

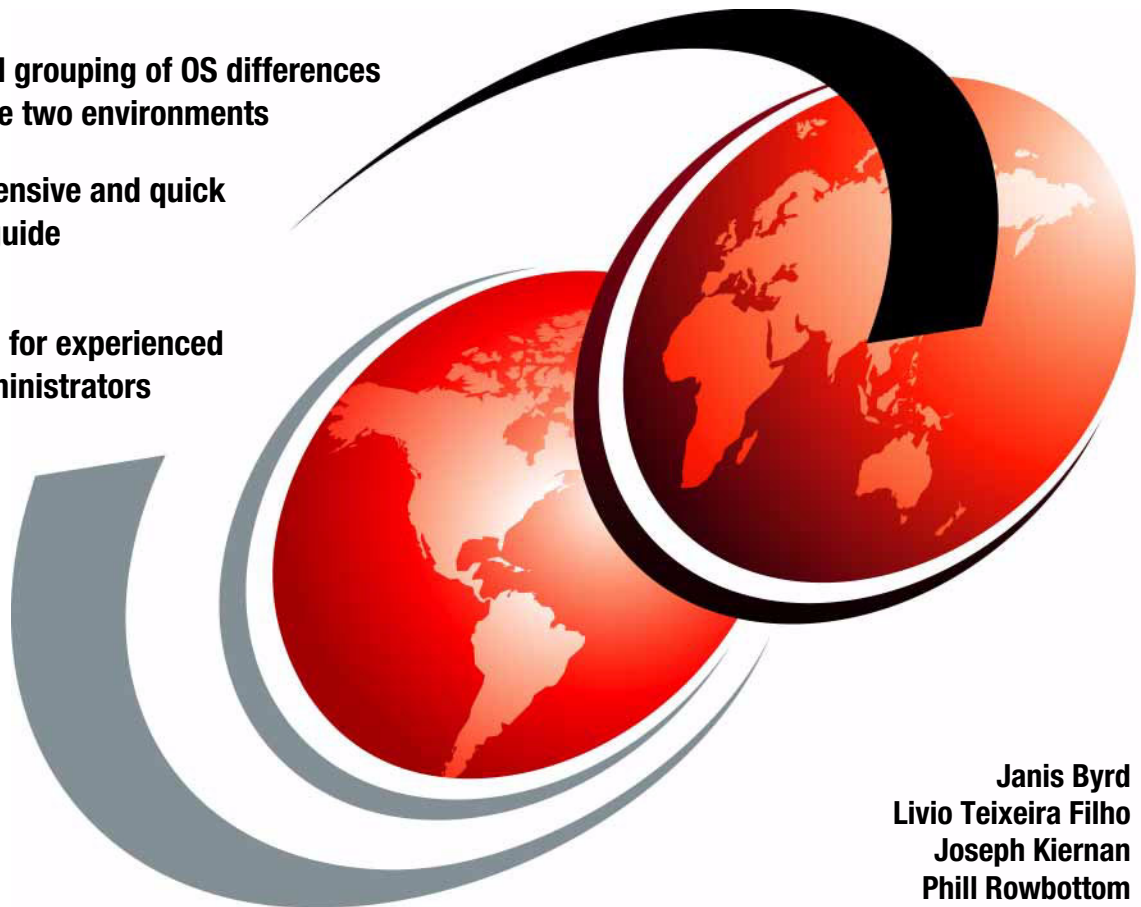


Sun Solaris to IBM AIX 5L Migration: A Guide for System Administrators

Task-based grouping of OS differences
between the two environments

A comprehensive and quick
transition guide

A reference for experienced
system administrators



Janis Byrd
Livio Teixeira Filho
Joseph Kiernan
Phill Rowbottom

ibm.com/redbooks

Redbooks



International Technical Support Organization

**Sun Solaris to IBM AIX 5L Migration: A Guide for
System Administrators**

April 2007

Note: Before using this information and the product it supports, read the information in “Notices” on page xiii.

First Edition (April 2007)

This edition applies to AIX 5L Version 5.3.

© Copyright International Business Machines Corporation 2007. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	xiii
Trademarks	xiv
Preface	xv
The team that wrote this IBM Redbook	xvi
Acknowledgements	xvii
Become a published author	xvii
Comments welcome	xviii
Part 1. Introduction	1
Chapter 1. AIX 5L and Solaris: Approaches to administration	3
1.1 System configuration methods	4
1.2 The System Management Interface Tool	7
1.2.1 The SMIT selector screen	9
1.2.2 The SMIT dialog screen	10
1.2.3 The SMIT output screen	12
1.3 Web-based System Manager	14
1.4 Object Data Manager: The system configuration storage facility in AIX 5L15	15
1.5 Errpt and syslog in AIX 5L	15
1.6 Operator panel or light-emitting diode	21
1.7 Important reminders: The inittab file and the Object Data Manager	21
1.8 AIX 5L kernel parameters versus Solaris kernel parameters	22
1.9 Some useful AIX 5L hints for the Solaris administrator	23
Part 2. System administration differences	27
Chapter 2. Introduction to IBM System p	29
2.1 Introduction to IBM System p and IBM RS/6000 architectures	30
2.1.1 RS/6000 system bus types	30
2.1.2 POWER2 Super Chip	31
2.1.3 POWER3	31
2.1.4 POWER3 II chip	32
2.1.5 PowerPC	32
2.1.6 The RS64 processor family	32
2.1.7 POWER4 and POWER4+	33
2.1.8 POWER5 and POWER5+	33
2.1.9 POWER4-based server features	34
2.1.10 POWER5-based server features	35

2.2	Planning considerations	36
2.2.1	IBM System p	36
2.3	Concepts for AIX 5L logical partitions	37
2.3.1	Hardware requirements for AIX 5L logical partitions	39
2.3.2	Logical partition planning tasks	40
2.4	IBM eServer BladeCenter JS20	40
2.4.1	Network planning	41
2.4.2	Minimal network requirements	41
2.5	IBM System p High Performance Switch	45
2.6	IBM System Cluster 1600	46
Chapter 3. Operating system installation		47
3.1	Basic system installation	48
3.2	Graphical installation or text installation	50
3.3	New and complete overwrite installation	53
3.4	Migration installation	54
3.5	Preservation installation	54
3.6	Advanced installation options	55
3.7	Other installation methods	55
3.7.1	Alternate disk installation	56
3.7.2	Alternate disk migration installation	64
3.8	Using the multibos utility	67
3.9	Network Installation Manager	67
3.9.1	Network Installation Management environments	69
3.9.2	Network Installation Management setup	69
3.9.3	Installing Network Installation Management from a command line	73
3.9.4	Installing the Base Operating System on a Network Installation Management client	75
3.9.5	Booting a machine over the network	76
3.10	AIX 5L installation in a partitioned environment	77
3.10.1	Installing AIX 5L in a partitioned environment	77
3.10.2	Configuring an initial partition as a NIM master	77
3.10.3	Installing AIX 5L using a CD-ROM device	85
3.11	Installing AIX 5L on IBM BladeCenter	89
Chapter 4. Disks and file systems		91
4.1	Disk administration	92
4.2	Disk recognition	92
4.3	Multipath I/O	93
4.4	Storage area network administration	94
4.4.1	SAN command-line examples on AIX 5L	95
4.5	Logical Volume Manager administration on AIX 5L	96
4.5.1	Logical Volume Manager configuration data	97

4.6	Physical volumes	101
4.7	Volume groups	102
4.8	Logical volumes	105
4.8.1	File system	107
4.8.2	Disk mirroring	107
4.9	File system types and management	109
4.9.1	Basic administration and concepts	109
4.9.2	File system types on Solaris and AIX 5L	110
4.9.3	Network File System	111
4.9.4	Autofs automounter	114
4.9.5	Virtual file systems	115
4.9.6	Swap space	118
4.9.7	File system journaling	122
4.10	Migration from physical disks partition to AIX 5L	127
4.11	Migration from Solaris Volume Manager to AIX 5L	128
4.11.1	Concepts	128
4.11.2	Commands	128
4.12	Migration from Veritas Volume Manager	130
4.12.1	Concepts	130
4.12.2	Commands	131
Chapter 5. Software management		133
5.1	Packages	134
5.1.1	Package management in Solaris	135
5.1.2	Package management in AIX 5L	135
5.2	AIX 5L Base Operating System	140
5.2.1	Bonus pack and expansion pack	140
5.2.2	Software updates	140
5.2.3	Software states under AIX 5L	141
5.2.4	Installing software under AIX 5L using smitty	142
5.2.5	Installing optional software using the Web-based System Manager	144
5.3	Patching	146
5.3.1	Patching in Solaris	146
5.3.2	Patching in AIX 5L	147
5.4	Maintenance levels	147
5.5	Dependencies	150
5.5.1	Dependency management in Solaris	150
5.5.2	Package dependencies in AIX 5L	151
5.5.3	Package distribution methods	151
5.6	Automated software management	151
5.6.1	Automated software management in Solaris	151
5.6.2	Automated software management in AIX 5L	152
5.7	Activating the fixes after updating	154

5.7.1 Patch activation in Solaris	154
5.7.2 Patch activation in AIX 5L	154
5.7.3 Verifying the integrity of the operating system	154
5.8 Software management in clustered environments	154
5.8.1 Solaris	155
5.8.2 AIX 5L	155
Chapter 6. Device management	157
6.1 Device access and configuration	158
6.1.1 Device naming and access	158
6.1.2 Solaris logical disk devices	158
6.1.3 AIX 5L disk devices	159
6.2 Accessing devices	159
6.3 Listing device information	160
6.3.1 Solaris	160
6.3.2 AIX 5L	160
6.4 Adding a device	165
6.4.1 Solaris	165
6.4.2 AIX 5L	166
6.5 Modifying a device	170
6.5.1 Solaris	170
6.5.2 AIX 5L	170
6.6 Removing a device	173
6.6.1 Solaris	173
6.6.2 AIX 5L	173
6.7 Alternate disk paths (multipathing)	174
6.7.1 Solaris	175
6.7.2 AIX 5L	176
6.8 Device management summary	180
Chapter 7. Network services	183
7.1 Network configuration changes	184
7.1.1 Instructions for Solaris	184
7.1.2 Instructions for AIX 5L	185
7.1.3 Common network configuration files in Solaris and AIX 5L	188
7.1.4 Other networking differences	189
7.2 Differences between Internet Protocol V4 and Internet Protocol V6	191
7.3 Mixed IPv4 and IPv6 networks	192
7.3.1 Tunneling	192
7.4 Network load balancing and failover solutions	195
7.4.1 Solaris	195
7.4.2 AIX 5L	195
7.5 Static and dynamic routing	198

