Contents

List of Figures xiii

List of Tables xv

IRIX Admin Manual Set xvii

About This Guide xix
What This Guide Contains xix
Part I xix
Part II xix
Part III xx
Conventions Used in This Guide xx
How to Use This Guide xxi
Additional Resources xxi
Books xxi
Internet Resources xxii
World Wide Web Resources for System Security xxii
USENET News Groups xxiii
Commercial and Free Products xxiii
Connecting to the Internet xxiv

PART I Backup

1. Planning a Backup Strategy 3
Types of Backup Media 3
Choosing a Backup Tool 4

Backup Strategies 6
When to Back Up Data and What to Back Up 6
Root Filesystems 6
User Filesystems 7
Incremental Backups 7
Backing Up Files Across a Network 8
Automatic Backups 9
Storing Backups 9
How Long to Keep Backups 10
Reusing Tapes 10

2. Backup and Recovery Procedures 11
General Backup Procedure 12
System Backups 13
Recovery After System Corruption 13
Changing the Default Backup Device 17
bru 19
Saving Data With bru 19
Estimating Space Required for Backup 19
Backing Up a Filesystem With bru 20
Backing Up Files With bru 20
Saving Files by Modification Date 20
Saving Files Using Data Compression 20
Incremental Backups With bru 21
Examining bru Archives 21
Comparing Archived Files 21
Inspecting an Archive for Consistency 22
Restoring bru Archives 22
Restoring a Filesystem With bru 23
Restoring Individual Files With bru 23

Backup and Restore 23
Estimating Space Required for Backup 24
Saving Data with Backup 24
Restoring Backup Archives With Restore 25
Restoring a Filesystem With Restore 25
dump and restore 26
Saving Data With dump 26
Saving a Filesystem With dump 27
Incremental Backups With dump 27
Restoring dump Archives With restore 28
Restoring a Filesystem With restore 28
Restoring Individual Files With restore 28

xfsdump and xfsrestore 30
Features of xfsdump and xfsrestore 31
Media Layout 32
Terminology 32
Possible Dump Layouts 32
Saving Data With xfsdump 40
Specifying Local Media 40
Specifying a Remote Tape Drive 42
Backing Up to a File 43
Reusing Tapes 44
Erasing Used Tapes 44
Incremental and Resumed Dumps 45
Examining xfsdump Archives 47
Restoring xfsdump Archives With xfsrestore 50
Simple Restores With xfsrestore 52
Restoring Individual Files with xfsrestore 54
Network Restores with xfsrestore 55
Interactive Restores With xfsrestore 55
Cumulative Restores With xfsrestore 57
Interrupting xfsrestore 60
housekeeping and orphanage Directories 61
Using xfsdump and xfsrestore to Copy Filesystems 62
tar 62
Saving Data With tar 62
Backing Up Files With tar 63
Saving Files by Modification Date 63
Incremental Backups With tar 63
Examining tar Archives 64
Restoring tar Archives 64

cpio 65
Saving Data With cpio 65
Backing Up Files With cpio 65
Saving Files by Modification Date 65
Incremental Backups With cpio 66
Examining cpio Archives 66
Restoring cpio Archives 67
dd 67

3. Troubleshooting Backup and Recovery 69
Unreadable Backups 69
Reading Media From Other Systems 69
Errors Creating the Backup 71
Restoring the Wrong Backup 72
Testing for Bad Media 73
Backup and Recovery Error Messages 74

PART II Security

4. System Security 79
Standard Security Features 80
Security Guidelines 81
Password Administration 84
Choosing Passwords 84
PROM Passwords 85
Clearing the PROM Password Using nvram 86
Setting the PROM Password From the Command Monitor 86
Second (Dialup) Passwords 87
Creating a Shadow Password File 89
Password Aging 90
Password Aging With the *passwd* Command 90
Using Password Aging Manually 91
Using pwck to Check the Password File 93

Login and Account Administration 93
Special Accounts 93
Locking Unused Logins 94
System Login Options 95
Restricting root Logins 96
Maximum Login Attempts (MAXTRYS) 97
Length of Time to Disable a Line (DISABLETIME) 98
Recording Login Attempts 98
Forcing a Password 98
Displaying the Last Login Time 98
Set-UID and Set-GID Permissions 99
Checking for Set-UID Files Owned by root 99
Checking for Set-UIDs in the root Filesystem 100
Checking Set-UIDs in Filesystems Other Than root 101
General File and Directory Permissions 102
Accounts Shipped Without Passwords 103
Security File and Command Reference 104

5. Network Security 107
Local Area Network Access 107
Controlling Network Access 108
Limiting X11 Access 109
xhost Command 109
X*.xhost File 110
Local inetd Services 111
Network Security and Firewalls 111
What is the Internet? 112
Network Security Issues 112
What Is a Firewall? 113
Firewall Design Philosophy 114
World Wide Web Issues 115

Hardware Configuration 115
Routers and Firewalls 116
Configuring SGI Hardware for Use as a Firewall 117
Dual-Homed Host Firewall 117
Screened Host Gateway 117
IRIX Configuration 119
Network Software Setup on a Dual-Homed Host 120
Tightening Security in IRIX 120
Disable Forwarding of IP Packets 120
Limiting inetd Services 121
Password Protection 123
Limiting rpc Services Access 124
Disabling NIS (YP) 124
Limiting NFS Access 125
Setting Up a Proper Log File 125
Checking Software Integrity 125
Educating Users 126
Internal Network Configuration 127
Domain Name System (DNS) 127
Mail Configuration 127
Sendmail Configuration and Mail Aliases 127
Spool Isolation 128
Using Proxy Servers 128

PART III Accounting

6. Administering the System Audit Trail 133
Enabling Auditing 134
Default Auditing 134

Customizing Auditing 135
What Should I Audit? 135
Auditable Events 137
Using satconfig 141
Using sat_select 142
Saving and Retrieving Your Auditing Environment 143
Placing the Audit Files 143
How to Audit a Specific User 145
How to Audit a File 146
How to Audit a Label Under Trusted IRIX/B 146
Understanding the Audit Data 147
Potential Security Violations 148
Use and Abuse by Outsiders 148
Attempts at Unauthorized Entry 148
System Usage at Unusual Hours or From Unusual Locations 149
Connections with Machines Outside the Local Network 150
Use and Abuse by Insiders 150
File Permission Violations 150
Unexpected Use of Root Privilege 151
Activity by Particularly Interesting Users 152
Access to Particularly Interesting Files or Resources 152
Proper and Improper Management 153
Modifications of System Data Files 153
Modifications of Attributes of System Programs 153
Manipulation of the Audit Trail 154
Archiving Audit Data 154
Removing Audit Data 154
Recovering From Audit File Overflow 155

7. System Accounting 157
Process (System) Accounting 157
Parts of the Process Accounting System 158
Turning on Process Accounting 159
Turning Off Process Accounting 159
Controlling Accounting File Size 160
Accounting Files and Directories 160
Daily Operation 160
Setting Up the Accounting System 162
runacct 163
Recovering from a Failure 165
Restarting runacct 166
Fixing Corrupted Files 166
Fixing wtmp Errors 166
Fixing tacct Errors 167
Updating Holidays 168
Daily Reports 168
Daily Usage Report 170
Daily Command and Monthly Total Command Summaries 171
Files in the /var/adm Directory 172
Files in the /var/adm/acct/nite Directory 173
Files in the /var/adm/acct/sum Directory 173
Files in the /var/adm/acct/fiscal Directory 174
Additional Resources 174

Index 175