligent Peripheral Platform

System Manager's Guide

Part Number: AA-QU0JC-TE

June 1999

This guide provides configuration information for the *AlphaServer Intelligent Peripheral Platform*. Use this guide in conjunction with the *AlphaServer Intelligent Peripheral Platform Hardware Owner's Guide*, the *Intelligent Peripheral Fault Manager for Tru64 UNIX Installation and User's Guide* and *Tru64 UNIX* system management documentation.

Operating System and Version: *Tru64 UNIX*, Version 4.0D or 4.0E

Software Version: Version 2.2

**Compaq Computer Corporation
Maynard, Massachusetts**

October 1997

June 1999

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL. THIS INFORMATION IS PROVIDED "AS IS" AND COMPAQ COMPUTER CORPORATION DISCLAIMS ANY WARRANTIES, EXPRESS, IMPLIED OR STATUTORY AND EXPRESSLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, GOOD TITLE AND AGAINST INFRINGEMENT.

This publication contains information protected by copyright. No part of this publication may be photocopied or reproduced in any form without prior written consent from Compaq Computer Corporation.

© 1999 Digital Equipment Corporation. All rights reserved.

The software described in this guide is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement.

Compaq, the Compaq logo and the Digital logo are registered in United States Patent and Trademark Office.

AlphaServer, DECEvent, DIGITAL, StorageWorks, Tru64 UNIX, and TruCluster are trademarks of Compaq Computer Corporation.

Microsoft, Windows, and Windows NT are registered trademarks and Internet Explorer and Outlook are trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Ltd.

Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Table of Contents

Preface

1 AlphaServer IP Platform Configuration Preparation

- System Configuration Preparation 1-1
- System Console 1-2
- Network Controllers 1-2
 - TCP/IP Network Address worksheet 1-2

2 Configuring AlphaServer IP Software

- Summary of Configuration Steps 2-1
- Connecting to the AlphaServer Console Port 2-2
- Configuring the Tru64 UNIX Operating System 2-2
- Configuring the Network Setup Device 2-2
- Configuring /etc/hosts File for UNIX Systems 2-6

3 Configuring the IPFM Software

- Configuring DECEvent Software 3-1
- Customizing the IPFM Configuration File 3-1
- Modifying the SNMP Agent Configuration File 3-4
- Configuring the IPFM SNMP Trap Style 3-4
 - Default IPFM SNMP Trap Style 3-4
 - Alternate IPFM SNMP Trap Style 3-5
- Configuring the Network Management Station (NMS) 3-6
 - Configuring the NMS with ServerWORKS 3-6
 - Enrolling the IPFM MIB into the ServerWORKS NMS 3-7
 - Setting Up IPFM Alarm Traps 3-7
 - Enrolling the IPFM MIB into the TeMIP NMS 3-8

4 Configuring the Logical Storage Manager

5 Configuring AdvFS

6 Configuring TruCluster ASE Software

Glossary

Index

Tables

Table 1-1: System Node Names and TCP/IP Addresses	1-2
Table 2-1: Required Software Per System.....	2-1
Table 3-1: Configuration File Keywords.....	3-2
Table 3-2: Default SNMP Trap Variable Binding List	3-4
Table 3-3: Variable Binding List	3-5

Preface

About This Guide

This guide explains how to configure the *AlphaServer Intelligent Peripheral Platform*. It is intended to assist the system manager in bringing the system to operation, but does not provide a complete description of configuration details for all of the layered products involved. For complete details, refer to the layered product documentation.

This guide includes configuration guidelines for the required and optional software layered products that have been factory-installed in your Intelligent Peripheral. Your hardware configuration may or may not contain the optional components listed in this document.

Keep this guide with your *IPFM* distribution kit; you will need it to install maintenance updates or to reinstall the product for any other reason.

Intended Audience

This document is intended for system managers who have a working knowledge of the *Tru64 UNIX* operating system configuration and management.

Structure of This Document

This guide is organized as follows:

Chapter 1, AlphaServer IP Platform Configuration Preparation – Describes the prerequisite hardware and software configurations.

Chapter 2, Configuring AlphaServer IP Software – Describes how to connect to the console port, configure the *Tru64 UNIX* operating system, perform the network setup, and configure the */etc/host* file.

Chapter 3, Configuring IPFM Software – Describes the configuration of *DECevent* and the Network Management Station, and the customization of the *IPFM* configuration file.

Chapter 4, Configuring the Logical Storage Manager – Describes the configuration of LSM volumes on either the duplex system (required) or simplex system (recommended).

Chapter 5, Configuring AdvFS – Describes how to use the AdvFS graphical user interface to configure the *Advanced File System*.

Chapter 6, Configuring TruCluster ASE Software – Describes how to configure *TruCluster ASE* on duplex systems.

Related Documentation

For additional information on the *AlphaServer IP Platform* subsystem components and related software, refer to the documentation in the following table. Order numbers may change as documents are revised or updated. Check with your Compaq sales representative for additional information.

Document	Order Number
AlphaServer IP Peripheral Platform	
<i>Intelligent Peripheral Fault Manager for Tru64L UNIX Installation and User's Guide</i>	AA-QN0FD-TE
<i>AlphaServer Intelligent Peripheral Platform Hardware Owner's Guide</i>	EK-ASIP2-OG
AlphaServer Processor	
<i>AlphaServer 1000A Rackmount Owner's Guide</i>	EK-RMNOR-OG
<i>DIGITAL UNIX Installation Guide</i>	AA-QTLGB-TE
<i>DIGITAL UNIX System Administration</i>	AA-PS2RE-TE
Layered Product Documentation	
<i>Logical Storage Manager</i>	AA-Q3NCE-TE

Conventions

The following table of conventions explains the use of abbreviations, symbols, and special characters in this guide.

Conventions

Convention	Description
IP	IP is an industry-standard acronym for <i>intelligent peripheral</i> .
#	A pound sign (#) is the default superuser prompt.
%	A percent sign (%) is the default user prompt.
Ctrl/C	This symbol indicates that you must press the Ctrl key while you simultaneously press another key (in this case, C).
<RETURN>	In examples, this symbol indicates that you press the Return key.
% cat	In interactive examples, typed user input appears in a bold typeface.
monospaced	In text, this typeface indicates the exact name of a command, routine, partition, pathname, directory, or file. This typeface is also used in interactive examples and other screen displays.
UPPERCASE lowercase	The <i>Tru64 UNIX</i> operating system differentiates between lowercase and uppercase characters. Literal strings that appear in text, examples, syntax descriptions, and function definitions must be typed exactly as shown.
<i>italic</i>	Italic text emphasizes important information and indicates product names and complete titles of manuals.
[y]	In a prompt, square brackets indicate that the enclosed item is the default response. For example, [y] means the default response is Yes.

AlphaServer IP Platform Configuration Preparation

The *AlphaServer Intelligent Peripheral (IP) Platform* is a rackmount hardware product that can provide voice processing, FAX, voice recognition, and voice messaging services for telecommunications service providers. The *AlphaServer IP Platform* is available in two basic variations: simplex and duplex. The simplex version provides one each, and the duplex two each, of the following components:

- *AlphaServer* system processor with EISA/ISA bus.
- ISA bus expansion chassis

Optional components include the following:

- -48 Vdc power controller subassembly
- *StorageWorks* storage shelf with SCSI disks
- Communications hub
- SNMP-compliant Network Management Station
- Alarm Indicator Panel

Your system has been shipped to your site with the operating system and layered product software (included in the IP purchase) installed. Your *AlphaServer* system was configured and tested at the factory prior to shipping. All components were configured to the extent that they could be used to test the configuration.

Note

You may need to change parameter settings from those used in the factory to the settings that you desire.

System Configuration Preparation

System node names and TCP/IP addresses are defined as part of the hardware and software configuration. System node names and TCP/IP addresses must be coordinated with other nodes configured in the computer network. You need to provide node names and TCP/IP addresses for every CPU in the Intelligent Peripheral configuration.

Hardware options affect the configuration of software, the system console, and single or multiple network controllers.

System Console

The system console can be connected in any of three ways:

1. A graphics terminal can be connected to a PCI graphics controller.
2. A character cell terminal can be connected to the system's serial console port.
3. The system's serial console port can be connected to a terminal server.

The type of console connection determines the method of connecting to the system when configuring the network.