7.6	IP network services	201
7.6.1	inetd-based	201
7.6.2	Dynamic Host Configuration Protocol	202
7.6.3	Domain Name System	204
7.6.4	Network Time Protocol	205
7.6.5	Lightweight Directory Access Protocol	206
7.6.6	Network Information Service and Network Information Service+	206
7.6.7	Network File System	206
7.6.8	Mail services	209
7.7	Simple Network Management Protocol	210
Chapter 8. Boot and system initialization		213
8.1	Booting a system	214
8.1.1	Booting types	214
8.1.2	Overview of Solaris for SPARC booting process	216
8.1.3	Overview of the AIX 5L boot process	216
8.1.4	Boot modes	219
8.1.5	Using the Hardware Management Console to perform a slow boot	222
8.2	Useful commands	223
8.3	The /etc/inittab file	225
8.3.1	Startup process in Solaris	226
8.3.2	Startup process in AIX 5L	226
8.3.3	AIX 5L run levels	230
8.4	System shutdown	233
8.5	Network booting	237
Chapter 9. Managing system resources		239
9.1	Displaying system information	240
9.2	Resource management	243
9.2.1	Solaris domains and dynamic reconfiguration	243
9.2.2	Solaris Resource Manager	244
9.2.3	AIX 5L logical partitioning, dynamic LPAR, and virtualization	244
9.2.4	AIX 5L Partition Load Manager	245
9.2.5	AIX 5L Work Load Manager	246
9.2.6	Reliable Scalable Cluster Technology	248
9.3	Starting and stopping the system services	250
9.4	Scheduling services	254
9.5	Quotas	256
9.6	Process accounting	259
9.7	Management tools	260
9.7.1	Common system management tools	260
9.7.2	Solaris remote system management	262
9.7.3	AIX 5L management tools	263

9.7.4 Web-based System Manager	269
Chapter 10. Printing services	279
10.1 Overview	280
10.2 AIX 5L print subsystem versus Solaris lpsched print subsystem	280
10.3 Print queue administration.	283
10.3.1 Adding a local print queue.	284
10.3.2 Displaying a queue configuration information	290
10.3.3 Deleting a queue.	291
10.3.4 Enabling and disabling a queue	293
10.3.5 Cancelling print jobs	294
10.4 Print job management.	294
10.4.1 Submitting printing jobs	294
10.4.2 Checking the status.	299
10.4.3 Print queue status	304
10.4.4 Cancelling a printing job	305
10.4.5 Prioritizing a printing job	305
10.4.6 Holding and releasing a printing job	307
10.4.7 Moving a job between queues	308
10.5 Printer pooling	310
10.6 Using System V print subsystem on AIX 5L	310
10.7 System files associated with printing.	312
10.8 Remote printing	313
10.9 Common UNIX Printing System	317
10.10 Quick reference.	318
Chapter 11. Users and groups	321
11.1 Overview	322
11.2 Adding users	325
11.3 Removing users	328
11.4 Displaying users who are currently logged in	329
11.5 Changing users, passwords, and other attributes.	331
11.5.1 Changing a user's password.	331
11.5.2 Disabling a user account.	334
11.5.3 Modifying a user account	335
11.6 Customizing a user's work environment	341
11.7 Password files	344
11.8 Administering groups.	347
11.8.1 Adding a group	349
11.8.2 Modifying an existing group	351
11.8.3 Deleting a group	353
11.9 Checking for inconsistencies in passwords and group definitions	353
11.10 Defining the system resource limits for users	355

11.11 Quick reference	357
Chapter 12. Monitoring and performance	359
12.1 Monitoring memory	360
12.1.1 Solaris memory management	360
12.1.2 AIX 5L memory management	360
12.2 Virtual memory	361
12.2.1 The vmstat command	362
12.3 The top and topas commands	363
12.4 AIX 5L paging and memory statistics	366
12.5 Monitoring the processors and the CPU	368
12.5.1 Using sar to monitor CPU	369
12.5.2 Using filemon to monitor CPU	370
12.5.3 The procmon tool	372
12.6 Physical media, software RAID, Logical Volume Manager, and file systems	373
12.6.1 Physical media monitoring	373
12.6.2 Monitoring logical volumes and logical volume groups	373
12.6.3 Software Redundant Array of Independent Disks	374
12.6.4 Logical volume monitoring	374
12.6.5 File systems	375
12.7 Network	375
12.8 System and user processes	376
Chapter 13. Security and hardening	377
13.1 Hardware security	378
13.1.1 System Controllers on Sun servers	378
13.1.2 OpenBoot PROM on Sun servers	378
13.1.3 Hardware Management Console on IBM servers	379
13.1.4 IBM System p hardware security features	379
13.2 Additional security features	381
13.3 User and password policy	382
13.4 Securing the File Transfer Protocol	383
13.5 Removing unused services	384
13.6 Access control list	386
13.7 Auditing	389
13.8 Light Directory Access Protocol	390
13.9 Secure Shell	391
13.10 Transmission Control Protocol Wrapper	391
13.11 Network File System	393
13.12 Sudo	393
13.13 Kerberos	394
13.14 IP Security Architecture and Internet Key Exchange	395

13.15 Pluggable Authentication Module and Loadable Authentication Module	396
Chapter 14. Backup and restore	399
14.1 Local tape, CD, or DVD operating system backup	400
14.1.1 Solaris ufsdump backup	400
14.1.2 Solaris flash archive	400
14.1.3 AIX 5L tape image backup	401
14.1.4 AIX 5L CD or DVD image backup	404
14.2 Remote operating system backup	406
14.2.1 Creating an mksysb image of the machine using the Network Installation Manager	407
14.3 Volume group backup	410
14.4 File system or directory backup	412
14.5 Raw devices backup	415
14.6 AIX 5L SysBack (IBM Tivoli Storage Manager for System Backup and Recovery)	415
14.7 Compression tools	417
14.8 Managing tape backup media	417
Chapter 15. High availability and clustering overview	421
15.1 Introduction to clustering	422
15.2 Solaris clustering software	422
15.2.1 Sun cluster	422
15.2.2 Veritas Cluster Server for Solaris	423
15.2.3 Linux high availability on Solaris	424
15.3 AIX 5L clustering software	424
15.3.1 AIX 5L HACMP	424
15.3.2 AIX 5L HACMP/XD	425
15.3.3 AIX 5L Cluster Systems Management	426
Chapter 16. Troubleshooting	429
16.1 The booting process	430
16.1.1 Boot troubleshooting: Solaris	430
16.1.2 Boot troubleshooting: AIX 5L	430
16.2 Core files	433
16.2.1 Management of core files: Solaris	433
16.2.2 Management of core files: AIX 5L	434
16.2.3 Determining which process failed and caused a core file	434
16.3 Crash or system dumps	436
16.4 Logs	438
16.4.1 Syslogging	438
16.4.2 Differences in logging between Solaris and AIX 5L	439
16.4.3 Application logging	440

16.5 File systems	440
16.5.1 Journaled file systems	441
16.5.2 Remote file systems	441
16.6 Software Redundant Array of Independent Disks	442
16.7 Logical volumes	442
16.8 Packages	443
16.9 Root password recovery	443
16.10 Network	445
16.11 Tracing the system and user processes	447
16.12 Using the truss command in troubleshooting	449
Part 3. Appendices	455
Appendix A. Tasks reference	457
Packaging	459
Installation and upgrading tasks	459
Booting and shutting down	461
User management tasks	464
Device management and configuration	465
Multipath Input/Output management	466
Network management and configuration	466
Network File System management and configuration	470
Monitoring and performance	471
Memory management	471
Processors and CPU	472
Physical media	473
Software Redundant Array of Independent Disks	473
Logical volumes	474
File systems	474
Network	475
System and user processes	475
Displaying system information	476
Starting and stopping system services	477
Scheduling services	477
Quotas	479
Accounting	480
AIX 5L management tools	480
Backup and restore	481
Printer management and configuration	482
Disk and file system management	484
File systems	486
Physical disk and Logical Volume Manager	491
Troubleshooting	494

Managing core files	494
Crash dumps	495
Networking problems	496
Using logs to troubleshoot.	496
File systems	497
System and user problems	497
Appendix B. Quick reference: Comparable commands and configuration files	499
Configuration and other files	500
Appendix C. AIX 5L Object Data Manager	503
Overview	504
Object Data Manager components.	504
Object Data Manager commands.	504
Changing the attribute values.	505
Location and contents of the Objects Data Manager repository	506
Object Data Manager device configuration	507
Related publications	515
IBM Redbooks	515
Other publications	515
Online resources	516
How to get IBM Redbooks	516
Help from IBM	516
Index	517

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law. INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.


This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

1350™	LoadLeveler®	Redbooks (logo)  ™
AIX®	Lotus®	Redbooks™
AIX 5L™	Micro Channel®	Requisite®
AS/400®	Micro-Partitioning™	RISC System/6000®
BladeCenter®	OpenPower™	RS/6000®
Chipkill™	POWER™	SysBack™
CICS®	POWER2™	System i™
DB2®	POWER3™	System p™
Enterprise Storage Server®	POWER4™	System p5™
eServer™	POWER4+™	System x™
General Parallel File System™	POWER5™	Tivoli®
GPFS™	POWER5+™	TotalStorage®
HACMP™	POWER6™	VisualAge®
IBM®	POWER Hypervisor™	WebSphere®
Infoprint®	PowerPC®	Workplace™
iSeries™	PowerPC 750™	xSeries®
Language Environment®	pSeries®	

The following terms are trademarks of other companies:

Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

CacheFS, Java, JumpStart, OpenBoot, Solaris, Solstice, Solstice DiskSuite, Sun, Sun Enterprise, Sun Enterprise Authentication Mechanism, Sun Fire, Sun Microsystems, Sun Trunking, SunSHIELD, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Internet Explorer, Microsoft, Windows NT, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

The aim of this IBM® Redbook is to provide a technical reference for IT system administrators in organizations that are considering a migration from Sun™ Solaris™ to IBM AIX® 5L™-based systems. This book presents a system administrator view of the technical differences that exist and the methods that are necessary to complete a successful migration to AIX 5L-based systems.

Important: This book is designed primarily as a reference for experienced Sun Solaris 8 or 9 system administrators who will be working with AIX 5L. This book is *not* an AIX 5L administration how-to book for system administrators who are beginners, but rather a guide for experienced administrators who have to translate a given Solaris system administration task to AIX 5L.

This book is organized into three main parts:

- ▶ Part 1, “Introduction” on page 1 starts with a system administrator’s perspective, focusing on important differences in operating system management.
- ▶ Part 2, “System administration differences” on page 27 covers a broad set of system administration topics. The chapters in this Part focus on specific configuration management tasks and system functions for which a system administrator is typically responsible. In each chapter, topics are discussed with the goal of identifying the major differences between how the tasks and functions are managed on Solaris and on AIX 5L. Because it is impossible to provide a comprehensive reference about each topic in a single volume, references are provided for finding more detailed information about the topics presented in each chapter.
- ▶ Part 3, “Appendixes” on page 455 provides a task-based quick reference and a comparable commands and configuration files quick reference. A detailed review of the AIX 5L Object Data Manager (ODM) facility is also included.

The team that wrote this IBM Redbook

This IBM Redbook was produced by a team of specialists who came from around the world to work together at the IBM International Technical Support Organization (ITSO) centre in Austin, Texas.

Janis Byrd is a Software Engineer with the IBM Tivoli® Global Response Team, based in Austin, Texas. In her current position, she provides hands on technical support and consulting services to IBM customers worldwide. Prior to her current role, she worked in the IBM Tivoli Level 2 Customer Support Center in Austin. Jan has over 20 years experience in the IT industry, including five years at the University of Texas Center for High Performance Computing, where she provided technical support to the community of researchers and students using the Cray, Convex, AIX 5L, Sun, and Silicon Graphics-based computing systems.

