

Contents

| | <i>Page</i> |
|---|-------------|
| Preface | xix |
| UNICOS system administration publications | xix |
| Related publications | xx |
| Ordering Cray Research publications | xxii |
| Conventions | xxii |
| Reader comments | xxiv |
| | |
| Introduction to System Administration [1] | 1 |
| Overview of contents | 1 |
| UNICOS multilevel security (MLS) feature and the Cray ML-Safe configuration | 2 |
| User Exits | 3 |
| | |
| File System Planning [2] | 7 |
| Introduction to UNICOS file systems | 7 |
| File system overview | 8 |
| File system types | 8 |
| File system strategies | 9 |
| File system concepts | 11 |
| Disk organization | 11 |
| Disk flawing (IOS-E and IPN-1 only) | 12 |
| Disk striping | 13 |
| Disk mirroring | 13 |
| Physical devices | 14 |
| Simple logical devices | 14 |
| Striped logical devices | 14 |
| | |
| SG-2301 10.0 | iii |

| | <i>Page</i> |
|---|-------------|
| Mirrored logical devices | 15 |
| Logical device descriptor files | 15 |
| Using the <code>mkspice(8)</code> command (IOS-E and IPN-1) | 15 |
| Creating file system nodes | 17 |
| Creating physical devices | 17 |
| Examples of physical device creation | 19 |
| Creating a physical disk device | 19 |
| Creating RAM disks | 21 |
| Creating SSD slices | 22 |
| Creating physical devices (GigaRing systems) | 22 |
| Creating logical devices | 23 |
| Creating simple logical devices | 24 |
| Creating striped logical devices | 25 |
| Creating mirrored logical devices | 26 |
| Restrictions on striped and mirrored logical devices | 27 |
| Creating logical descriptor files | 27 |
| Defining alternate disk paths | 28 |
| Configuring alternate paths on FCN devices | 29 |
| Configuring alternate paths on FCN devices | 29 |
| Failure modes | 32 |
| Shared dump and swap configuration | 33 |
| Configuring disk arrays | 36 |
| Installing an array | 36 |
| Replacing a failing spindle | 39 |
| Converting RAID members to single spindles | 40 |
| Software Limitations | 41 |
| File system initialization | 42 |
| Inode allocation strategies | 43 |

| | <i>Page</i> |
|---|-------------|
| rrf allocation | 44 |
| rrd1 allocation | 44 |
| rrda allocation | 44 |
| Inode region allocation | 45 |
| Labeling a file system | 46 |
| Mirrored file systems | 47 |
| Creating a mirrored file system | 47 |
| Configuring a mirrored device | 48 |
| Default configuration | 49 |
| Mirrored devices during startup | 50 |
| Manual startup of mirrored file systems | 51 |
| Performance considerations | 51 |
| Logical device cache | 51 |
| Setting cache configuration | 52 |
| Displaying cache statistics | 53 |
| Aging and threshold parameters of ldcache | 54 |
| System buffer cache | 55 |
| Using SSD as a file system | 56 |
| Secondary data segments (SDS) | 56 |
| File system placement | 57 |
| Startup and Shutdown Procedures [3] | 59 |
| System initialization | 59 |
| Deadstarting the system | 59 |
| Initializing the UNICOS operating system | 60 |
| Setting the system date and time | 61 |
| Setting the system time zone | 62 |
| Time-zone information | 62 |
| Time-zone example 1 | 64 |

| | <i>Page</i> |
|---|-------------|
| Time-zone example 2 | 65 |
| System shutdown | 65 |
| The shutdown command | 65 |
| System shutdown configuration | 67 |
| The shutdown.pre user exit | 67 |
| The shutdown.mid user exit | 68 |
| The shutdown.pst user exit | 68 |
| System shutdown procedures | 69 |
| Run-level configuration | 71 |
| Changing run level | 72 |
| Strategies for using run levels | 72 |
| Single-user mode | 72 |
| Multiuser mode | 73 |
| Dedicated system | 74 |
| Files that control run-level activity | 75 |
| The /etc/inittab file | 75 |
| The /etc/bcheckrc script | 76 |
| The /etc/rc script | 76 |
| System multiuser startup | 76 |
| Load the /etc/config/rcoptions file | 77 |
| Set up the /etc/rc log file | 84 |
| Execute /etc/rc.pre | 84 |
| Make and mount /tmp | 84 |
| Mount the /usr file system | 85 |
| Make and mount /usr/tmp | 85 |
| Preserve interrupted vi/ex sessions | 85 |
| Mount user file systems | 85 |
| Mount /proc | 85 |