Network Controllers

Each *Tru64 UNIX* system may be configured with more than one network controller (Ethernet, Fast Ethernet, FDDI and/or ATM). These controllers require TCP/IP addresses and subnet masks. Each controller within a given computer must be configured on different subnets within the network, and each controller must be configured with unique node names (configured in `netsetup`). One of these names will be the system's node name, and the other will be arbitrary. Consult your network administrator for information on IP addresses and subnets. If you are configuring a duplex system, you must define a *TruCluster* service name (similar to a node name) and its associated IP address.

TCP/IP Network Address worksheet

Table 1-1 provides a worksheet that you can use to document the node names, IP addresses, and subnet masks discussed in the following chapters. If you are configuring a single simplex system, fill in the information in the row labeled Server1. If you are configuring a duplex system, designate one system as Server1 and the other as Server2, and fill in the information in the rows labeled Server1 and Server2. In configuring a duplex system, you will also need a service name and TCP/IP address for every *TruCluster* service used. Your configuration may not contain every item listed.

Table 1-1: System Node Names and TCP/IP Addresses

System	Node Name	IP Address	Subnet Mask
Server1	_____	____.____.____.____	____.____.____.____
Server1 Alt Controller	_____	____.____.____.____	____.____.____.____
Server2	_____	____.____.____.____	____.____.____.____
Server2 Alt Controller	_____	____.____.____.____	____.____.____.____
TruCluster Service	_____	____.____.____.____	N/A

In this document, a simplex system is referred to as `ipsys1`, and the two systems in a duplex configuration are referred to as `ipsys1` and `ipsys2`.

Configuring AlphaServer IP Software

The *AlphaServer IP Platform* is configured as either a single *AlphaServer* system (simplex) or as two *AlphaServer* systems running the *TruCluster Available Server Environment* software (duplex). The configuration steps and guidelines detailed in the following sections must be performed on every *AlphaServer* system in the configuration (one for a simplex system or two for a duplex system) except where noted. For a duplex configuration, some steps are performed on both *AlphaServer* systems, and some steps are performed on only one of the systems.

The operating system and layered software products discussed in this chapter are listed in Table 2-1.

Table 2-1: Required Software Per System

Product	Simplex	Duplex
Tru64 UNIX	X	X
Logical Storage Manager	X	X
AdvFS Utilities	X	X
DECevent	X	X
IPFM for Tru64 UNIX	X	X
Dialogic Drivers	X	X
TruCluster Available Server		X

Summary of Configuration Steps

The steps generally required to configure the layered products on an *AlphaServer* system are summarized in the following list. The first three steps are described in this chapter. The remaining steps are described in the chapters that follow.

1. Connect to the *AlphaServer* console.
2. Configure the *Tru64 UNIX* operating system.
3. Configure the Network device using `netsetup`, including IP addresses.
4. Configure *DECevent*.
5. Configure the `/etc/hosts` file.
6. Configure the *IP Fault Manager for Tru64 UNIX* software.
7. Configure the *Logical Storage Manager (LSM)* volumes.
8. Configure *Advanced File Systems (AdvFS)*.

9. On duplex systems, configure *TruCluster Available Server* software. This step includes the configuration of the Network Time Protocol (NTP) software and the Network File Services (NFS).

Connecting to the AlphaServer Console Port

There are three options for connecting the system console. The type of console you configure determines how to log on to the system to configure the network.

1. For a graphics terminal connected to a PCI graphics controller:
Log on to the system using the graphics console to gain access to the system.
2. For a character cell terminal connected to the system's serial console port:
Log on to the system using the character call console to gain access to the system.
3. For a system with a serial console port connected to a terminal server:
Configure a local service on the terminal server to allow network connections to be made to the terminal server port that the console is connected to. Refer to the terminal server owner's manual for information on configuring local services.

Each *AlphaServer* system has two serial ports that are used as console ports. In order to allow remote access to the systems console ports (with no single point of failure), it is recommended that the two serial console ports be plugged into two separate terminal servers that are network accessible.

Configuring the Tru64 UNIX Operating System

The *Tru64 UNIX* operating system was installed at the factory prior to being shipped to your site. When your system is powered up for the first time (and you have logged into the system console), the system prompts you to answer several questions in order to complete the system configuration. Refer to the manufacturing FIS information letters and the *DIGITAL UNIX Installation Guide* for a complete description of the power-up configuration sequence.

When the *Tru64 UNIX* configuration is complete, you must configure the network and set up system node names and IP addresses.

Note

For more information about *Tru64 UNIX* system administration, refer to the *DIGITAL UNIX System Administration Guide*.

Configuring the Network Setup Device

The network devices require configuration. Each system in the IP platform may be configured with dual network controllers. Use the `netsetup` command to configure the Ethernet devices.

Note

When configuring more than one network device, the devices should be configured in different TCP/IP subnets.

The following example output shows you how to configure *two* network devices. User responses are in bold type. Your installation may require answers different from those shown in the example. Refer to the *Tru64 UNIX System Administration* documentation for instructions on how to run the `netsetup` script.

```
# netsetup

      **** MAIN MENU ****

      1  Configure Network Interfaces
      2  Enable/Disable Network Daemons and Add Static Routes
      3  Add/Delete Host Information
      4  Display Network Configuration
      5  Exit

Enter the number for your choice: 1

***** CONFIGURE/DELETE NETWORK INTERFACES *****

You can configure or delete network interfaces.  Configuration information
is updated in /etc/rc.config and /etc/hosts.  Choose "configure" or "delete"
at the prompt.

Enter whether you want to "(c)onfigure" or "(d)eleate" network interfaces.
If you are finished, press the RETURN key: c

You want to "configure" interfaces.  Is this correct [yes]? yes

You will now be asked a series of questions about the system.
Default answers are shown in square brackets ([]).  To use a
default answer, press the RETURN key.

This machine contains the following network interfaces:
      tu0
      tu1

Which interface do you want to configure [tu0]: tu0
You want to configure "tu0".  Is this correct [yes]? yes

Enter the hostname for the system [ipsys1.zko.dec.com]: ipsys1
The hostname for the system is " ipsys1.zko.dec.com".
Is this correct [yes]? yes

Enter the Internet Protocol (IP) address for interface "tu0"
in dot notation [16.30.144.208]: 16.126.124.101
The IP address for interface "tu0" is "16.126.224.101".
Is this correct [yes]? yes

Subnetworks allow the systems on a local area network to be on different
physical networks.  For the following question, use the default answer
unless the existing local area network is using subnet routing.
If the local area network is using subnet routing, you need to know
the subnet mask.

Enter the subnet mask in dot notation [255.255.255.0]: 255.255.255.0
The subnet mask for "tu0" is "255.255.255.0".
Is this correct [yes]? yes

For the following question USE THE DEFAULT ANSWER unless you would like
to add additional flags (found in the ifconfig reference page) to the
ifconfig command.  Normally, you will USE THE DEFAULT ANSWER.

Do you want to use additional ifconfig flags for this interface [no]? no
```

Configuring AlphaServer IP Software

The configuration looks like:

```
system hostname: "ipsys1.zko.dec.com"
ifconfig tu0 16.126.224.101 netmask 255.255.255.0
```

Is this correct [yes]? **yes**

```
***** UPDATING /etc/rc.config *****
```

```
"tu0" is configured in /etc/rc.config
```

```
***** CONFIGURING "tu0" *****
```

```
/sbin/ifconfig tu0 16.126.224.101 netmask 255.255.255.0 up
```

Do you want to configure another network interface [yes]? **Yes**

This machine contains the following network interfaces:

```
tu0
tu1
```

Which interface do you want to configure [tu0]: **tu1**

You want to configure "tu1". Is this correct [yes]? **yes**

Enter the hostname for the system [ipsys2.zko.dec.com]: **ipsys2**

The hostname for the system is "ipsys2.zko.dec.com".

Is this correct [yes]? **yes**

Enter the Internet Protocol (IP) address for interface "tu1"
in dot notation [16.30.144.208]: **16.126.124.102**

The IP address for interface "tu1" is "16.126.124.102".

Is this correct [yes]? **yes**

Subnetworks allow the systems on a local area network to be on different physical networks. For the following question, use the default answer unless the existing local area network is using subnet routing. If the local area network is using subnet routing, you need to know the subnet mask.