Joseph Kiernan is a UNIX® Systems Administrator working for the IBM Dublin Software Lab in Ireland. Joe provides UNIX system administration support for IBM Lotus® Workplace™ products undergoing systems and functional verification testing. Joe also supports IBM LanguageWare, IBM WebSphere® Portal and IBM Lotus Learning Management System (LMS). A postgraduate in Applied Physics from Maynooth University, Ireland, Joe has a total of five years IT industry experience. His areas of expertise include AIX, Solaris, and FreeBSD systems administration, AIX network-based installation methods, and patching and software management. In 2005 he coauthored and published an article on Network Install Manager for AIX in *Sys Admin Magazine* (<http://www.samag.com>).

Livio Teixeira Filho is a Senior IT Specialist, Electronic Data Systems (EDS) Brazil, where he is a member of the Midrange Hosting team. He provides technical and problem-solving support for EDS customers, handling complex and critical scenarios. He has experience in working on cross UNIX platforms on many migration and consolidation projects. Livio has engineering knowledge on Sun High-End Servers, and he is certified by the Information Technology Infrastructure Library (ITIL®), HP-UX CSA, Linux® Professional Institute, Conectiva Linux, and IBM eServer™ pSeries® Specialist Administration and Support for AIX 5L V5.3.

Phill Rowbottom is a Senior UNIX Systems Administrator currently working for the IBM Integrated Technology Delivery in Australia. Phill graduated from Monash University in 2000 with a double degree, Bachelor of Business (Accounting) and Bachelor of Computing (Applications Development). Phill started with IBM as a graduate hire in 2001, supporting Solaris in customer environments, and then moved to a major Solaris-focused project for a financial

services customer before joining the Midrange Systems Server Management Services team and branching into support of AIX and HP-UX. Phill has also provided support for IBM Tivoli Storage Manager, Linux, and HP OpenVMS. Phill holds certifications in AIX, Solaris, HP-UX, and Linux.

The production of this IBM Redbook was managed by:

Chris Almond, an ITSO Project Leader and IT Architect based at the ITSO Center in Austin, Texas. In his current role, Chris specializes in managing content development projects focused on Linux and AIX 5L systems engineering. He has a total of 15 years IT industry experience, including the last six with IBM.

Acknowledgements

This IBM Redbook team acknowledges the authors of the IBM Redbook *Solaris to Linux Migration: A Guide for System Administrators*, SG24-7186. The authors of SG24-7186, **Mark Brown, Chuck Davis, William Dy, Paul Ionescu, Jeff Richardson, Kurt Taylor**, and **Robbie Williamson**, created a framework that helped us accelerate the content development of our closely related topic.

This IBM Redbook team acknowledges **James Burke** and **Tim Barber** from the IBM Australia Integrated Technology Delivery team for their contributions and draft review feedback in support of this project.

This team also acknowledges the support efforts of **Jay Kruemcke**, the IBM Systems and Technology Group, IBM System p™ AIX Offering Manager, and our Editors for this book, **Lubna Esmail** and **Sharmela Pattabiraman** from our ITSO Authoring Services team in Bangalore, India.

Become a published author

Join us for a two-week to six-week residency program! Help write an IBM Redbook dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will team with IBM technical professionals, Business Partners and/or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our IBM Redbooks™ to be as helpful as possible. Send us your comments about this or other IBM Redbooks in one of the following ways:

- ▶ Use the online **Contact us** review IBM Redbook form found at:

ibm.com/redbooks

- ▶ Send your comments in an e-mail to:

redbook@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400



Part 1

Introduction

This part begins with a systems administrator's perspective on the fundamental differences between Solaris and AIX 5L in Chapter 1, "AIX 5L and Solaris: Approaches to administration" on page 3, followed by Chapter 2, "Introduction to IBM System p" on page 29.



AIX 5L and Solaris: Approaches to administration

This chapter provides a high-level overview of the conceptual differences between Solaris and AIX 5L. Although Solaris and AIX 5L are both UNIX-based operating systems (OS), there are important differences in the design of the two OS that system administrators must be aware of. This chapter provides the fundamental technical background that is necessary for system administrators to understand the differences between Solaris and AIX 5L.

This chapter contains information about the following topics:

- ▶ 1.1, “System configuration methods” on page 4
- ▶ 1.2, “The System Management Interface Tool” on page 7
- ▶ 1.4, “Object Data Manager: The system configuration storage facility in AIX 5L” on page 15
- ▶ 1.5, “Errpt and syslog in AIX 5L” on page 15
- ▶ 1.6, “Operator panel or light-emitting diode” on page 21
- ▶ 1.7, “Important reminders: The inittab file and the Object Data Manager” on page 21
- ▶ 1.8, “AIX 5L kernel parameters versus Solaris kernel parameters” on page 22
- ▶ 1.9, “Some useful AIX 5L hints for the Solaris administrator” on page 23

1.1 System configuration methods

One of the fundamental differences between Solaris and AIX 5L is the manner in which changes to the OS and its configuration are accomplished.

Solaris relies heavily on text-based configuration files to hold its system configuration. When making changes to a Solaris system, the administrator usually looks for the relevant configuration file to edit. The administrator then determines the action that must be taken for the changes to take effect.

Alternatively, the Solaris system administrator might go looking for a command that will effect the change, and then decide on whether the change is immediate, whether a reboot is required for the change to take effect, for example, changes made to the `/etc/system` file, or whether the change that is made is tied to the currently running system and will be lost after a reboot.

The AIX 5L way of making changes to the system configuration is quite different because AIX 5L stores the majority of its configuration in the Object Data Manager (ODM, which is discussed in detail in Appendix C, “AIX 5L Object Data Manager” on page 503. The ODM is a binary database that cannot be edited with a text editor. Some settings are contained in text files, many of which can be managed through commands or AIX 5L’s management tools. However, there are a few AIX 5L settings that require manual text editing.

In AIX 5L, making configuration changes to the OS involves using a tool or commands. In AIX 5L, these tools are the System Management Interface Tool (SMIT) and the Web-based System Manager (WSM).

Although it is possible to use the underlying commands that are called by SMIT and WSM, it is much easier to use the tools, especially when you are new to AIX 5L. The tools provide a listing of all the parameters, and perform some validation on the inputs to these parameters.

An example

An example of a networking-related task that a Solaris or AIX 5L system administrator must perform routinely is defining a new network interface for an existing system. This can be a new *physical interface*, for example, a new Network Information Card (NIC), or a *virtual interface*.

In Solaris, this requires manual editing of configuration files to make the interface definition consistent across reboots, and manual configuration of the interface to make the interface active without a reboot. Even if the update to the system can be performed online, it is a good practice to reboot the system to ensure that the changes to the configuration files are correct and will remain after reboot.

In AIX 5L, bringing the interface online and making the interface consistent across reboots can be achieved by using a single panel within the SMIT. The SMIT updates the configuration for the interface in the system configuration and brings the interface online. Because the SMIT combines both the steps into one validated command, it is not necessary to perform a reboot to verify that the system configuration is correct and that the interface persists across reboots. For more details about this, refer to Chapter 7., “Network services” on page 183.

When you work with AIX 5L, you will notice that just about all the errors from commands have a number associated with them (Example 1-1). You can refer to these message numbers in the AIX 5L documentation if you require more information about the cause of the error message and the solution to the error message.

Example 1-1 Typical seven-digit error message

```
# ls *fred*  
ls: 0653-341 The file *fred* does not exist.
```

The AIX 5L message center is a part of the IBM System p and AIX 5L Information Center on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

Figure 1-1 shows how to use the message center to query for information about the seven-digit error message shown in Example 1-1.

The screenshot shows a web browser window titled "AIX message center". The main heading is "Seven-digit error numbers". Below the heading, there is a paragraph of text explaining that this section provides detailed recovery articles for seven-digit error messages that receive the most calls for support. It notes that not all messages will have detailed information for recovery. There are two bullet points: the first says "To search by message number, enter the number in the field below and select the 'Submit query' button." and the second says "You can also search by text or a combination of number and text by selecting the 'Advanced search' option." Below this, there is a link to a PDF: "To view a printable copy of the error messages that include detailed recovery information, click on the following link: PDF".

Below the text is a "Search form" section. It contains a label "Message number:" followed by two input fields. The first field contains "0653" and the second field contains "341", with a hyphen between them. To the right of the input fields are two links: "* Search tips" and "* Advanced search". Below the input fields are two buttons: "Submit query" and "Clear form".

Figure 1-1 AIX 5L message center: Seven-digit error query

Figure 1-2 shows the results of the query.

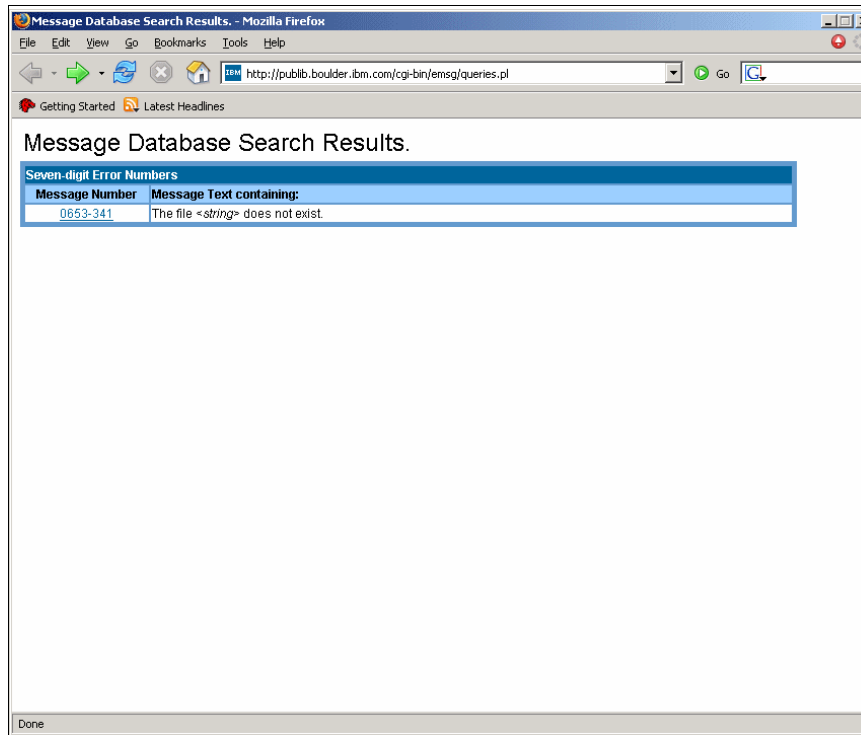


Figure 1-2 AIX 5L message center: Query results

1.2 The System Management Interface Tool

The System Management Interface Tool (SMIT) is the main tool for managing an AIX 5L system. It allows an administrator who is new to AIX 5L to quickly perform tasks without spending time looking through manuals for the required command and syntax. SMIT provides a menu or X Window-based approach to perform nearly all the system management tasks that are required to be undertaken on an AIX 5L system.

Solaris has a number of system management tools, including Admin Tool, Admin Wizard, Solaris Management Center, and Solaris Management Console. For its part, AIX 5L has an integrated task-based tool. One of the best things about SMIT is that it is task-based. If you know what you want to do, but do not know

the command to perform this, you can easily find your way through the menus to the required task. After finding the required task, press the F6 key or the Esc+6 keys depending on your terminal, in order to display the underlying command that is run by SMIT to perform the task.