| | <i>Page</i> |
|---|-------------|
| Activate logical device cache | 85 |
| Execute /etc/rc.mid | 86 |
| Perform administrative cleanup | 86 |
| Start the security log daemon | 86 |
| Start accounting | 86 |
| Start system activity data collection | 86 |
| Activate category SYS1 system daemons | 87 |
| Activate netstart | 87 |
| Activate category SYS2 system daemons | 87 |
| Create network access list | 87 |
| Set MLS wildcard files and directories | 87 |
| Execute /etc/rc.pst | 88 |
| Complete the multiuser startup | 88 |
| File System Maintenance [4] | 89 |
| Mounting and unmounting file systems | 89 |
| File system utilities | 90 |
| File system backup and restoration | 91 |
| Local backup | 91 |
| Using the dump command | 92 |
| Using the restore command | 94 |
| Remote backup | 98 |
| File system checking and repair with fsck | 99 |
| Overview of file system operation | 99 |
| Using fsck | 100 |
| fsck phases | 103 |
| Initialization phase | 103 |
| Phase 1 | 104 |
| Phase 2 | 104 |

| | <i>Page</i> |
|---|-------------|
| Phase 2X | 104 |
| Phase 3 | 104 |
| Phase 4 | 105 |
| Phase 5 | 105 |
| Phase 6 | 105 |
| Termination phase | 105 |
| | |
| Basic Administration [5] | 107 |
| Using the cron and at utilities | 107 |
| Administrative use of cron | 107 |
| Administrative use of at | 109 |
| Restricting use of crontab and at utilities | 111 |
| The temporary directory (TMPDIR) | 111 |
| Communicating with users | 112 |
| The wall command | 112 |
| The /etc/motd file | 113 |
| The /etc/issue file | 113 |
| The /usr/news directory | 114 |
| The write utility | 114 |
| The mail utility | 116 |
| Monitoring system security | 117 |
| Super-user privileges | 117 |
| Password security for super user | 117 |
| Physical security | 118 |
| setuid programs | 118 |
| root PATH | 119 |
| User security | 120 |
| The umask utility | 120 |
| Default PATH variable | 121 |
| User groups | 121 |

| | <i>Page</i> |
|--|-------------|
| File-owner fraud | 121 |
| Login attempts | 122 |
| Partition security | 122 |
| Job and process recovery | 122 |
| Restrictions to job and process recovery | 123 |
| Restrictions common to batch and interactive | 123 |
| Recovery restrictions unique to batch | 125 |
| Checkpoint and restart errors | 125 |
| Examining the restart-information buffer | 125 |
| Recovery and signals | 126 |
| SIGSHUTDN | 126 |
| SIGRECOVERY | 127 |
| Kernel user exit (uesyscall) | 127 |
| User Database (UDB) [6] | 129 |
| Login accounts and the UDB | 129 |
| Providing login accounts | 130 |
| Removing login accounts | 130 |
| User control capabilities | 131 |
| User limits | 131 |
| Privileges | 132 |
| Quota fields | 133 |
| Other UDB information | 134 |
| The /etc/passwd and /etc/group files | 134 |
| The /etc/passwd file | 134 |
| The /etc/group file | 135 |
| The nu command | 136 |
| Crash and Dump Analysis [7] | 139 |
| Introduction | 139 |
| SG-2301 10.0 | ix |

| | <i>Page</i> |
|---|-------------|
| Using the crash program | 139 |
| Analyzing system problems | 141 |
| Panic | 141 |
| Debugging panics | 141 |
| Buffer flushing | 142 |
| Running system | 143 |
| The fdmp command | 143 |
| UNICOS Multilevel Security (MLS) Feature [8] | 145 |
| Overview of UNICOS security mechanisms | 146 |
| System management | 148 |
| The super-user mechanism (PRIV_SU) | 150 |
| UNICOS categories | 150 |
| The PAL-based privilege mechanism | 151 |
| Overview of process privilege attributes | 152 |
| UNICOS security privileges | 154 |
| Process privileges | 158 |
| Privilege assignment list (PAL) | 159 |
| Propagation of privileges | 162 |
| Super-user PALs | 162 |
| Software not part of the set of Cray ML-Safe components | 164 |
| Determining PAL privileges | 165 |
| Process privilege management | 166 |
| Privilege text management | 166 |
| Privileged shell | 167 |
| Overview of access and privilege checks | 169 |
| Discretionary access control | 171 |
| umask on a MLS system | 172 |