Enter the subnet mask in dot notation [255.255.255.0]: **255.255.255.0**

The subnet mask for "tu1" is "255.255.255.0".

Is this correct [yes]? **yes**

For the following question USE THE DEFAULT ANSWER unless you would like to add additional flags (found in the ifconfig reference page) to the ifconfig command. Normally, you will USE THE DEFAULT ANSWER.

Do you want to use additional ifconfig flags for this interface [no]? **no**

The configuration looks like:

```
system hostname: "ipsys2.zko.dec.com"
ifconfig tu1 16.126.224.102 netmask 255.255.255.0
```

Is this correct [yes]? **yes**

```
***** UPDATING /etc/rc.config *****
```

```
"tu0" is configured in /etc/rc.config
```

```
***** CONFIGURING "tu1" *****
```

```
/sbin/ifconfig tu1 16.126.224.102 netmask 255.255.255.0 up
```

Do you want to configure another network interface [yes]? **no**

Enter whether you want to "(c)onfigure" or "(d)elete" network interfaces. If you are finished, press the RETURN key: **<RETURN>**

**** MAIN MENU ****

- 1 Configure Network Interfaces
- 2 Enable/Disable Network Daemons and Add Static Routes
- 3 Add/Delete Host Information
- 4 Display Network Configuration
- 5 Exit

Enter the number for your choice: **2**

***** ENABLE/DISABLE NETWORK DAEMONS AND ADD STATIC ROUTES *****

You can choose whether you want to enable or disable rwhod (rwhodaemon), and either gated (gateway daemon) or routed (route daemon). You can also configure static routes. Daemons and static route commands are executed when the network is started up.

Do you want to run rwhod [no]? **no**

rwhod is disabled.

Are you setting up your system to be an IP router [no]? **no**

You can run either gated or routed but not both. Choose "(g) ated" or "(r)outed" at the prompt.

Do you want to run "(g)ated" or "(r)outed.

If you do not want either, then press the RETURN key: **g**

You want to run gated. Is this correct [yes]? **Yes**

You can use flags (see the gated reference page) when you run the gateway daemon.

Enter the gated flags separated by a space.

If you do not want any flags, press the RETURN key: **<RETURN>**

You do not want any flags. Is this correct [yes]? **Yes**

gated is enabled.

Static route commands can be configured in /etc/routes that will be executed when the network is started up on this system.

Do you want to add a static route [no]? **no**

**** MAIN MENU ****

- 1 Configure Network Interfaces
- 2 Enable/Disable Network Daemons and Add Static Routes
- 3 Add/Delete Host Information
- 4 Display Network Configuration
- 5 Exit

Enter the number for your choice: **5**

Do you want netsetup to automatically restart the network services on this system [no]? **yes**

Configuring /etc/hosts File for UNIX Systems

The network configuration file `/etc/hosts` must contain the node names and IP addresses of every system in the IP platform. This file can be modified using a text editor, or by using the `netsetup` script.

The following example output shows you how to configure the `/etc/hosts` file using the `netsetup` script (responses are in bold type.) Your installation may require answers different from those shown in the example. Refer to the *Tru64 UNIX System Administration* documentation for instructions on how to run the `netsetup` script.

```
# /usr/sbin/netsetup

**** MAIN MENU ****

1  Configure Network Interfaces
2  Enable/Disable Network Daemons and Add Static Routes
3  Add/Delete Host Information
4  Display Network Configuration
5  Exit

Enter the number for your choice: 3

**** HOST INFORMATION MENU ****

1  /etc/hosts
2  /etc/hosts.equiv
3  /etc/networks
4  Exit

Enter the number for your choice: 1

***** ADD/DELETE HOSTS IN /etc/hosts *****

You can add or delete hosts in /etc/hosts.  When finished, press
the RETURN key at the prompt that asks whether you want to add
or delete hosts.

Enter whether you want to "(a)dd" or "(d)delete" hosts in /etc/hosts.
If you are finished, press the RETURN key: a
You want to "add" to /etc/hosts.  Is this correct [yes]? yes

Enter the host name, aliases and Internet Protocol (IP) address for
each host in the network.  Enter this information on separate lines
when prompted.  This information is added to the /etc/hosts file.

Enter the name of the host to add to /etc/hosts.
If you are finished, press the RETURN key: ipsys1

You want to add host "ipsys1".
Is this correct [yes]? yes

Enter any aliases for "ipsys1", separated by a space.
If you do not want any aliases, press the RETURN key: <RETURN>

You do not want any aliases for "ipsys1".
Is this correct [yes]? yes

Enter the Internet Protocol (IP) address of "ipsys1"
in dot notation: 16.126.224.101

The IP address for "ipsys1" is "16.126.224.101".
```

Is this correct [yes]? **yes**

The /etc/hosts entry looks like:

```
16.126.224.101 ipsys1
```

Is this correct [yes]? **yes**

"16.126.224.101 ipsys1 " is added to /etc/hosts

Enter the name of the host to add to /etc/hosts.
If you are finished, press the RETURN key: **ipsys2**

You want to add host "ipsys2".
Is this correct [yes]? **yes**

Enter any aliases for "ipsys2", separated by a space.
If you do not want any aliases, press the RETURN key: **<RETURN>**

You do not want any aliases for "ipsys2".
Is this correct [yes]? **yes**

Enter the Internet Protocol (IP) address of "ipsys2"
in dot notation: **16.126.224.102**

The IP address for "ipsys2" is "16.126.224.102".
Is this correct [yes]? **yes**

The /etc/hosts entry looks like:

```
16.126.224.102 ipsys2
```

Is this correct [yes]? **yes**

"16.126.224.102 ipsys2 " is added to /etc/hosts

Enter the name of the host to add to /etc/hosts.
If you are finished, press the RETURN key: **<RETURN>**

Enter whether you want to "(a)dd" or "(d)etele" hosts in /etc/hosts.
If you are finished, press the RETURN key: **<RETURN>**

**** HOST INFORMATION MENU ****

- 1 /etc/hosts
- 2 /etc/hosts.equiv
- 3 /etc/networks
- 4 Exit

Enter the number for your choice: **4**

**** MAIN MENU ****

- 1 Configure Network Interfaces
- 2 Enable/Disable Network Daemons and Add Static Routes
- 3 Add/Delete Host Information
- 4 Display Network Configuration
- 5 Exit

Enter the number for your choice: **5**

Configuring AlphaServer IP Software

To perform additional tasks in setting up the network, see the Network Configuration reference. For the netsetup modifications to take effect, either restart the network services on this system with the following command:

```
/usr/sbin/rcinet restart
```

or reboot this system with the following command:

```
/usr/sbin/shutdown -r now
```

NOTE: If you are going to use the '/usr/sbin/rcinet restart' command, warn the users that the network services on this system are going to be restarted. Also, any NFS filesystems not mounted via fstab or automount will not be remounted.

Do you want netsetup to automatically restart the network services on this system [no]? **yes**

```
***** NETWORK SETUP COMPLETE *****
```

Configuring the IPFM Software

Familiarize yourself with the *Intelligent Peripheral Fault Manager for Tru64 UNIX Installation and User's Guide* prior to performing the *IPFM* configuration.

Configuring DECEvent Software

To run the *IPFM* software with *DECEvent*, *DECEvent* must be set to the report type `ETM_2_RE`.

1. To check the DECEvent report type, enter the following command:

```
# dia shw set DEFAULT_REPORT
```
2. If the report type is not `ETM_2_RE`, enter the following set of commands to set the report type:

```
#dia -int  
dia> sets DEFAULT_REPORT ETM_2_RE  
dia> sav sys  
dia> quit
```
3. Restart the *IPFM* software by running the following commands:

```
# ipfm_shutdown  
# ipfm_init.d
```

Customizing the IPFM Configuration File

The *IPFM* configuration file contains the following information:

- Event Category - The category of event to be detected and reported.
- Event Severity - The severity level of the event.
- Event Text - The text of the event.

The *IPFM* configuration file is located in the following directory:

```
/usr/opt/IPFM/bin/online/ipfm.conf
```

The user can modify the *IPFM* configuration file in order to:

- Enable or disable the detection of events
- Change the severity of an event
- Change the text used for an event.

Note

The event severity and event text can not be modified on the "system" detected events. The severity and text will be determined from the component generating the error.