For more details about using SMIT, refer to the following Web site:

<http://www-03.ibm.com/servers/aix/products/aixos/whitepapers/smit.pdf>

You can invoke SMIT by using the following commands:

- ▶ **smit**
This command invokes SMIT in graphical mode if the TERM variable is set. If it is not set, SMIT is invoked in the American Standard Code for Information Interchange (ASCII) mode.
- ▶ **smitty**
This command invokes SMIT in ASCII mode.
- ▶ **smit -a**
This command invokes SMIT in ASCII mode.
- ▶ **smit -m**
This command invokes SMIT in graphical mode.

1.2.1 The SMIT selector screen

Figure 1-3 shows the SMIT selector screen. A *selector screen* is a special version of a dialog screen in which there is only one value to change. This value of the object is used to determine which subsequent dialog screen is displayed.

```
+-----+
+-----+
          Available Network Interfaces

Move cursor to desired item and press Enter.

en0  10-80  Standard Ethernet Network Interface
et0  10-80  IEEE 802.3 Ethernet Network Interface
tr0  10-88  Token Ring Network Interface

F1=Help          F2=Refresh          F3=Cancel
F8=Image         F10=Exit           Enter=Do
/=Find           n=Find Next

+-----+
+-----+
```

Figure 1-3 The SMIT selector screen

1.2.2 The SMIT dialog screen

Figure 1-4 shows the SMIT dialog screen. A dialog screen allows you to enter input values for the selected operation. Some fields already have the default values in the system. Usually, you can change these values.

To enter data, move the highlighted bar to the value you want to change and then, either enter a value or select one from a pop-up list. Fields that you can type into are indicated by square brackets ([]). Fields that have data that is larger than the space available to display it are indicated by angle brackets (<>), indicating that there is data further to the left or right (or both) of the display area.

Add a Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]	[Entry
* Group NAME	[]
ADMINISTRATIVE group?	false +
Group ID	[] #
USER list	[] +
ADMINISTRATOR list	[] +

F1=Help	F2=Refresh	F3=Cancel
F4=List		
F5=Reset	F6=Command	F7=Edit
F8=Image		
F9=Shell	F10=Exit	Enter=Do

Figure 1-4 The SMIT dialog screen

Table 1-1 shows the different SMIT symbols. Special symbols on the screen are used to indicate how data must be entered.

Table 1-1 SMIT symbols

Symbols in SMIT dialog screen	Explanation
*	A required field
#	A numeric value is required for this field

Symbols in SMIT dialog screen	Explanation
/	A path name is required for this field
X	A hexadecimal value is required for this field
?	The value entered will not be displayed
+	A pop-up list or ring is available

An asterisk (*) symbol in the left-most column of a line indicates that the field is required. A value must be entered here before you commit the dialog and execute the command.

In the ASCII version, a plus sign (+) is used to indicate that a pop-up list or ring is available. To access a pop-up list, press F4. A ring is a special type of list. If a fixed number of options are available, you can press Tab to cycle through the options.

In the Motif version, a list button is displayed. Either click the button or press Ctrl+L to get a menu to select from.

You can use the following keys when viewing the menus and the dialog screens. Some keys are only valid in particular screens. Those that are valid only for the ASCII interface are marked (A), and those that are valid only for the Motif interface are marked (M). Table 1-2 provides an overview of all the function keys.

Table 1-2 SMIT function keys

Function keys	Explanation
F1 (or Esc+1)	Help: Show contextual help information
F2 (or Esc+2)	Refresh: Redraw the display (A)
F3 (or Esc+3)	Cancel: Return to the previous screen (A)
F4 (or Esc+4)	List: Display a pop-up list of possible values (A)
F5 (or Esc+5)	Reset: Restore the original value of an entry field
F6 (or Esc+6)	Command: Show the AIX 5L command that will be executed
F7 (or Esc+7)	Edit: A field in a pop-up box or select from a multiselection pop-up list
F8 (or Esc+8)	Image: Save the current screen to a file (A) and show the current fast path
F9 (or Esc+9)	Shell: Start a subshell (A)

Function keys	Explanation
F9	Reset all the fields (M)
F10 (or Esc+0)	Exit: Exit SMIT immediately (A)
F10	Go to the command bar (M)
F12	Exit: Exit SMIT immediately (M)
Ctrl+L	List: Give a pop-up list of possible values (M)
PgDn (or Ctrl+V)	Scroll down one page
PgUp (or Esc+V)	Scroll up one page
Home (or Esc+<)	Go to the top of the scrolling region
End (or Esc+>)	Go to the bottom of the scrolling region
Enter	Run the current command or select from a single-selection pop-up list
/text	Finds the text in the output
n	Finds the next occurrence of the text

1.2.3 The SMIT output screen

Figure 1-5 shows the SMIT output screen. The Command field can have the following values:

- ▶ OK
- ▶ RUNNING
- ▶ FAILED

Note: In the Motif version, there is a running man icon in the top right-hand corner of the screen that is used to indicate this value.

stdout is the standard output, that is, an output is produced as a result of running the command. The output is displayed in the body section of this screen. stderr indicates error messages, if any. In Figure 1-5, there are no error messages.

The body of the screen holds the output or error messages of the command output in Figure 1-5.

```
COMMAND STATUS

Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

system 0      true   root   files
staff  1      false  invscout,snapp,daemon  files
bin    2      true   root,bin   files
sys    3      true   root,bin,sys  files
adm    4      true   bin,adm  files
uucp   5      true   nuucp,uucp   files
mail   6      true   files
security 7      true   root   files
cron   8      true   root   files
printq 9      true   lp     files
audit  10     true   root   files
ecs    28     true   files
nobody -2      false  nobody,lpd   files
usr    100    false  guest  files
perf   20     false  files
shutdown 21     true   files
lp     11     true   root,lp,printq  files
imnadm 188    false  imnadm  files

F1=Help          F2=Refresh          F3=Cancel
F6=Command       F9=Shell            F10=Exit
F8=Image         /=Find
n=Find Next
```

Figure 1-5 The SMIT output screen

1.3 Web-based System Manager

Web-based System Manager is the AIX 5L client/server-based administration tool. The client system can be AIX 5L, Linux, or Windows®. Figure 1-6 shows the Web-based System Manager.

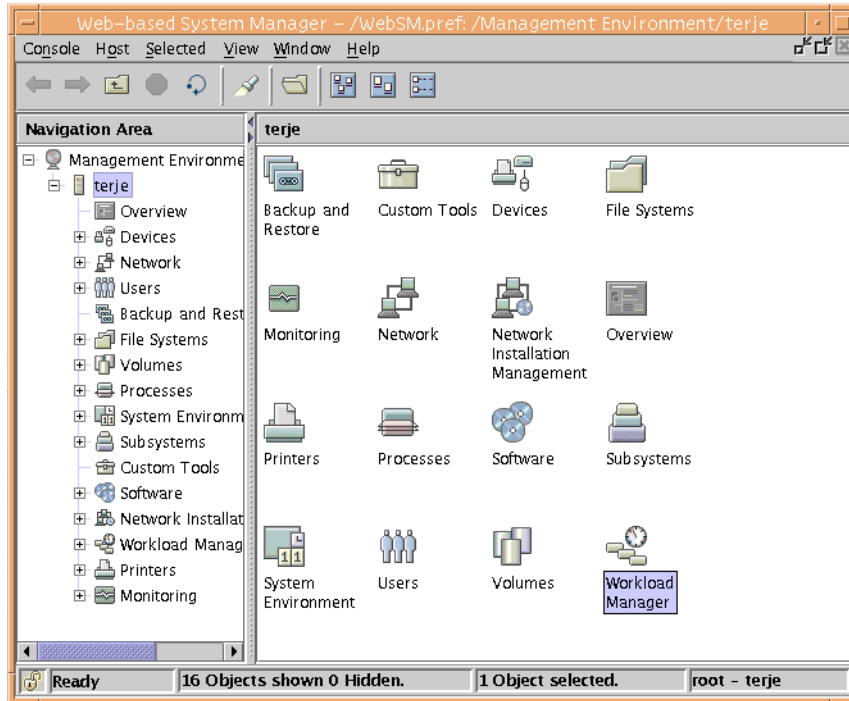


Figure 1-6 The Web-based System Manager

The client can operate in either an application mode on AIX 5L with Java™ 1.42, or in an applet mode on platforms that support Java 1.42. The objectives of the Web-based System Manager are:

- ▶ Simplifying AIX 5L administration with a single interface
- ▶ Enabling AIX 5L systems to be administered from almost any client platform (client must have a browser that supports Java 1.42)
- ▶ Enabling AIX 5L systems to be administered remotely
- ▶ Providing a system administration environment that provides a similar look and feel to the Windows and AIX 5L Common Desktop Environment (CDE)

The Web-based System Manager provides a comprehensive system management environment and covers most of the tasks in the SMIT user interface. Because you can run the Web-based System Manager only from a graphics terminal, use SMIT in the ASCII environment.

1.4 Object Data Manager: The system configuration storage facility in AIX 5L

AIX 5L utilizes a unique system for managing configuration and device details. This system is known as the Object Data Manager (ODM). Solaris depends heavily on text-based configuration files for its system settings. AIX 5L stores them in the ODM. The ODM is functionally equivalent to having a database system built into the OS. It stores a vast majority of AIX 5L OS configuration settings. You can also use it to manage data for application programs. There are some AIX 5L configuration items that are stored in text-based files and in the ODM. In such instances, the ODM takes precedence over the items stored in the configuration files.

If you have a command available to update an AIX 5L configuration setting, use the command instead of manually changing the contents of the configuration files. This way, you can leverage the ODM to make sure that it performs all the necessary updates to the system.

For more details about the ODM, refer to Appendix C, “AIX 5L Object Data Manager” on page 503.

1.5 Errpt and syslog in AIX 5L

In Solaris, all OS and hardware error notifications are channeled through the syslog daemon, and by convention, directed to `/var/adm/messages`. AIX 5L handles OS and hardware errors quite differently from Solaris.

AIX 5L stores OS and hardware error notifications in the AIX 5L error log. You can access the AIX 5L error log using the **errpt** command. For successful integration with operational monitoring tools such as IBM Tivoli Distributed Monitoring, Hewlett-Packard OpenView IT/Operations, Computer Associates

Unicenter, and so on that monitor UNIX systems through syslog, it is necessary to have AIX 5L forward its error log messages to syslog. To enable this, perform the following tasks to add an entry to the ODM, instructing the AIX 5L error daemon to forward all the errors to syslog:

1. Create a file and insert the text into it, for example, /tmp/odmadd, by using the command shown in Example 1-2.

Example 1-2 Creating a file and inserting text

```
errnotify:
    en_name = "syslog1"
    en_persistenceflg = 1
    en_method = "logger Message from errpt: `~/usr/bin/errpt -l $1 |
grep -v 'IDENTIFIER TIMESTAMP'`"
```

2. Add the information to the ODM by using the following command:

```
odmadd /tmp/odmadd
```

The headers from the messages in the error log are now forwarded to syslog through the user facility, and can be detected by operational monitoring software. When seen in syslog, these messages appear as shown in Example 1-3. These messages, which are passed to syslog from the error log, are quite basic and only include the headers from the error messages.

Example 1-3 An AIX 5L error log message forwarded to syslog

```
May  2 10:59:23 nueces root: Message from errpt: AA8AB241 0502105906 T
0 OPERATOR OPERATOR NOTIFICATION
```

Use the **errpt** command to access further information about the error message. There are a number of options to the **errpt** command (refer to the man page for the complete list). The most useful option for obtaining detailed information is **-a**. Example 1-4 and Example 1-5 show the output of the **errpt** and **errpt -a** commands when test messages are sent to the error log using the **errlogger** command.