| | <i>Page</i> |
|--|-------------|
| Managing set-user-ID and set-group-ID files | 172 |
| Mandatory access control | 173 |
| Directory operations | 175 |
| Removing files from directories | 176 |
| Wildcard and multilevel directories (MLDs) | 176 |
| Directory permissions | 186 |
| File system and file operations | 186 |
| System high and system low labels | 186 |
| File system labeling | 189 |
| Changing file labels | 190 |
| File system access controls | 190 |
| File system back up operations | 191 |
| File system security | 193 |
| File labeling | 194 |
| Single-level and multilevel files and devices | 195 |
| Assignment and access rules for labeling information | 198 |
| The <code>spdev(8)</code> command | 199 |
| Pseudo terminals | 200 |
| Pty device inodes | 200 |
| <code>cron(8)</code> , <code>batch(1)</code> , and <code>at(1)</code> operations | 201 |
| Multilevel mail operations | 202 |
| The <code>/proc</code> file system operations | 203 |
| <code>syslogd</code> operations | 203 |
| Destructive reads on named pipes | 204 |
| IPC objects | 204 |
| MLS identification and authentication (I&A) | 204 |
| Overview of I&A security implementation | 205 |
| Login procedures | 207 |

| | <i>Page</i> |
|---|-------------|
| Interactive logins | 207 |
| Remote logins with SecurID card | 208 |
| Centralized identification and authentication (I&A) | 208 |
| Checks and operations | 209 |
| Library routines supporting I&A | 210 |
| I&A user exits | 213 |
| Password security | 215 |
| Last login notification | 217 |
| Generic login message | 217 |
| Password aging | 217 |
| Password suppression | 218 |
| Password encryption | 218 |
| Password locking | 218 |
| User trapping | 218 |
| Restricted directory | 219 |
| Login attempts | 219 |
| Machine-generated passwords | 219 |
| MLS login and password protection features | 222 |
| Password auditing | 228 |
| Reenabling accounts | 229 |
| Object reuse | 230 |
| MLS installation and configuration | 232 |
| System startup procedure | 233 |
| Subsystem startup procedure | 233 |
| System shutdown procedure | 233 |
| System clearing procedure | 234 |
| MLS configuration parameters | 234 |
| The secparm.h file | 234 |

| | <i>Page</i> |
|--|-------------|
| The <code>uts/cf.SN/config.h</code> file | 235 |
| The <code>seclabs.c</code> file | 237 |
| Permission definitions | 237 |
| Defining MLS UDB entries | 239 |
| Directory initialization procedures | 241 |
| The <code>privcmd(8)</code> command | 242 |
| MLS installation and configuration procedures | 242 |
| Cray ML-Safe configuration | 243 |
| Single level UNICOS system to a multilevel UNICOS system | 254 |
| MLS auditing on a UNICOS system | 261 |
| Security log overview | 263 |
| Security logging daemon | 266 |
| Security logging daemon in single-user mode | 266 |
| The <code>spaudit(8)</code> command | 267 |
| Security logging configuration parameters | 268 |
| Security log record types | 270 |
| Auditing on a Cray ML-Safe system configuration | 273 |
| Security log record header definition | 274 |
| System start record (SLG_GO) | 276 |
| System shutdown record (SLG_STOP) | 278 |
| System configuration change record (SLG_CCHG) | 278 |
| System time change record (SLG_TCHG) | 279 |
| Discretionary access violation record (SLG_DISC_7) | 280 |
| Discretionary access change record (SLG_DAC_CHNG) | 286 |
| Mandatory access record (SLG_MAND_7) | 289 |
| Login validation record (SLG_LOGN) | 292 |
| Tape activity record (SLG_TAPE) | 298 |
| End-of-job record (SLG_EOJ) | 302 |