The configuration file allows the user to modify what types of events are monitored, and in some cases the severity to be used when the associated alarms are generated. For a sample `ipfm.conf` file, see the Configuration File appendix of the *Intelligent Peripheral Fault Manager for Tru64 UNIX Installation and User's Guide*.

Table 3-1 shows the keywords that are defined in the `ipfm.conf` file. Comments in the file and descriptions in the table explain how the configuration file can be modified. In most cases the configuration file contains examples on the format and options of the keywords and parameters.

Table 3-1: Configuration File Keywords

Keyword	Description
Configuration Keywords	
CONTROL	Indicates whether there is an IPFM PCI control module in the system. The parameter is TRUE if there is a control module in the system and FALSE if there is not.
INDICATOR	Indicates whether there is an IPFM Alarm panel indicator module hooked up to the CONTROL module. The parameter is TRUE if there is an alarm panel attached to the system and FALSE if there is not.
ASC-LED	Defines the pattern displayed in the status LED. Compaq recommends that this parameter not be modified.
KEEP-ALIVE	Specifies the keep-alive update frequency. The parameter specifies the number of seconds between sending the alarm panel a keep-alive signal. If the keep-alive signal is reset within x seconds, the alarm panel signals a minor alarm.
SHUTOFF_SW	Detect Audible Disable switch.
AUDIBLE	Enable or Disable the audible alarm. If this parameter is set to TRUE, the alarm panel signals alarms using an audible beep. If the parameter is set to FALSE, no audible beep is generated.
POLLING	Controls the polling interval. The parameter contains the polling interval, in seconds, for the checking of File System, System Environmental, and Process Missing events. The default is 5 seconds.
TRAP-THRESHOLD	Specifies the SNMP trap threshold severity. The parameter allows the user to limit the SNMP traps that are generated. The user can specify a TRAP-THRESHOLD severity to cause IPFM to only generate SNMP traps when the alarm has an equal or greater severity than the TRAP-THRESHOLD severity.

Keyword	Description
System Events	<p>The following four keywords monitor system events.</p> <p>The severity and alarm text may not be modified on these events.</p> <p>If one of these event types is not desired, comment out the line by inserting a # before the keyword.</p>
CPU	Monitors CPU-related events.
DISK	Monitors DISK-related events.
NETWORK	Monitors NETWORK-related events.
MEMORY	Monitors MEMORY-related events
FS	<p>Defines File System capacity thresholds.</p> <p>The user can specify a file system to be monitored by the IPFM software. The user specifies the file system mount point, the available capacity (in either bytes or as a percentage) and the associated alarm severity.</p>
PROCESS	<p>Monitors the system for one or more specific process names.</p> <p>The user can instruct IPFM to monitor the system for the presence of one or more processes. The user specifies the process name, the process's UID, the number of processes that should be running, the associated alarm severity and an optional action script to run if the number of processes is lower than expected.</p>
System Environmental Events	<p>The following three keywords monitor environmental events.</p> <p>The user can specify the associated alarm severity and alarm text in the configuration file if desired.</p> <p>If one of these events is not desired, comment out this line by inserting a # before the keyword.</p>
TEMP-CPU	Monitors the temperature of the system. If the system temperature thresholds are crossed, IPFM generates a TEMP-CPU alarm.
FAN-CPU	Monitors the system fan. If the system fan is detected to fail, IPFM generates a FAN-CPU alarm.
POWER-CPU	Monitors the system power supply (valid only if there is redundant power supplies). If a failure in the redundant power supply is detected, IPFM generates a POWER-CPU alarm.
Expansion Chassis Events	<p>The following three keywords monitor expansion chassis events.</p> <p>The user can specify the associated alarm severity and alarm text in the configuration file if desired.</p> <p>Since the expansion box is an optional component, the expansion chassis event keywords are commented out by default. To enable an expansion chassis event keyword, remove the commenting by deleting the # before the keyword</p>
TEMP-EXT	Monitors the temperature of the external expansion box (if present). If the expansion box temperature threshold is crossed, IPFM generates a TEMP-EXT alarm.
FAN-EXT	IPFM monitors the external expansion box fan. If a fan failure is detected, IPFM generates a FAN-EXT alarm.
POWER-EXT	IPFM monitors the expansion box power supply. If a power supply failure is detected, IPFM generates a POWER-EXT alarm.

Keyword	Description
External Signals	<p>The following three keywords represent three external signals that can be monitored. These external signals are connected to the -48Vdc power supply by a cable if the system was configured with a -48Vdc power option.</p> <p>The user can specify the associated alarm severity and alarm text in the configuration file if desired.</p> <p>Since the -48Vdc power supply is an optional component, the USER-EVENTx keywords are commented out by default. To enable a USER-EVENTx keyword, remove the commenting by deleting the # before the keyword.</p>
USER-EVENT1	When enabled, defaults to the "Fail relay on" event description for the -48V power inverter.
USER-EVENT2	When enabled, defaults to the "Minor alarm relay on" event description for the -48V power inverter.
USER-EVENT3	When enabled, defaults to the "Major alarm relay on" event description for the -48V power inverter.

Modifying the SNMP Agent Configuration File

The SNMP Agent configuration file , `/etc/snmpd.conf`, must have the following items added to allow the Network Management System (NMS) to work with the *IPFM* target system:

1. To get started, it is suggested that the public community be set to read/write as follows:

```
Community public 0.0.0.0 write
```

2. A community specification may be added to include the IP address of the NMS and to allow read and write privileges as follows (where `xx.xx.xx.xx` stands for the IP address of the NMS and `ipfm` is the community name):

```
community ipfm xx.xx.xx.xx write
```

3. The trap community specification must be added as follows (where `xx.xx.xx.xx` stands for the IP address of the NMS):

```
trap ipfm xx.xx.xx.xx
```

Configuring the IPFM SNMP Trap Style

Two SNMP trap styles are available:

- Default IPFM SNMP trap style
- Alternate IPFM SNMP trap style, for IPFM that is OSI compliant

Default IPFM SNMP Trap Style

The default SNMP trap style consists of the following variable bindings:

Table 3-2: Default SNMP Trap Variable Binding List

OID	Value	Description
1.3.6.1.4.1.36.2.15.25.5.1.1	1	Alarm ID
1.3.6.1.4.1.36.2.15.25.5.1.2	CRITICAL	"ASCII" severity
1.3.6.1.4.1.36.2.15.25.5.1.3	New critical alarm	Text description of alarm
1.3.6.1.4.1.36.2.15.25.5.1.4	ACTIVE	Alarm state (ACTIVE, ACK, or CLEAR)

alarmIndex (OID: 1.3.6.1.4.1.36.2.15.25.5.1.1)

The alarmIndex contains an alarm index. This is a unique value that can be used to further identify the alarm within the IP.

alarmSeverity (OID: 1.3.6.1.4.1.36.2.15.25.5.1.2)

The alarmSeverity is a text string containing the severity of the particular alarm: CRITICAL, MAJOR, MINOR, WARNING or INFO.

alarmDescript (OID: 1.3.6.1.4.1.36.2.15.25.5.1.3)

The alarmDescript contains the alarm text.

alarmStatus (OID: 1.3.6.1.4.1.36.2.15.25.5.1.4)

The alarmStatus is a text string containing status of the particular alarm: ACTIVE, ACK or CLEAR.

Alternate IPFM SNMP Trap Style

The Alternate SNMP trap style was created for IPFM that is OSI compliant. Using this alarm trap style simplifies the integration of IPFM with TeMIP and other Network Management Systems.

To generate the alternate style alarm, define the environment variable IPFM_NMS_ALARM to 1 prior to starting IPFM. Normally, this is done by specifying it in the “.profile “ file executed at login. For example, enter the following in the /.profile file:

```
IPFM_NMS_ALARM=1
export IPFM_NMS_ALARM
```

If IPFM_NMS_ALARM is not specified, or it is set to any value other than 1, IPFM defaults to the standard alarm it sends. Note, the alarm style cannot be changed while IPFM is running. IPFM needs to be restarted to change the alarm style.