Example 1-4 Sample errpt output

```
# errpt
IDENTIFIER  TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
AA8AB241    0502110106 T 0 OPERATOR       OPERATOR NOTIFICATION
AA8AB241    0502110006 T 0 OPERATOR       OPERATOR NOTIFICATION
AA8AB241    0502105906 T 0 OPERATOR       OPERATOR NOTIFICATION
AA8AB241    0502105706 T 0 OPERATOR       OPERATOR NOTIFICATION
```

Example 1-5 Sample errpt -a output

```
# errpt -a
```

```
-----  
----  
LABEL:          OPMSG  
IDENTIFIER:     AA8AB241  
  
Date/Time:      Tue May  2 11:01:13 CDT 2006  
Sequence Number: 131  
Machine Id:     00C4790E4C00  
Node Id:        nueces  
Class:          0  
Type:           TEMP  
Resource Name:  OPERATOR
```

```
Description  
OPERATOR NOTIFICATION
```

```
User Causes  
ERRLOGGER COMMAND
```

```
Recommended Actions  
REVIEW DETAILED DATA
```

```
Detail Data  
MESSAGE FROM ERRLOGGER COMMAND  
test
```

You will also notice that the default syslog configuration on AIX 5L is quite basic. It is recommended that you customize `/etc/syslog.conf` to the requirements of your site. Refer to the syslog man page for information about the configuration of syslog for AIX 5L. There are additional options for syslog for AIX 5L for the management and rotation of the log files.

Log files in AIX 5L can be automatically rotated, based on either the size of the file, a time duration, or both. You can specify the number of files that are kept and the compression and archiving options. The options for log file management are explained in the default `syslog.conf` file that is installed as part of the base install of AIX 5L. Example 1-6 shows an AIX 5L `syslog.conf` file with two entries defined. The first entry for `*.debug` rotates the log file when they reach 1 MB in size, and retains nine files. The second entry for `user.*` rotates the log file based on a time duration of one day, and retains 60 files and compresses them.

For more information about the use of the syslog facility in AIX 5L, refer to Chapter 16., "Troubleshooting" on page 429.

Example 1-6 AIX 5L syslog configuration file

```
# @(#)34      1.11  src/bos/etc/syslog/syslog.conf, cmdnet, bos530 4/27/04 14:
47:53
# IBM_PROLOG_BEGIN_TAG
# This is an automatically generated prolog.
#
# bos530 src/bos/etc/syslog/syslog.conf 1.11
#
# Licensed Materials - Property of IBM
#
# (C) COPYRIGHT International Business Machines Corp. 1988,1989
# All Rights Reserved
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# IBM_PROLOG_END_TAG
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
"/etc/syslog.conf" 110 lines, 4356 characters
#    line applies
```

```

# 2) An action.
#
# Each line can contain an optional part:-
#
# 3) Rotation.
#
# The fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list> <destination> [rotate [size <size> k|m] [files <files>] [time <
time> h|d|w|m|y] [compress] [archive <archive>]]
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
#     * - all (except mark)
#     mark - time marks
#     kern,user,mail,daemon, auth,... (see syslogd(AIX Commands Reference))
#
# <priority> is one of (from high to low):
#     emerg/panic,alert,crit,err(or),warn(ing),notice,info,debug
#     (meaning all messages of this priority or higher)
#
# <destination> is:
#     /filename - log to this file
#     username[,username2...] - write to user(s)
#     @hostname - send to syslogd on this machine
#     * - send to all logged in users
#
# [rotate [size <size> k|m] [files <files>] [time <time> h|d|w|m|y] [compress] [
archive <archive>]] is:
#     If <destination> is a regular file and the word "rotate" is
#     specified, then the <destination> is limited by either
#     <size> or <time>, or both <size> and <time>. The <size> causes
#     the <destination> to be limited to <size>, with <files> files
#     <size> or <time>, or both <size> and <time>. The <size> causes
#     the <destination> to be limited to <size>, with <files> files
#     kept in the rotation. The <time> causes the <destination> to be rotated
after
#     <time>. If both <time> and <size> are specified then logfiles
#     will be rotated once the the logfile size exceeds the <size>
#     or after <time>, whichever is earlier. The rotated filenames
#     are created by appending a period and a number to <destination>,

```

```

# starting with ".0".
#
# If compress option is specified then the logfile names will be
# generated with a ".Z" extension. The files keyword will be applicable
# to the logfiles which are currently under rotation. For example
# if we specify the compress option then only fileis with ".Z" extension
# will be under rotation and number of such files will be limited by
# <files> files. Any logfiles with an extension other than ".Z"
# will not be under the rotation scheme and thus will not be within
# the limit of <files> files. Similarly if we remove the compress
# option then the files which have been generated with ".Z" extension
# will no longer be the part of rotation scheme and will not be limited
# by the <files> files.
#
# The minimum size that can be specified is 10k, the minimum
# number of files that can be specified is 2. The default
# size is 1m (meg) and the default for <files> is unlimited.
# Therefore, if only "rotate" is specified, the log will be
# rotated with <size> = 1m.
# The compress option means that rotated log files that are not
# in use will be compressed.
# The archive option will save rotated log files that are not
# in use to <archive>.
# The default is not to rotate log files.
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
# mail.debug /usr/spool/mqueue/syslog
# If compress option is specified then the logfile names will be
# generated with a ".Z" extension. The files keyword will be applicable
# to the logfiles which are currently under rotation. For example
# if we specify the compress option then only fileis with ".Z" extension
# will be under rotation and number of such files will be limited by
# <files> files. Any logfiles with an extension other than ".Z"
# will not be under the rotation scheme and thus will not be within
# the limit of <files> files. Similarly if we remove the compress
# option then the files which have been generated with ".Z" extension
# will no longer be the part of rotation scheme and will not be limited
# by the <files> files.
#
# The minimum size that can be specified is 10k, the minimum
# number of files that can be specified is 2. The default
# size is 1m (meg) and the default for <files> is unlimited.

```



```

#       Therefore, if only "rotate" is specified, the log will be
#       rotated with <size> = 1m.
#       The compress option means that rotated log files that are not
#       in use will be compressed.
#       The archive option will save rotated log files that are not
#       in use to <archive>.
#       The default is not to rotate log files.
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
# mail.debug          /usr/spool/mqueue/syslog
# *.debug             /dev/console
# *.crit              *
# *.debug             /tmp/syslog.out      rotate size 100k files 4
# *.crit              /tmp/syslog.out      rotate time 1d
*.debug /var/log/messages      rotate size 1m files 9
user.* /var/log/user.log       rotate time 1d files 60 compress

```

1.6 Operator panel or light-emitting diode

A feature of the IBM AIX 5L pSeries combination is the operator panel or the light-emitting diode (LED) display in front of the machine or as part of the status of a logical partitioning (LPAR) on the Hardware Management Console (HMC). The operator panel is used to display the hardware status and diagnostic codes during system POST. It displays various status and error codes during the boot up and operation of AIX 5L. Refer to Chapter 8., “Boot and system initialization” and Chapter 16., “Troubleshooting” on page 429 for more information.

1.7 Important reminders: The inittab file and the Object Data Manager

This section provides some important reminders for system administrators who are new to AIX 5L.

The inittab file

Do not edit with a text editor. There are specialized commands for editing the inittab on an AIX 5L system. Many administrators who are new to AIX 5L have ended up with a nonbootable system because they manually edited the inittab

file with a text editor. Instead, always use the system commands for modifying the system init behavior. Following is a list of these commands:

- ▶ **chitab**
Use this command to change an entry (line) in the inittab file.
- ▶ **lsitab**
Use this command to display an entry from the inittab file.
- ▶ **mkitab**
Use this command to create a new entry in the inittab file.
- ▶ **rmitab**
Use this command to remove an entry from the inittab file. For more information, refer to 8.3, “The /etc/inittab file” on page 225.

The Object Data Manager

ODM contents override text-based configuration files. In AIX 5L, the majority of system configuration items are stored in the ODM. It is always best to modify AIX 5L settings using commands. When there are some AIX 5L settings found in the text-based files that are also duplicated in the ODM, it is the contents of the ODM that take precedence. In some instances, it is safe to modify a text-based configuration file, for example, /etc/hosts, /etc/environment. However, always refer to the AIX 5L documentation for the correct method of modifying a system setting. Do not just edit a file if the setting exists in a file.

1.8 AIX 5L kernel parameters versus Solaris kernel parameters

In Solaris, it is common to set System V interprocess communication parameters (shared memory, message queue, and semaphore settings) to suit application requirements. AIX 5L dynamically adjusts its settings for shared memory, messages queues, and semaphores.

There are also a number of other tunable parameter categories in Solaris:

- ▶ TCP/IP parameters
- ▶ Disk and file system parameters
- ▶ Process sizing and scheduling parameters
- ▶ Paging parameters
- ▶ A group of general parameters
- ▶ Terminal parameters
- ▶ Streams parameters
- ▶ Timer parameters

- ▶ Network File System (NFS) parameters
- ▶ System facility parameters
- ▶ Network cache accelerator

The commonly adjusted kernel parameters in AIX 5L fall within five categories:

- ▶ Scheduler and memory load control parameters
- ▶ Virtual memory manager parameters
- ▶ Synchronous input/output (I/O) parameters
- ▶ Asynchronous I/O parameters
- ▶ Disk and adapter parameters

For more information about the AIX 5L tunable parameters in the IBM System p and AIX 5L Information Center (look up “kernel parameters” using the Search field), refer to:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

Also refer to *AIX 5L Practical Performance Tools and Tuning Guide*, SG24-6478, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246478.pdf>

1.9 Some useful AIX 5L hints for the Solaris administrator

This section contains a few typical configuration tasks that a Solaris administrator must be aware of.

System dump configuration

A common postinstallation task on a Solaris machine involves ensuring that *crash dump* is configured. On AIX 5L, the system dump (crash dump) is automatically configured as part of the AIX 5L installation process. There is no requirement to manually configure the system dump as part of a postinstallation customization process. Two standard system dump configurations are used by the installer:

- ▶ The primary paging space `/dev/hd6` that is used as the dump device
This is the default for machines with less than 4 GB random access memory (RAM).
- ▶ A dedicated dump device
This is the default for machines with 4 GB RAM or more.

You can view and alter the system dump settings using the **sysdumpdev** command. Refer to the **sysdumpdev** man page or the AIX 5L information center for more information.

A flashing 888 on the operator panel of the machine indicates that a system dump has taken place. For more information about troubleshooting with regard to AIX 5L, refer to Chapter 16., “Troubleshooting” on page 429.

The System Resource Controller subsystem

The AIX 5L System Resource Controller (SRC) is an AIX 5L subsystem that is used for the management of system services such as syslogd, automountd, ypserv, and inetd. SRC controls the startup, shutdown and restarting of these services in a way that is very different than the rc.d script management methods used by Solaris. For more information about this, refer to “AIX 5L system services” on page 250.