| | <i>Page</i> |
|---|-------------|
| Change directory record (SLG_CHDIR) | 303 |
| Security-related system call record (SLG_SECSYS) | 305 |
| NAMI function record (SLG_NAMI) | 311 |
| setuid system call record (SLG_SETUID) | 313 |
| su attempt record (SLG_SU) | 315 |
| Networks security violations record (SLG_IPNET) | 316 |
| Cray NFS request record (SLG_NFS) | 319 |
| File transfer record (SLG_FXFR) | 321 |
| Network configuration change record (SLG_NETCF) | 323 |
| Audit criteria change record (SLG_AUDIT) | 326 |
| NQS configuration change record (SLG_NQSCF) | 328 |
| NQS activity record (SLG_NQS) | 330 |
| Cray ML-Safe process activity record (SLG_TRUST) | 332 |
| Use of privilege record (SLG_PRIV) | 335 |
| Cray/REELlibrarian (CRL) activity record (SLG_CRL) | 338 |
| The reduce command | 343 |
| Selecting record types (-t option) | 344 |
| Printing security labels in record header (-S and -L options) | 345 |
| Selecting records by object label (-O option) | 345 |
| Displaying path names (-p option) | 347 |
| Tracking a specific user name (-l and -u options) | 348 |
| Tracing a user's login session (-j option) | 349 |
| Reducing security log input (-r, -R, and -f options) | 352 |
| Monitoring security-relevant events | 352 |
| Security violation error codes | 354 |
| NQS operations | 358 |
| Tape operations | 358 |
| TCP/IP operations | 359 |

| | <i>Page</i> |
|--|-------------|
| UNICOS NFS operations | 359 |
| MLS data migration operations | 359 |
| Administration of Online Documentation [9] | 361 |
| Modifying online glossary files | 361 |
| Modifying the Cray Research definitions file | 361 |
| Creating a local definitions file | 362 |
| Glossary keywording rules | 363 |
| Cray message system | 364 |
| Overview | 365 |
| Message system files | 366 |
| File names | 367 |
| File location | 367 |
| Installing message system files | 368 |
| Changing the message text file | 368 |
| Editing the message text file | 369 |
| Rebuilding catalogs | 369 |
| Rebuilding with nmake | 370 |
| Rebuilding with message system commands | 370 |
| Printing messages | 371 |
| Cray DynaWeb server | 373 |
| Local man pages | 374 |
| Examples | 375 |
| Example 1 | 375 |
| Example 2 | 376 |
| Display order for same-name man pages | 377 |
| Appendix A User-defined Locales | 379 |
| The localedef utility | 379 |

| | <i>Page</i> |
|--|-------------|
| Character specifications | 380 |
| General syntax of the locale definition file | 384 |
| The LC_MONETARY category | 386 |
| The LC_MESSAGES category | 388 |
| The LC_NUMERIC category | 389 |
| The LC_TIME category | 390 |
| The LC_CTYPE category | 393 |
| Character class and case mappings | 394 |
| The LC_COLLATE category | 395 |
| Collation sequence | 396 |
| String ordering | 397 |
| Glossary | 401 |
| Index | 403 |
| Figures | |
| Figure 1. Configuration with no alternate path | 30 |
| Figure 2. Configuration 1: One FCN device, two Fibre Channel Loops | 30 |
| Figure 3. Configuration 2: Two FCN devices, one GigaRing channel | 31 |
| Figure 4. Configuration 3: Two FCN devices, two GigaRing channels | 31 |
| Figure 5. UNICOS security mechanisms | 147 |
| Figure 6. Interaction of UNICOS security mechanisms | 148 |
| Figure 7. Propagation of privileges | 162 |
| Figure 8. Overview of initial MAC/DAC checks and assigning of privileges | 170 |
| Figure 9. I&A security implementation | 205 |

| | <i>Page</i> |
|---|-------------|
| Figure 10. Overview of security auditing | 262 |
| Tables | |
| Table 1. Spindle to unit number mapping | 39 |
| Table 2. United States time zones | 63 |
| Table 3. rcoptions Decide String Parameters | 78 |
| Table 4. rcoptions Non-decide String Parameters | 81 |
| Table 5. rcoptions File System String Parameters | 82 |
| Table 6. Login protection parameter configuration, example 1 | 225 |
| Table 7. Login protection parameters configuration, example 2 | 226 |
| Table 8. Login protection parameters configuration, example 3 | 227 |
| Table 9. Suggested values for UDB security fields | 240 |
| Table 10. Security log records | 272 |
| Table 11. Security violation error codes | 355 |