The alternate SNMP trap style has the following format:

Table 3-3: Variable Binding List

OID	Value	Description
1.3.6.1.4.1.36.2.15.25.5.1.1	1	Alarm ID
1.3.6.1.4.1.36.2.15.25.5.1.2	CRITICAL	“ASCII” severity
1.3.6.1.4.1.36.2.15.25.5.1.3	New critical alarm	Text description of alarm
1.3.6.1.4.1.36.2.15.25.5.1.4	ACTIVE	Alarm state (ACTIVE, ACK, or CLEAR)
1.3.6.1.4.1.36.2.15.25.5.1.6	1	Integer severity
1.3.6.1.4.1.36.2.15.25.5.1.7	0	Alarm probable cause
1.3.6.1.4.1.36.2.15.25.5.1.8	0	Alarm event type

The first four variables (OIDs) are the same variables generated in the default IPFM alarm. The following describes the additional three variables (OIDs).

alarmIntSeverity (OID: 1.3.6.1.4.1.36.2.15.25.5.1.6)

alarmIntSeverity is the integer representation of the severity variable. It can have the following values:

Severity	Integer Value
critical	1
major	2
minor	3
warning	4
clear	5

The value of alarmIntSeverity is based on the IPFM “ASCII” Severity and the alarm state. Alarms with a severity of “INFO” are mapped to the alarmIntSeverity of 4 (Warning). AlarmIntSeverity is set to 5 (CLEAR) when the alarm state (variable 4) is set to CLEAR. Note, a CLEAR alarm is sent with the same alarm ID as the “ACTIVE” alarm, that generated the original alarm. Since the alarm ID in both alarm messages is the same, this allows an NMS to automatically correlate alarms. The chart below displays how alarmIntSeverity is assigned.

	ACTIVE	ACK	CLEAR
<i>critical</i>	1	1	5
<i>major</i>	2	2	5
<i>minor</i>	3	3	5
<i>warning</i>	4	4	5
<i>info</i>	4	4	5

alarmProbableCause (OID: 1.3.6.1.4.1.36.2.15.25.5.1.7)

The alarmProbableCause indicates the cause of the alarm. Presently, this OID is not used and defaults to 0.

This field may be used in a future release of the IPFM product.

alarmEventType (OID: 1.3.6.1.4.1.36.2.15.25.5.1.8)

The alarmEventType indicates the type of alarm. Presently, this OID is not used and defaults to 0. This field may be used in a future release of the IPFM product.

Configuring the Network Management Station (NMS)

Any SNMP-compliant Network Management System can be used with IPFM. This section describes the configuration of the following:

- *ServerWORKS*
- *TeMIP*

Configuring the NMS with ServerWORKS

Install *ServerWORKS* on a Windows NT system and run IP Discovery from the Open Viewer window on the target network segment. The target nodes of interest should be visible on the displayed network topology map.

Enrolling the IPFM MIB into the ServerWORKS NMS

The following steps are required to load the *IPFM* MIB into the *ServerWORKS* NMS:

1. Copy the *IPFM* MIB (`/usr/opt/IPFM/src/event_man/ipfm_mib.my`) from the *Tru64 UNIX* system to the NMS.
2. Go into the ServerWORKS Manager main window.
3. Select the MIB Enroller option from the Tools menu pulldown.
4. Select the MIB Compiler option from the Compile menu pulldown.
5. Select the Open option from File menu pulldown.
6. Select the `ipfm.mib` file from the location where it was stored. The open menu disappears and you are returned to the MIB Compiler window.
7. Select the Enroll... option.
8. Shutdown and restart *ServerWORKS* so that the MIB will be recognized by the system.

Setting Up IPFM Alarm Traps

The following steps are required to set up the *IPFM* traps in the recommended configuration:

1. Double-click on the target node for the ServerWORKS Manager - [IP Discovery] window. This causes the System Browser window to come up for the target node.
2. Select Alarm Configuration... from the Tools menu pulldown.
3. Double-click on the "SNMP Traps" option in the "Alarm Type:" window. The "Add New SNMP Trap Alarms" window comes up.
4. Search down the "SNMP Traps:" window until you find the following IPFM traps: `ipfmcritTrap`, `ipfmmajorTrap`, `ipfmminorTrap`, `ipfmwarningTrap`, and `ipfmInfoTrap`.
5. Click on `ipfmcritTrap`. It will be displayed in the "Alarm message (can be modified):" window.
6. Select High from the "Severity" section and then click on the "OK" button.
7. Follow steps 3-6 for each of the remaining four traps (`ipfmmajorTrap`, `ipfmminorTrap`, `ipfmwarningTrap`, and `ipfmInfoTrap`), the only difference being that the severity should be set as follows:
 - a. `ipfmmajorTrap` – severity Medium.
 - b. `ipfmminorTrap` – severity Low.
 - c. `ipfmwarningTrap` – severity Informational
 - d. `ipfmInfoTrap` – severity Informational.
8. Select each newly defined trap in the "Currently defined alarms:" window and click on the "Enable" button.

You are now ready to remotely manage your *IPFM* software on the target node through SNMP.

Enrolling the IPFM MIB into the TeMIP NMS

The following steps are required to load the *IPFM* MIB into the *TeMIP* NMS:

1. Copy the *IPFM* MIB (`/usr/opt/IPFM/src/event_man/ipfm_mib.my`) from the *Tru64 UNIX* system to the NMS.

2. Compile the MIB into *TeMIP* using the following commands:

```
# mcc_tcpip_mtu ipfm_mib.my -n -s
# mcc_msl -Xad -mipfm_mib.ms,1
# mcc_ptb
```

3. Shutdown and restart *TeMIP* for the MIB to be recognized by the system using the following commands:

```
# temip_stop
# temip_start
```

4. On the AlphaServer running *IPFM*, add the following lines to the `/.profile` file. This instructs *IPFM* to send SNMP traps using the alternate SNMP trap style.

```
IPFM_NMS_ALARM=1
export IPFM_NMS_ALARM
```

5. Restart *IPFM* using the following commands:

```
# ipfm_shutdown
# ipfm_init.d
```

Configuring the Logical Storage Manager

If your system is not configured with external *StorageWorks* disks, proceed to the next chapter.

If you do need to configure the *Logical Storage Manager* (LSM), familiarize yourself with LSM prior to performing the configuration. For additional information about LSM, refer to the *Logical Storage Manager System Administrator's Guide*.

LSM setup is required on *TruCluster* clusters; it is optional (but recommended) on a simplex system. The simplex and duplex systems are configured with a local SCSI bus that contains one or more disks, tape drive, and the CD-ROM device. A BA35x *StorageWorks* shelf is also supplied on an external SCSI bus that contains one or more disks. LSM requires that a disk group *rootdg* be configured on the local SCSI disks, and that one or more different disk groups (not *rootdg*) be configured on the BA35x disks.

LSM requires a dedicated LSM simple disk to store the *rootdg* configuration database. The partition *rz0h* is used for the LSM configuration database and is initialized into the *rootdg* LSM disk group.

Note

If a duplex system is configured, the LSM setup and configuration on the BA35x disks need only be configured on one system. The system that is used to configure the BA35x disks should be the same one used to configure the *TruCluster* software.

To configure *LSM* volumes, perform the following steps:

1. To start LSM, enter the following command and press the Return key:

```
# /sbin/volinstall
```
2. LSM must have the *rootdg* disk group defined and configured on the local (non-shared) disks. The *rootdg* disk group cannot include any shared disks (disks on the external SCSI buses).

To create the *rootdg* LSM disk group on the *rz0h* partition, issue the following command:

```
# /sbin/volsetup rz0h
```

Where: *rz0h* is the *H* partition to be initialized into the LSM root diskgroup.

3. Add each disk or disk partition into LSM using the LSM Administrators menu:

```
# /usr/sbin/voldiskadm
```

Configuring the Logical Storage Manager

- a) Select the option *Add or initialize a disk*. Enter the disk or disk partition name for every disk in the BA35x *StorageWorks* shelf and press the Return key.

Note

If the disk or disk partition already contains data, the disk and/or partition must be encapsulated into LSM, not initialized.

- b) Enter the disk group name and press the Return key. Shared disks cannot belong to the `rootdg` disk group.
4. Create the new disk group(s) that includes all of the desired shared disks in the BA35x *StorageWorks* shelf. These disks can be divided into the appropriate subdisks, plexes and volumes. The plexes can either be simple or striped, and the volumes can have up to eight (8) plexes per volume.
5. To access the LSM graphical user interface, enter the following command:

```
# dxlsm &
```

If your graphical display is not the console, you will be required to define the `DISPLAY` environment variable to point to your graphics workstation.