The Resource monitoring and control subsystem

Monitoring a condition such as file system full, for example, on Solaris requires the use of either a script or other vendor-supplied software. AIX 5L has an inbuilt subsystem that can also be used to monitor for a condition. It is called *Resource Monitoring and Control* (RMC). This subsystem is installed and is running by default on an AIX 5L system and is a building block for both AIX 5L High Availability Cluster Multi-Processing (HACMP™) and communications storage manager clusters. RMC comes with a number of predefined conditions, but it is also possible to define custom conditions that can be used to monitor a custom application. RMC conditions can be used as triggers to perform an action, for example, to grow a file system when it hits a defined threshold.

For more information, refer to *A Practical Guide for Resource Monitoring and Control (RMC)*, SG24-6615. This IBM Redbook contains information and examples pertaining to RMC configuration. It is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246615.pdf>

Application start and stop

Historically, AIX 5L used /etc/inittab to start applications and /etc/rc.shutdown to stop applications. Some applications still utilize this start and stop method, while others use the newer /etc/rc.d file control method that is much more similar to the manner in which things are handled in Solaris. Refer to Chapter 8., “Boot and system initialization” on page 213 for more information about this.

Integration with IBM Tivoli Storage Manager

The AIX 5L sysback backup tool can be integrated with IBM Tivoli Storage Manager for managing bare metal recovery of AIX 5L systems. For more

information, refer to 14.6, “AIX 5L SysBack (IBM Tivoli Storage Manager for System Backup and Recovery)” on page 415. Also refer to *IBM Tivoli Storage Manager: Bare Machine Recovery for AIX with SYSBACK*, REDP-3705, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/redp3705.html?Open>



Part 2

System administration differences

This part of the book contains chapters describing system administration differences, where each chapter focuses on a specific functional area. This book assumes that the reader is an experienced Solaris system administrator who is undertaking (or considering) a migration to AIX 5L. Therefore, each chapter assumes reader knowledge about how the task topic is performed on a Solaris system and compares that with the procedures for performing a similar task on AIX 5L.

Each chapter attempts to “match” AIX 5L graphical user interface (GUI) tools, commands, and configuration files with AIX 5L-based counterparts where they are similar. The chapters also describe the differences in or lack of comparable functionality. The chapters include links to the appropriate AIX 5L guides and “how-to” documentation.

Important: Because this book assumes that the reader is an experienced Solaris system administrator who is undertaking (or considering) a migration to AIX 5L, the content in this part of the book must *not* be used as a substitute for detailed AIX 5L system administration documentation, but rather as a “cross-reference” work for an administrator trying to find out what tools are available on AIX 5L to perform a given job.

Following are the functional areas that this part deals with:

- ▶ Chapter 3, “Operating system installation” on page 47
- ▶ Chapter 4, “Disks and file systems” on page 91
- ▶ Chapter 5, “Software management” on page 133
- ▶ Chapter 6, “Device management” on page 157
- ▶ Chapter 7, “Network services” on page 183
- ▶ Chapter 8, “Boot and system initialization” on page 213
- ▶ Chapter 9, “Managing system resources” on page 239
- ▶ Chapter 10, “Printing services” on page 279
- ▶ Chapter 11, “Users and groups” on page 321
- ▶ Chapter 12, “Monitoring and performance” on page 359
- ▶ Chapter 13, “Security and hardening” on page 377
- ▶ Chapter 14, “Backup and restore” on page 399
- ▶ Chapter 15, “High availability and clustering overview” on page 421
- ▶ Chapter 16, “Troubleshooting” on page 429



Introduction to IBM System p

This chapter provides an introduction to IBM System p platforms.

This chapter discusses the following topics:

- ▶ 2.1, “Introduction to IBM System p and IBM RS/6000 architectures” on page 30
- ▶ 2.1.9, “POWER4-based server features” on page 34
- ▶ 2.1.10, “POWER5-based server features” on page 35
- ▶ 2.2, “Planning considerations” on page 36
- ▶ 2.5, “IBM System p High Performance Switch” on page 45
- ▶ 2.6, “IBM System Cluster 1600” on page 46

2.1 Introduction to IBM System p and IBM RS/6000 architectures

In February 1990, IBM introduced the first reduced instruction set computer, IBM RISC System/6000® (IBM RS/6000®) with the first Performance Optimization With Enhanced RISC (IBM POWER™) architecture. Since that date, several POWER architectures have been designed for the RS/6000 models.

The IBM PowerPC® family of microprocessors, a single-chip implementation jointly developed by Apple, IBM, and Motorola, established a rapidly expanding market for RISC-based hardware and software. IBM has many successful lines of PowerPC-based products for workstations and servers.

Motorola introduced a broad range of desktop and server systems, and other companies such as Bull, Canon, and FirePower have announced or shipped PowerPC-based systems. Apple has Power Macintosh systems, and companies such as Daystar, Pioneer, Power Computing, and Radius have also announced Power Macintosh-compatible systems. With these successes, the alliance ended and IBM continued to build on this CPU architecture and design, later introducing the powerful copper and silicon on insulator technology deployed in the IBM eServer pSeries and IBM eServer iSeries™ servers.

2.1.1 RS/6000 system bus types

The function of the bus is to provide the highway for information to flow between the RS/6000 system elements and the optional input/output (I/O) feature cards, for example, Small Computer System Interface (SCSI) adapters and Ethernet cards, that are plugged into the adapter slots.

Peripheral Component Interconnect-based RS/6000 systems

Peripheral Component Interconnect (PCI) buses are an open industry specification that supports complete processor independence. The PCI bus works across multiple operating system (OS) platforms. IBM uses this technology in all its RS/6000.

RS/6000 also contains an Industry Standard Architecture (ISA) bus for use with some built-in devices such as the diskette drive and the keyboard.

Some earlier model PCI systems contain ISA slots that accept standard ISA cards. However, the latest models no longer support this.

The first RS/6000s were based on IBM Micro Channel® architecture (MCA). The MCA systems are sometimes referred to as classical systems. These were very popular. MCA machines can be easily recognized by the physical key in front of the machines. PCI and MCA are basically the same from an administrative viewpoint. However, there are differences in the startup procedure.

Architecture types

AIX 5L V5.1 supports the three architecture types shown in Table 2-1.

Table 2-1 Architecture types

Architecture	Processor	Description
rs6k	POWER	This is the original or “classic” RS/6000 workstation, based on the Micro Channel bus
rspc	POWER	POWER Reference Platform, based on the PCI bus
chrp	POWER	Common Hardware Reference Platform, based on the PCI bus

Note: The `bootinfo -p` command returns the system architecture type.

2.1.2 POWER2 Super Chip

The next microprocessor launched by IBM was the IBM POWER2™ Super Chip (P2SC) processor. This microprocessor was first introduced in RS/6000 Model 595. Currently, the P2SC processors are employed only in the RS/6000 SP Thin4 nodes, where they run at a clock speed of 160 MHz, with a theoretical peak speed of 640 MEGAFLOPS.

The POWER2 Super Chip is a compression of the POWER2 eight-chip architecture into a single chip with increased processor speed and performance. It retains the design of its predecessor, the POWER2. The initial models had clock speeds of 120 MHz and 135 MHz. High-density CMOS-6S technology allows each to incorporate 15,000,000 transistors.

2.1.3 POWER3

IBM POWER3™ was the next microprocessor developed by IBM. The POWER3 microprocessor introduced a new generation of 64-bit processors designed specially for high-performance and visual computing applications. POWER3 processors are the replacement for POWER2 and POWER2 Super Chip in high-end RS/6000 workstations and technical servers.

The POWER3 processor was designed to provide high-performance floating point computation. This type of microprocessor is widely used in areas such as the oil and gas industry, reservoir simulation, seismic processing, and weather forecast prediction.

The POWER3 is designed for frequencies of up to 600 MHz when fabricated with advanced semiconductor technologies, such as copper metallurgy and Silicon-On-Insulator (SOI). In contrast, the P2SC design has reached its peak operating frequency at 160 MHz. The first POWER3-based system, RS/6000 43P 7043 Model 260, runs at 200 MHz.

2.1.4 POWER3 II chip

POWER3 II is a third-generation super scalar design that is used for 64-bit technical and scientific applications. The POWER3 and POWER3 II microprocessors are similar. The use of copper and an increased number of transistors in POWER 3 II are the main differences. This processor operates between 333 MHz and 400 MHz.

2.1.5 PowerPC

The PowerPC family of processors was started by the alliance between Apple, Motorola, and IBM in 1991. This alliance established a rapidly expanding market for RISC-based hardware and software.

The IBM PowerPC architecture has an entire range of variants, most of which are still used in workstation and server products. Both the processors have a 32-bit architecture, and both the processors provide the support required to support graphics, computation, and multimedia-intensive applications.

The 604e is a 32-bit implementation of the PowerPC architecture, with clock speeds of 233 - 375 MHz. IBM PowerPC 750™ is another model of the PowerPC chip. This is a second 32-bit implementation, clocked between 300 - 466 MHz.

2.1.6 The RS64 processor family

The RS64 processor is a second 64-bit implementation, clocked at 262 MHz and 340 MHz. There are four generations of this processor.

The main characteristic of the RS64-II processor is that it runs at 262 MHz, compared to 125 MHz for the earlier RS64 processor. This chip also has an 8 MB cache, which is double the earlier size.

In summary, the RS64 Series processors are robust, delivering real performance on real applications for the next generation 64-bit RISC commercial and server processors, while retaining the optimum chip size and power. They achieve high performance on real applications because of their low latency design and the superior silicon technology from IBM. The POWER4+™ processor is an update of the original POWER4™. It was produced using a 0.13 micron process, thus enabling higher clock speeds and performance improvements on the original POWER4.

For additional information, refer to the following Web site:

http://www.ibm.com/servers/eserver/pseries/library/wp_systems.html

2.1.7 POWER4 and POWER4+

The IBM POWER4 processor was designed to operate at speeds of over 1 GHz and to handle commercial and technical workloads. Business applications include attributes from both commercial and technical workloads. Binary compatibility with 64-bit PowerPC architecture is maintained. One of the main characteristics is that a single POWER4 processor chip contains two POWER4 processors. The IBM eServer pSeries 690 was the first pSeries model to utilize this microprocessor.

The POWER4+ processor is an update of the original POWER4. It was produced using a 0.13 micron process, thus enabling higher clock speeds and performance improvements on the original POWER4.

2.1.8 POWER5 and POWER5+

POWER5™ is the current (at time of writing this IBM Redbook) generation of processors used in IBM eServer pSeries and IBM eServer iSeries servers. Following is a list of its features:

- ▶ Binary and structural compatibility with existing POWER4 systems
- ▶ Enhanced and extended Symmetric Multiprocessing (SMP) scalability
- ▶ Symmetric multithreading
- ▶ Superior performance
- ▶ Advanced virtualization features
- ▶ Sub-CPU dynamic logical partitioning (DLPAR) capability
- ▶ Dynamic power management
- ▶ Enhanced reliability, availability, and serviceability

POWER5+™ is an update of POWER5 for a 0.90 micron process, featuring increased clock speeds and higher performance, using less power.