If you do not have a graphics terminal, you may issue the raw LSM commands. Please refer to the LSM documentation for a description of these commands.

6. Using `dxlsm`, create the LSM volumes on the disks in the *StorageWorks* shelf. For maximum data integrity, the *StorageWorks* disks should be mirrored with one mirror component on each SCSI bus. The following commands can be used to create a volume that is mirrored and striped:
 - a) Use the mouse to select a disk.
 - b) Create one or more subdisks on each disk:

```
Advanced-Ops -> Subdisk -> Create
```

You are *required* to enter the subdisk name, and the subdisk length.
 - c) If there are more disks in the LSM configuration, repeat steps a and b for each disk.
 - d) Create one or more plexes:

```
Advanced-Ops -> Plex -> Create
```

You are required to enter the plex name and the layout.
 - e) Create one or more volumes:

```
Advanced-Ops -> Volume -> Create
```

You are required to enter the volume name.
 - f) Add the subdisk(s) to the plex(s) using the mouse (drag and drop).
 - g) Add the plex(s) to the volume(s) using the mouse (drag and drop).
 - h) Start the Volume(s) by selecting the specific volume (using the mouse), then use the following menus and options:

```
Advanced-Ops -> Volume -> Start
```

The volume should be ready to use.

Configuring AdvFS

You should familiarize yourself with the *Advanced File System* (AdvFS) Utilities prior to performing the AdvFS configuration. For additional information about the AdvFS Utilities, refer to the *Advanced File System and Utilities Guide to File System Administration*.

Your system was factory installed with both the `root` and the `/usr` partitions configured, using *Advanced File System* (AdvFS).

To launch the AdvFS Utilities GUI, enter the following command and press the Return key:

```
# dxadvfs &
```

If you do not have a graphics terminal, you may issue the raw AdvFS commands. Please refer to the AdvFS documentation for a description of these commands.

Note

The LSM volumes should be set up (and started) prior to configuring AdvFS domains and filesets.

Within the interface, perform the following commands:

1. Specify the desired volume (as defined by LSM), and select the new domain name using the following menu options:
`Setup -> Make File Domain`
2. Select the new file domain, and select the MAKE FILESET button using the following menu options:
`Manage -> File Domain`
3. Enter the fileset name and press the Return key. If this is a *TruCluster* cluster, do not mount the fileset and do not add the fileset/mount point to the `/etc/fstab` file.

Configuring TruCluster ASE Software

Configuring the *TruCluster Available Server Environment* (ASE) software is optional, and may not be applicable to your configuration.

You should familiarize yourself with the *TruCluster Available Server* software prior to performing the *TruCluster* configuration. For additional information about the *TruCluster* product, refer to the *TruCluster Available Server* documentation.

Note

The *TruCluster* product need only be configured on one of the *AlphaServer* systems in the duplex system. The *TruCluster* product automatically copies the configuration database to the other system in the cluster.

To configure the *TruCluster* product, follow these six steps:

1. The Network Time Protocol (NTP), which comes with the *Tru64 UNIX* operating system, must be running on all cluster members. If you are configuring a duplex system, the *AlphaServer* systems must be running NTP. NTP requires an NTP server as a reference. The node name and IP address of the NTP server must be in the */etc/hosts* file prior to running `ntpsetup`.

The following example output shows you how to configure NTP using the `ntpsetup` script (responses are in bold type.) Your installation may require answers different from those shown in the example. Refer to the *Tru64 UNIX System Administration* documentation for instructions on how to run the `ntpsetup` script.

```
# /usr/sbin/ntpsetup
```

```
*****
*
*           Network Time Protocol (NTP V3) Setup           *
*
*****
```

`Ntpsetup` configures and runs the Network Time Protocol service (NTP) for your system. NTP is a distributed time service which provides accurate, synchronized time to each host in a hierarchical network of systems. `Ntpsetup` runs the University of Delaware's `xntpd V3` daemon, including support for authentication.

Each system in an NTP hierarchy must either have a local reference clock or be served by other NTP hosts (local or remote). `Ntpsetup` sets up your host to be served by other NTP hosts. If you have a local reference clock, please see the documentation for the setup procedure.

Configuring TruCluster ASE Software

[Press the RETURN key to continue] : <RETURN>

Default answers are shown in square brackets ([]). To use a default answer, press RETURN.

Authentication mode

Authentication mode causes the server to synchronize with peers only if the peer has been correctly authenticated using a trusted key and key identifier.

In choosing to enable authentication, you must already know the key number and the key identifier in order to correctly configure each host name and the /etc/ntp.keys file.

If you do not know this information, enter 'n' in response to the next question. See the Network Administration manual and ntp.conf(4) for information on authentication.

Would you like to enable authentication (y/n) [n]? **n**

NTP Server/Peer Selection

During the selection of servers and peers, you will be asked for a hostname, and for the mode, server or peer, to be associated to each hostname.

Press RETURN to terminate the list.

Hostname of NTP server/peer [no default]: **ipsys1**

Mode for ipsys1 (server or peer) (s/p) [s]? **s**

Looking up host ipsys1 ... found.

Is ipsys1 running ntpd (V1) or xntpd (V2 or V3) (V1/V2/V3) [V3]? **v3**

Hostname of NTP server/peer [no default]:

The list of NTP servers is:
server ipsys1 version 3

Enter "r" to REDO the servers list, "e" to EXIT the ntpsetup procedure, or "c" to CONTINUE [no default]: **c**

Created ntp.conf

IMPORTANT NOTE

If any of the NTP servers you specified are not in the same IP subnet as your system, you must run either routed or gated in order to access them. Please see the networking documentation to set up one of these services.

[Press RETURN to continue] : <RETURN>

Xntpd (the NTP daemon) Options

 NOTE: The default answers are RECOMMENDED.

Correct large time differences, -g

If your system time differs from the network time by more than 1000 seconds while xntpd is running, the daemon will suspect that something is very wrong with your system or your servers. It will then log a message to the syslog and exit, to allow the system manager to resolve the problem.

The -g option allows xntpd to correct large time differences without logging a message or exiting. It should be used by systems which are not monitored very closely by a system manager (such as workstations).

Would you like to use the -g option (y/n) [y]? **y**

Prevent time getting set backwards, -x

The -x option prevents xntpd from correcting time when the offset is negative. This can happen for example if the server(s) have fallen behind for some reason.

Would you like to use the -x option (y/n) [n]? **n**

Configuring your system to run NTP... done.

Starting the NTP daemon (xntpd)...
 Setting kernel timezone variable
 Setting the current time and date with ntpdate
 Network Time Service started

To monitor NTP, enter "/usr/bin/ntpq -p".

***** NTPSETUP Complete *****

2. The *TruCluster* service name and IP address must be loaded into the */etc/hosts* file on each server. The network configuration file */etc/hosts* must contain the *TruCluster* service name(s) and IP addresses that will be used by the *TruCluster* configuration. This file can be modified using a text editor, or by using the *netsetup* script.

The following example output shows you how to configure the */etc/hosts* file using the *netsetup* script (responses are in bold type.) Your installation may require different answers to the questions than those shown in the example. Refer to the *Tru64 UNIX System Administration* documentation for instructions on how to run the *netsetup* script.

/usr/sbin/netsetup

**** MAIN MENU ****

- 1 Configure Network Interfaces
- 2 Enable/Disable Network Daemons and Add Static Routes
- 3 Add/Delete Host Information
- 4 Display Network Configuration
- 5 Exit

Enter the number for your choice: **3**

Configuring TruCluster ASE Software

```
      **** HOST INFORMATION MENU ****

1  /etc/hosts
2  /etc/hosts.equiv
3  /etc/networks
4  Exit

Enter the number for your choice: 1

***** ADD/DELETE HOSTS IN /etc/hosts *****

You can add or delete hosts in /etc/hosts.  When finished, press
the RETURN key at the prompt that asks whether you want to add
or delete hosts.

Enter whether you want to "(a)dd" or "(d)elele" hosts in /etc/hosts.
If you are finished, press the RETURN key: a
You want to "add" to /etc/hosts.  Is this correct [yes]? yes
Enter the host name, aliases and Internet Protocol (IP) address for
each host in the network.  Enter this information on separate lines
when prompted.  This information is added to the /etc/hosts file.

Enter the name of the host to add to /etc/hosts.
If you are finished, press the RETURN key: nfs001

You want to add host "nfs001".
Is this correct [yes]? yes

Enter any aliases for "ipsys1", separated by a space.
If you do not want any aliases, press the RETURN key: <RETURN>

You do not want any aliases for "nfs001".
Is this correct [yes]? yes

Enter the Internet Protocol (IP) address of "nfs001"
in dot notation: 16.126.224.216

The IP address for "ipsys1" is "16.126.224.216".
Is this correct [yes]? yes

The /etc/hosts entry looks like:

      16.126.224.216 nfs001

Is this correct [yes]? yes
16.126.224.216 nfs001 " is added to /etc/hosts

Enter the name of the host to add to /etc/hosts.
If you are finished, press the RETURN key: <RETURN>

Enter whether you want to "(a)dd" or "(d)elele" hosts in /etc/hosts.
If you are finished, press the RETURN key: <RETURN>
```

```
      **** HOST INFORMATION MENU ****

1  /etc/hosts
2  /etc/hosts.equiv
3  /etc/networks
4  Exit

Enter the number for your choice: 4
```


**** MAIN MENU ****

- 1 Configure Network Interfaces
- 2 Enable/Disable Network Daemons and Add Static Routes
- 3 Add/Delete Host Information
- 4 Display Network Configuration
- 5 Exit

Enter the number for your choice: **5**

3. If providing an Network File System (NFS) disk service, ensure that NFS is set up for both incoming and outgoing support. Use the command `nfsetup` to configure the Network File System daemons.

The following example output shows how to configure an NFS file system. User responses are in bold type. Your installation may require answers different from those shown in the example. Refer to the *Tru64 UNIX System Administration* documentation for instructions on how to run the `netsetup` script.

At the # superuser prompt, enter the following command and press the Return key:

```
# nfsetup
```

```
Checking kernel configuration...
```

```
The nfsetup command configures the network file system (NFS)
environment for your system. All systems using NFS facilities
must run the Remote Procedure Call (RPC) port mapper daemon.
An entry for this daemon is in /sbin/init.d/nfs
along with entries for the optional daemons you select.
```

```
You will be asked a series of questions about your system.
Default answers are shown in square brackets ([]). To use a
default answer, press the RETURN key.
```

```
Local locking supports local file and file region locking.
NFS locking supports local and remote (NFS) file and file region
locking. If you would like to disable the NFS locking
functionality, then answer 'n' to the following question.
```

```
NFS locking to be enabled [y] ? y
```

```
Will you be exporting any directories [n] ? y
```

```
Do you want to allow non-root mounts [n] ? n
```

```
Systems that export NFS directories must run /usr/sbin/nfsd to
handle NFS requests from clients. It is suggested that between 8 and 24
(inclusive) nfsd daemons be run. For average workload situations,
8 is a good number to run. There are two types of server daemons.
One processes UDP requests, the other processes TCP requests. Both
are started by nfsd.
```

```
Enter the number of TCP daemons to run (0 to 128) [8] : 8
```

```
Enter the number of UDP daemons to run (0 to 120) [8] : 8
```

```
The property list daemon (proplisd) allows property list
operations to be performed on exported files. The daemon is
not started by default. To enable proplisd, answer
'y' to the following question.
```

```
Would you like to run the property list daemon [n] ? n
```

Configuring TruCluster ASE Software

NFS clients can use block I/O daemons for buffering data transfers, although their use is not required. It is suggested that between 4 and 12 nfsiod daemons be run. The best number to run is dependent on server speed and network bandwidth. To work most efficiently with Digital Unix servers, 7 is a good number to run.

Enter the number of block I/O daemons to run [7] : **7**

The PC-NFS daemon (rpc.pcnfsd) provides authentication and print services for PC-NFS clients. The daemon is not started by default. To enable rpc.pcnfsd, answer 'y' to the following question.

Would you like to run the PC-NFS daemon [n] ? **n**

The automount daemon automatically and transparently mounts and unmounts NFS file systems on an as-needed basis. See the automount(8) manpage for details.

Would you like to run the automount daemon [n] ? **n**

You are now setting up your directory export list. Enter the full pathnames of the directories to be exported. For each pathname, enter the network group names and/or machine names to be given access permission to this directory, or a null list to indicate general permission. (Network groups are ONLY available on machines using NIS). This information is placed in the /etc/exports file. Press the RETURN key to terminate the pathname and permissions lists.

Enter the directory pathname: **<RETURN>**
Directory export list complete...

You will now be asked to provide information about the remote file systems you wish to access. First list the name of the remote host serving the directories you wish to mount, then give the full directory pathnames. Also, for each remote directory, you must specify the full directory pathname of the mount point on the local machine and whether the mount is read-only or read-write. (Nfssetup will create the mount point directory if it does not already exist.) Press the RETURN key to terminate the host and directory pathname lists:

Enter the remote host name: **<RETURN>**
Remote directory mount list complete...

Please confirm the following information which you have entered for your NFS environment:

8 TCP server daemons, 8 UDP server daemons
7 nfsiod daemons
locking daemons installed

No directories (in addition to those already in /etc/exports) exported

No additional remote directories to mount

Enter "c" to CONFIRM the information, "q" to QUIT nfssetup without making any changes, or "r" to RESTART the procedure [no default]: **c**

Updating files:
/etc/rc.config

The necessary NFS daemon entries have been placed in the file /sbin/init.d/nfs. In order to begin using NFS, you must now start the daemons and mount any remote directories you wish to access. You may either

allow nfssetup to start these daemons automatically or invoke them by hand, but in either case they will be started automatically on subsequent reboots.

If you choose to have nfssetup stop and start the daemons now (without a reboot), all nfs-related daemons will be stopped, then those you chose to be run in the preceding questions will be started. In addition, the remote directories listed in /etc/fstab will be mounted.

```
Would you like nfssetup to stop/start the daemons now [y]? y
kill: 391: no such process
NFS mount daemon started
NFS export service started
NFS IO service started
NFS Locking: rpc.statd and rpc.lockd started
Mounting NFS filesystems
```

The NFS daemons for your machine have been started.

[Press the RETURN key to continue]: **<RETURN>**

***** NFSSETUP COMPLETE *****

4. Use the asemgr menu to configure cluster members and services. The first time the asemgr menu is entered, the user is prompted for the names of every system in the *TruCluster* cluster. When the list is complete, the asemgr utility will present the user with the following menus:

```
# asemgr
  TruCluster Available Server Environment (ASE)
                ASE Main Menu
a)  Managing the ASE          -->
m)  Managing ASE Services    -->
s)  Obtaining ASE Status     -->

x)  Exit                      ?)  Help
```

Enter your choice: **m**

Managing ASE Services

```
c)  Service configuration    -->
r)  Relocate a service
on) Set a service on line
off) Set a service off line
res) Restart a service
s)  Display the status of a service
a)  Advanced utilities      -->

x)  Exit to the Main Menu    ?)  Help
```

Enter your choice [x]: **c**

Service Configuration

```
a)  Add a new service
m)  Modify a service
d)  Delete a service
s)  Display the status of a service

x)  Exit to Managing ASE Services  ?)  Help
```

Configuring TruCluster ASE Software

Enter your choice [x]: **a**

Adding a service

Select the type of service:

- 1) NFS service
- 2) Disk service
- 3) User-defined service

- x) Exit to Service Configuration ?) Help

Enter your choice [1]: **1**

You are now adding a new NFS service to ASE.

An NFS service consists of an IP host name and disk configuration that are failed over together. The disk configuration can include UFS file systems, AdvFS filesets, or LSM volumes.

NFS Service Name

The name of an NFS service is a unique IP host name that has been set up for this service. This host name must exist in the local hosts database on all ASE members.

Enter the NFS service name: **ase001**

Checking to see if ase001 is a valid host...

Specifying Disk Information

Enter one or more UFS device special files, AdvFS filesets, or LSM volumes to define the disk storage for this service.

For example: UFS device special file: /dev/rz3c
 AdvFS fileset: domain1#set1
 LSM volume: /dev/vol/dg1/vol01

To end entering disk information, press the 'Return' key at the prompt.