In April 2002, IBM disclosed information about its future server chips. IBM's plans included enhancing its POWER5 and POWER6™ processors with an ability called *fast path*. Fast path is designed to take over tasks that are usually handled by software applications. POWER5 can perform some software tasks that are commonly handled by an operating system, such as the packaging of data that is to be sent to networks. POWER6 will add more fast path enhancements. For more information, refer to the following Web site:

<http://www.chips.ibm.com>

2.1.9 POWER4-based server features

The POWER4 range of IBM System p servers range from the entry-level 1-way or 2-way p615 to the high-end 32-way p690 (*Regatta*). All of them feature the 64-bit POWER4 or POWER4+ processor and DLPAR¹ capabilities on LPAR capable models. Other features of this series of servers include:

- ▶ An integrated service processor
- ▶ Hot-swap redundant power supplies
- ▶ Hot-swap fans and disk drives
- ▶ Light-emitting diode (LED) service identification
- ▶ Auto reboot on power loss
- ▶ Dynamic processor deallocation when a processor error is encountered (multiprocessor systems only)
- ▶ Predictive failure analysis
- ▶ Persistent component deallocation on reboot
- ▶ IBM Chipkill™ correction in memory
- ▶ Hot-plug for Peripheral Component Interconnect-X (PCI-X) slots
- ▶ Concurrent runtime diagnostics
- ▶ Automatic first failure data capture and diagnostic fault isolation
- ▶ Dynamic error recovery
- ▶ PCI bus parity error recovery
- ▶ System's management services
- ▶ Capacity upgrade on demand (select models)
- ▶ Choice of AIX 5L and Linux OS

¹ Dynamic LPAR requires AIX 5L V5.2 or later.

POWER4-based servers that support LPAR are capable of providing one LPAR per CPU, with dynamic reallocation of resources between the LPARs, possibly where both the firmware and the OS support this feature. pSeries LPAR differs from Sun Fire™ domains, in that, the domains are defined at a system-board level. LPARs can be said to provide a finer level of control over the allocation of system resources.

For more information about POWER4-based systems, refer to *IBM eServer pSeries Systems Handbook 2003 Edition*, SG24-5120, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg245120.html?Open>

2.1.10 POWER5-based server features

The POWER5 range of IBM System p servers range from the entry level 1-way or 2-way p610 and p505 blade to the high-end 64-way mainframe inspired p595 (*Squadron*). POWER5 technology is also available in the System i™ line of servers. Although these are traditionally used to run i5 OS (IBM AS/400®), they can also be used to run AIX 5L². This section focuses on the p5 series of servers on which AIX 5L is normally found. All of them feature the 64-bit POWER5 or POWER5+ processor and micro partitioning³ capabilities by adding the Hardware Management Console (HMC) or using the Integrated Virtualization Manager on select models. Other features of this series of servers include:

- ▶ An integrated service processor
- ▶ Hot-swap redundant power supplies
- ▶ Hot-swap fans and disk drives
- ▶ LED service identification
- ▶ Auto reboot on power loss
- ▶ Dynamic processor deallocation when a processor error is encountered (multiprocessor systems only)
- ▶ Predictive failure analysis
- ▶ Persistent component deallocation on reboot
- ▶ Chipkill correction in memory
- ▶ Hot-plug for PCI-X slots
- ▶ Concurrent runtime diagnostics
- ▶ Automatic first failure data capture and diagnostic fault isolation

² Refer to *AIX 5L on IBM eServer i5 Implementation Guide*, SG24-6455:
<http://www.redbooks.ibm.com/abstracts/sg246455.html?Open>

³ Requires AIX 5L V5.3 or later

- ▶ Dynamic error recovery
- ▶ PCI bus parity error recovery
- ▶ System's management services
- ▶ Capacity upgrade on demand (select models)
- ▶ Choice of AIX 5L and Linux OS
- ▶ Advanced POWER virtualization
 - Micro Partitioning
 - Virtual Ethernet
 - Virtual SCSI
 - Virtual Serial
 - Partition Load Manager

For more information about p5 virtualization, refer to:

<http://www-03.ibm.com/systems/p/apv/index.html>

The latest information about POWER5-based servers is available in the following Web sites:

- ▶ <http://publib.boulder.ibm.com/eserver/>
- ▶ <http://www-03.ibm.com/systems/p>

2.2 Planning considerations

This section describes the issues that system administrators must consider before beginning the installation of an IBM System p, or IBM eServer BladeCenter® JS20 (IBM BladeCenter JS20).

2.2.1 IBM System p

Two general paths are available for installing AIX 5L on IBM eServer p5 systems, depending on your configuration choice, a stand-alone system or a partitioned system.

Monolithic (stand-alone)

In a monolithic installation, AIX 5L owns the entire server and all its resources. A monolithic install does not require any POWER technology-specific preinstallation planning.

Note: IBM System p is initially preconfigured for monolithic operation.

Hosted (partitioned)

In a hosted installation, AIX 5L runs in a partition along with other instances of AIX 5L or Linux. By using LPAR, a single physical system can be divided into multiple logical partitions, each running their own OS image.

2.3 Concepts for AIX 5L logical partitions

This section provides information that helps you familiarize yourself with the hardware and software required for AIX 5L logical partitions.

Logical partitioning is the ability to make a server run as if there were two or more independent servers. When you logically partition a server, you divide the resources on the server into subsets called logical partitions. Processors, memory, and input/output (I/O) devices are examples of resources that you can assign to logical partitions. You can install software on the logical partition, and the logical partition runs as an independent logical server with the processor, memory, and I/O resources that you have allocated to it.

Use tools to partition the IBM System p. The tool that you use to partition each server depends on the server model and the OS and features that you want to use:

- ▶ Hardware Management Console

The HMC is a hardware appliance that connects to the server firmware. Use the HMC to specify to the server firmware how you want resources to be allocated among the logical partitions on the managed system. Also use the HMC to start and stop the logical partitions, update the server firmware code, manage IBM eServer Capacity on Demand, and transmit service information to service and support if there are any hardware problems with your managed system.

The server firmware is code-stored in system flash memory on the server. The server firmware directly controls the resource allocations on the server and the communications between the logical partitions on the server. The HMC connects with the server firmware and specifies how the server firmware allocates resources on the server.

If you use a single HMC to manage a server, and the HMC malfunctions or becomes disconnected from the server firmware, the server continues to run, but you will not be able to change the logical partition configuration of the server or manage the server. If necessary, attach an additional HMC to act as a backup and to provide a redundant path between the server and IBM service and support.

Partitioning using the HMC is supported on all IBM System p5™, and IBM eServer OpenPower™ server models, although some models require you to enter an Advanced POWER Virtualization activation code before you partition the server.

► Integrated Virtualization Manager

The Integrated Virtualization Manager is a browser-based system management interface for a Virtual I/O Server that enables you to create and manage logical partitions on a single IBM System p5 server. The Integrated Virtualization Manager is supported only on select IBM eServer p5, IBM System p5, and the IBM eServer OpenPower⁴ server models.

A Virtual I/O Server is a software that provides virtual storage and shared Ethernet resources to the other logical partitions on the managed system. A Virtual I/O Server is not a general purpose OS that can run applications. A Virtual I/O Server is installed on a logical partition in place of a general purpose OS and is used solely to provide virtual I/O resources to other logical partitions with general purpose OS. Use the Integrated Virtualization Manager to specify to a Virtual I/O Server about how these resources are assigned to the other logical partitions.

To use the Integrated Virtualization Manager, first install a Virtual I/O Server on an unpartitioned server. A Virtual I/O Server automatically creates a logical partition for itself, called the management partition, for the managed system. The management partition is the Virtual I/O Server logical partition that controls all the physical I/O resources on the managed system.

After you install the Virtual I/O Server, configure a physical Ethernet adapter on the server to connect to the Integrated Virtualization Manager from a computer with a Web browser.

For more information about the use of Virtual I/O Server, refer to the following publications:

- *System p5 and i5, eServer p5 and i5 and OpenPower: Using the Virtual I/O Server*

<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/topic/iphb1/iphb1.pdf>

- *Advanced POWER Virtualization on IBM System p5, SG24-7940*
- *Advanced POWER Virtualization on IBM eServer p5 Servers: Architecture and Performance Considerations, SG24-5768*

► Micro-Partitioning™ or shared processing

This enables logical partitions to share the processors in the shared processor pool. The shared processor pool includes all the processors on the

⁴ OpenPower systems are primarily used for running Linux

server that are not dedicated to specific logical partitions. Each logical partition that uses the shared processor pool is assigned a specific amount of processor power from the shared processor pool. If the logical partition requires more processor power than its assigned amount, the logical partition is set by default to use the unused processor power in the shared processor pool. The amount of processor power that the logical partition can use is limited only by the virtual processor settings of the logical partition and the amount of unused processor power available in the shared processor pool.

- ▶ **Dynamic logical partitioning**

This enables you to move resources to, from, and between the running logical partitions manually without shutting down or restarting the logical partitions. This enables you to share devices that logical partitions use occasionally, for example, if the logical partitions on your server use an optical drive occasionally, you can assign a single optical drive to multiple logical partitions as a desired device. The optical drive will belong to only one logical partition at a time, but you can use dynamic logical partitioning to move the optical drive between logical partitions, as required. On servers that are managed using the Integrated Virtualization Manager, dynamic logical partitioning is supported only for the management partition. Dynamic logical partitioning is not supported on servers that are managed using the Virtual Partition Manager.

- ▶ **Virtual I/O**

This enables logical partitions to access and use I/O resources on other logical partitions, for example, virtual Ethernet enables you to create a virtual local area network (LAN) that connects the logical partitions on your server to each other. If one of the logical partitions on the server has a physical Ethernet adapter that is connected to an external network, you can configure the OS of that logical partition to connect the virtual LAN with the physical Ethernet adapter. This enables the logical partitions on the server to share a physical Ethernet connection to an external network.

2.3.1 Hardware requirements for AIX 5L logical partitions

During the process of planning for logical partitions, decide how you want to configure hardware resources. Each AIX 5L logical partition on an IBM eServer hardware system requires the following minimum hardware resources:

- ▶ One dedicated processor or 0.1 processing unit
- ▶ 128 MB memory
- ▶ One storage adapter (physical or virtual)

- ▶ Approximately 2.2 GB of space provided by one of the following storage options:
 - Internal storage using SCSI adapters and drives attached within the system
 - External storage using storage area network (SAN) adapters and drives in an external storage unit
 - Virtual storage using a virtual SCSI adapter and storage in a different partition
- ▶ One network adapter (physical or virtual)

2.3.2 Logical partition planning tasks

Perform the following partition planning tasks:

1. Identify the hardware requirements for each logical partition based on the hardware configuration of the server.
2. Identify whether the partitions will communicate with other partitions, servers, or workstations using physical or virtual Ethernet connections.
3. Design and validate your partition configuration using the IBM LPAR Validation Tool (LVT), which is available at:

<http://www.ibm.com/servers/eserver/series/lpar/>

The LVT provides you with a validation report that reflects your system requirements when not exceeding logical partition recommendations.

2.4 IBM eServer BladeCenter JS20

This section discusses planning considerations associated with the implementation of IBM eServer BladeCenter JS20. Specifically, it covers network planning.

For detailed information about AIX 5L on BladeCenter JS20, refer to *The IBM eServer BladeCenter JS20*, SG24-6342, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg246342.html?open>

2.4.1 Network planning

Successful installation of IBM BladeCenter JS20 requires that you have a clear plan about how you will use the various networking capabilities of the BladeCenter infrastructure. This plan must address the following questions:

- ▶ What network connectivity is required for the blade servers to support the applications installed on them?
- ▶ What network connectivity is required to manage the BladeCenter, I/O modules, and blade servers?
- ▶ What virtual local area networks (VLANs) are required for each LAN Switch I/O Module to provide the network connectivity established previously?
- ▶ What IP subnet will be used for each VLAN and how will IP addresses be allocated to each device on the VLAN?
- ▶ Will IP addresses be assigned statically or dynamically using Dynamic Host Configuration Protocol (DHCP)?
- ▶ What host names will be used for each network interface?
- ▶ How will host names be resolved to IP addresses?
- ▶ Are there requirements for a high-performance, low-latency interconnection network?
- ▶ Where multiple BladeCenter chassis are installed, how will they be interconnected?