Enter a device special file, an AdvFS fileset, or an LSM volume as storage for this service (press 'Return' to end): **tcr_domain#tcr**

ADVFS domain `tcr_domain` has the following volume(s):

/dev/vol/tcr/vol01

Is this correct (y/n) [y]: **y**

Following is a list of device(s) and pubpath(s) for disk group tcr:

DEVICE PUBPATH

rz9 /dev/rz9g

```
rzl7 /dev/rzl7g
```

Is this correct (y/n) [y]: **y**

Enter a directory pathname(s) to be NFS exported from the storage area "tcr_domain#tcr". Press 'Return' when done.

Directory pathname: **/asel**

Enter a host name, NIS netgroup, or IP address for the NFS exports list. (press 'Return' for all hosts):

Directory pathname:

AdvFS Fileset Read-Write Access and Quota Management

Mount `tcr_domain#tcr` fileset with read-write or read-only access?

- 1) Read-write
- 2) Read-only

Enter your choice [1]: **1**

You may enable user, and group and fileset quotas on this file system by specifying the full pathnames for the quota files. Quota files must reside within the fileset. Enter "none" to disable quotas.

User quota file path [/var/ase/mnt/nfs001/asel/quota.user]: **<Return>**

Group quota file path [/var/ase/mnt/nfs001/asel/quota.group]: **<Return>**

AdvFS Mount Options Modification

Enter a comma-separated list of any mount options you want to use for the `tcr_domain#tcr` fileset (in addition to the defaults listed in the mount.8 reference page). If none are specified, only the default mount options are used.

Enter options (Return for none): **<Return>**

Specifying Disk Information

Enter one or more UFS device special files, AdvFS filesets, or LSM volumes to define the disk storage for this service.

```
For example: UFS device special file: /dev/rz3c
AdvFS fileset:          domain1#set1
LSM volume:            /dev/vol/dg1/vol01
```

To end entering disk information, press the 'Return' key at the prompt.

Enter a device special file, an AdvFS fileset, or an LSM volume as storage for this service (press 'Return' to end): **<Return>**

Modifying user-defined scripts for `nfs001`:

Configuring TruCluster ASE Software

- 1) Start action
- 2) Stop action
- 3) Add action
- 4) Delete action

- x) Exit - done with changes

Enter your choice [x]: **x**

Selecting an Automatic Service Placement (ASP) Policy

Select the policy you want ASE to use when choosing a member to run this service:

- b) Balanced Service Distribution
- f) Favor Members
- r) Restrict to Favored Members

- x) Exit to Service Configuration ?) Help

Enter your choice [b]: **b**

Selecting an Automatic Service Placement (ASP) Policy

Do you want ASE to consider relocating this service to another member if one becomes available while this service is running (y/n/?): **y**

Enter 'y' to add Service 'nfs001' (y/n): **y**

Adding service...

Starting service...

Saving the updated database...

Service nfs001 successfully added...

Service Configuration

- a) Add a new service
- m) Modify a service
- d) Delete a service
- s) Display the status of a service

- x) Exit to Managing ASE Services ?) Help

Enter your choice [x]: **x**

Managing ASE Services

- c) Service Configuration -->
- r) Relocate a service
- on) Set a service on line
- off) Set a service off line
- res) Restart a service
- s) Display the status of a service

```

a)  Advanced Utilities      -->

x)  Exit to the Main Menu   ?)  Help

```

Enter your choice [x]: **x**

DECsafe Available Server Environment (ASE)

ASE Main Menu

```

a)  Managing the ASE      -->
m)  Managing ASE Services -->
s)  Obtaining ASE Status -->

x)  Exit                  ?)  Help

```

Enter your choice: **x**

5. If configuring a *TruCluster* NFS service, you may want to configure the NFS mount points for the service. The *TruCluster* product automatically mounts the disk service on only one node in the cluster. The other nodes will not have the disk service mounted directly. To allow local access to the disk service, add the NFS remote mount line to your `/etc/fstab` file.

An example `/etc/fstab` file follows:

```

/dev/rz0a      /      advfs  rw 1 1
/proc         /proc  procfs  rw 0 0
/dev/rz0b     swapl  ufs     sw 0 2
usr_domain#usr /usr   advfs  rw 0 0
/ase1@nfs001  /ase1  nfs     rw 0 0    # TruCluster service mountpoint

```

Where: `/ase1` is the remote mount point, and `nfs001` is the *TruCluster* NFS service name.

6. The *TruCluster* software notifies the `root` account, by means of mail messages, of critical problems detected on one or more member systems. The `root` account mail should either be forwarded to another system or checked periodically.

Glossary

agent

A background task running on each monitored node, scanning devices and data structures and generating event messages in an internal list. The agent responds to requests for information by the network management station (NMS). The agent is responsible for performing get and set operations, generating traps, and controlling access.

AlphaServer

Compaq's new generation of server systems based on the Alpha 64-bit computing architecture.

boot

Short for bootstrap. To load an operating system into memory.

bus

A collection of many transmission lines or wires. The bus interconnects computer system components, providing a communications path for addresses, data, and control information or external terminals and systems in a communications network.

Ethernet

The IEEE 802.3 standard local area network.

event

An event is a problem or situation detected by the system.

hub

A central device, usually in a star topology local area network (LAN), to which each network module is attached.

initialization

The sequence of steps that prepare the computer system to start. Initialization occurs after a system has been powered up.

ISA

Industry Standard Architecture. An 8-bit or 16-bit industry-standard I/O bus, widely used in personal computer products. The EISA bus is a superset of the ISA bus.

MAC (media access control) address

A unique 48-bit binary number (usually represented as a 12-digit hexadecimal number) encoded in a device's circuitry to identify it on a local area network.

module

A hardware or software component that is a self-contained system interacting with a larger system. Hardware modules are often made to plug into a main system.

network

A collection of computers, terminals, and other devices together with the hardware and software that enables them to exchange data and share resources over either short or long distances.

protocol

A formal set of rules governing the format, timing, sequencing, and error control of exchanged messages on a data network.

SCSI

Small Computer Systems Interface. An ANSI-standard interface for connecting disks and other peripheral devices to computer systems. Some devices are supported under the SCSI-1 specification; others are supported under the SCSI-2 specification.

server

A network node or specialized device that provides and manages access to shared network resources, such as hard disks, printers, and software.

Simple Network Management Protocol (SNMP)

A high-level, standards-based protocol for network management, usually used in TCP/IP (Transmission Control Protocol/Internet Protocol) networks.

SNMP agent

An entity in a hardware device that executes SNMP requests.

StorageWorks

Compaq's modular storage subsystem (MSS), which consists of a family of low-cost mass storage products that can be configured to meet current and future storage needs.

Telnet

The TCP/IP standard protocol for remote terminal connections. Using Telnet, a user at one site can connect to a timesharing system at another site as if the user's terminal is connected directly to the remote machine.

terminal server

A module that allows a terminal to connect to a network node.

Transmission Control Protocol (TCP)

The transport protocol offering a connection-oriented transport service in the Internet suite of protocols.

Index

A

Advanced File System
 AdvFS configuration, 5–1
AlphaServer IP Platform
 components, 1–1

C

Configuration
 Advanced File System, 5–1
 Logical Storage Manager
 volumes, 4–1
 network /etc/hosts file, 2–6
 Network File System (NFS),
 6–5
 network setup device, 2–2
 of duplex system, 1–2, 2–1,
 4–1, 6–1
 summary of steps, 2–1
 Tru64 UNIX operating system,
 2–2
Console
 connecting, 2–2
Conventions
 used in this guide, vi

D

Documentation
 related, vi

I

IPFM MIB
 enrolling for *ServerWORKS*,
 3–6
 enrolling for *TeMIP*, 3–7

N

Network
 address, 1–2
 configuring
 /etc/hosts file, 2–6
 controllers, 1–2
 device configuration, 2–2
 node names and TCP/IP
 addresses, 1–2
Network File System (NFS)
 configuring, 6–5

S

ServerWORKS
 configuring on NMS, 3–6
SNMP agent configuration file, 3–4
System configuration
 overview, 1–1
System console
 connecting, 1–2

T

TCP/IP, 1–2
TruCluster software
 configuring, 6–1
 documentation, 6–1