2.4.2 Minimal network requirements

At the minimum, most IBM BladeCenter JS20 environments have the following network requirements:

- ▶ A dedicated hardware management subnet
This is used to access both the management module and the management interfaces of the I/O modules that are installed on each BladeCenter chassis.
- ▶ A Serial over LAN (SoL) subnet internal to each BladeCenter chassis that supports the SoL remote text console function
This is always implemented using a LAN Switch I/O module installed in I/O module bay 1.
- ▶ A subnet connected to each BladeCenter JS20
This is used to install and manage the OS on the blade server.

- ▶ One or more subnets connected to each BladeCenter JS20
 - They are used by the applications installed on the blade server to communicate to other systems.

Figure 2-1 illustrates how these requirements can be provided in a logical network view.

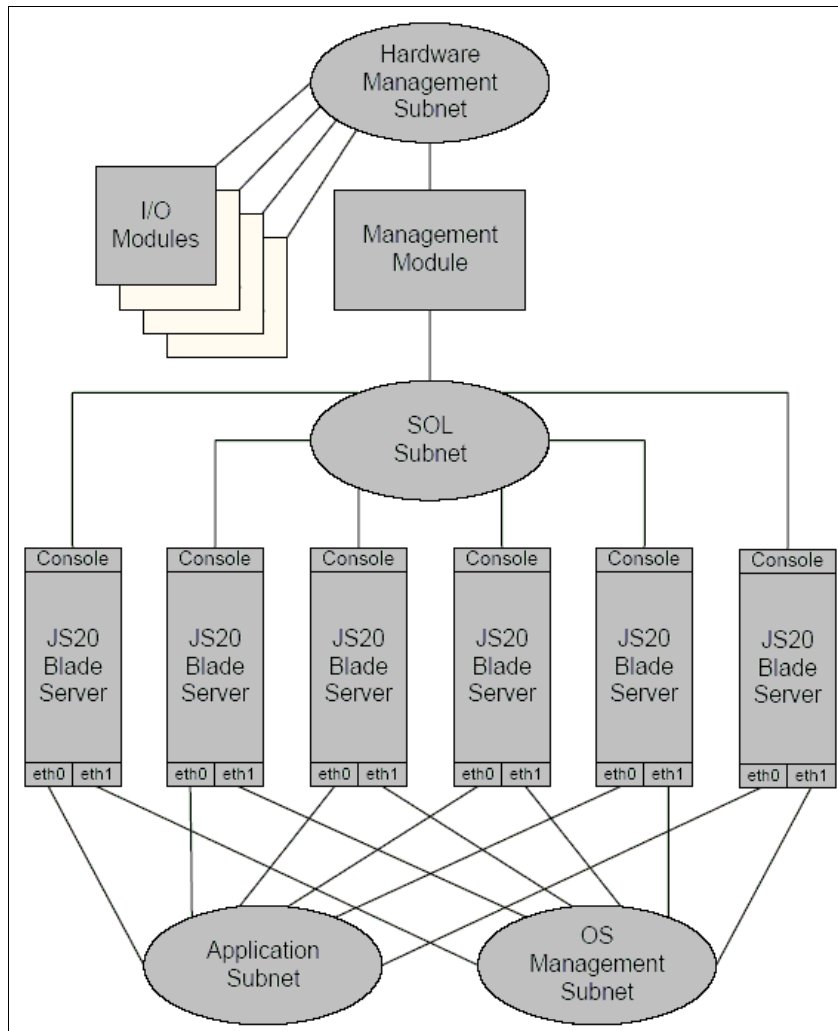


Figure 2-1 Network logical view

The following four sections describe each of the logical networks illustrated in Figure 2-1.

Hardware management subnet

It is recommended that you establish a dedicated hardware management subnet. The 10/100BaseT Ethernet interface on the management modules installed on each BladeCenter chassis provides the gateway to this subnet for each BladeCenter chassis. Install external LAN switches or hubs to interconnect the 10/100BaseT Ethernet interface on the management modules of each BladeCenter chassis with external management systems.

Use this subnet to access the management module Web interface and command-line interface (CLI). You can also use this subnet to access the Web interface and CLI of the I/O modules.

System management applications such as IBM Director and IBM Cluster Systems Management also use this subnet to communicate with the hardware management functions of the BladeCenter infrastructure.

Restrict the access to this subnet to those management systems, system administrators, and operators who have the responsibility of managing the BladeCenter infrastructure.

Allocate multiple IP addresses to each BladeCenter chassis on this subnet, including the following:

- ▶ One IP address for the external interface of the management module in each BladeCenter chassis
- ▶ One IP address for the internal interface of the management module in each BladeCenter chassis
- ▶ One IP address for the management interface of each I/O module in each BladeCenter chassis

Note: Although the logical network view shown in Figure 2-1 illustrates the I/O management module interfaces connecting directly to the hardware management subnet, they are physically connected through the management module that acts as a gateway to those interfaces. The management module performs a proxy Address Resolution Protocol (ARP) function to make it look as if the I/O module management interfaces are attached to the hardware management subnet.

It is possible to use a different subnet for the management module internal network interface and I/O module management interfaces. However, this configuration is *not* recommended.

Serial over local area network subnet

The SoL remote text console function requires a subnet and underlying VLAN that is implemented by a LAN Switch I/O Module installed in I/O module bay 1 of the BladeCenter chassis. This subnet and VLAN are entirely internal to each BladeCenter chassis and must not be externally accessible.

If you use the 4-Port Gigabit Ethernet Switch Module or the Nortel Networks Layer 2-7 Gigabit Ethernet Switch Module, the VLAN uses the VLAN ID 4095. If you use the Cisco Systems Intelligent Gigabit Ethernet Switch Module, you can select the VLAN ID.

Assign a unique range of IP addresses to this subnet for use by the SoL remote text console function.

Important: An IP address is required for each blade server.

Specify only the starting IP address within the range of IP addresses that you assign into the management module. The management module then automatically assigns consecutive IP addresses from the starting address that you provide to each blade server that you have installed.

Operating system management subnet

We expect most environments that use the BladeCenter JS20 to rely on the network installation procedure to install the OS.

The OS management subnet is used to support both the initial installation and the subsequent management of the OS installed on IBM BladeCenter JS20s. This subnet is implemented using a VLAN provided by the LAN Switch I/O modules installed in I/O module bay 2 of each BladeCenter chassis. Alternatively, you can implement it using a Pass-Thru I/O Module installed in I/O module bay 2 that is connected to an external LAN switch.

Application subnet

The primary reason you install BladeCenter JS20 is to support applications. Many applications have requirements to communicate with other systems. Use one or more application subnets for this purpose.

The primary application subnet is implemented using a VLAN provided by the LAN Switch I/O Modules installed in I/O module bay 1 of each BladeCenter chassis. The same LAN Switch I/O Module is used to support the SoL subnet and VLAN.

Where different BladeCenter JS20s participate in different applications, and there is a requirement for separate application traffic, you may have to define multiple application subnets and VLANs. Each BladeCenter JS20 is connected to the appropriate application subnet based on the applications that are installed on the blade server.

If application communication requirements with other systems are complex, install an additional pair of Gigabit Ethernet interfaces on each BladeCenter JS20, using the Gigabit Ethernet Expansion Card in conjunction with the compatible I/O modules installed in I/O module bays 3 and 4.

2.5 IBM System p High Performance Switch

The IBM System p High Performance Switch is a high-speed method of interconnecting IBM System p servers. It is used in situations where two or more IBM System p machines or LPARs require high-bandwidth, low-latency intercommunications that cannot be provided by other means. It is commonly used in High Performance Parallel Clusters as part of Cluster 1600.

The IBM System p High Performance Switch has been developed over many years by the IBM High Performance Computing Group. Following are the features of the High Performance Switch:

- ▶ High levels of reliability
- ▶ Highly scalable
- ▶ Reliable and secure
- ▶ Out-of-band monitoring
- ▶ Low latency
- ▶ Fast transfers

Refer to *An Introduction to the New IBM eServer pSeries High Performance Switch*, SG24-6978, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246978.pdf>

2.6 IBM System Cluster 1600

IBM System Cluster 1600 is a highly scalable clustering solution that can be used for large-scale computational modeling and analysis, large databases, business intelligence, and data center consolidation. A Cluster 1600 can comprise a combination of IBM System p and OpenPower servers. The IBM Cluster System 1600 can make:

- ▶ AIX 5L or Linux nodes
- ▶ Cluster Systems Management (CSM) software for managing the cluster
- ▶ Cluster interconnect can be:
 - Ethernet
 - IBM eServer pSeries High Performance Switch
 - InfiniBand
 - Myrinet (Linux only)
- ▶ Software for creating and running parallel software
 - Engineering and Scientific Subroutine Library (ESSL)
 - Parallel ESSL
 - Parallel environment
 - XL Fortran
 - VisualAge® C++
- ▶ General Parallel File System™ (GPFS™)
- ▶ Loadleveler job scheduling software
- ▶ High availability software

For more information about Cluster 1600, refer to the following Web site:

<http://www-03.ibm.com/servers/eserver/clusters/hardware/1600.html>



Operating system installation

This chapter describes the difference between the way Solaris and AIX 5L perform their installations. Both have the option of using either a text-based installation or a graphical user interface (GUI) installation format and allow installation from different media sources.

This chapter discusses the following topics:

- ▶ 3.1, “Basic system installation” on page 48
- ▶ 3.7, “Other installation methods” on page 55
- ▶ 3.8, “Using the multibos utility” on page 67
- ▶ 3.9, “Network Installation Manager” on page 67
- ▶ 3.10, “AIX 5L installation in a partitioned environment” on page 77
- ▶ 3.11, “Installing AIX 5L on IBM BladeCenter” on page 89

3.1 Basic system installation

This section discusses the basic installation procedure with a local CD-ROM or DVD-ROM drive. Solaris and AIX 5L offer other types of installation methods too. These are described in 3.7, “Other installation methods” on page 55.

Local CD or DVD installations are the same for Solaris and AIX 5L. The installation program prompts for information when required. An options menu is presented in some parts for you to make the appropriate choices.

As with a Solaris installation, AIX 5L too performs the following operations:

Note: The following list is not in any specific order and is not a complete list of the options that will be presented to you. It is a representation of the basic information that will be presented. When using another installation method, these prompts might not be displayed if they are preconfigured in the installation procedure, or you might have extra options.

- ▶ Probe the hardware for devices and load the appropriate device drivers
- ▶ Assign a host name
- ▶ Set up a network setup type, Dynamic Host Configuration Protocol (DHCP) or static IP

If you choose static IP, you will be asked to enter the IP address, subnet mask, default gateway, and Domain Name System (DNS) servers to use.

- ▶ Select a region type to use for languages
- ▶ Select a time zone
- ▶ Select the initial or upgrade installation type
- ▶ Prompt for a hard disk to use for root partition
- ▶ Prompt for an automatic or manual disk layout for the file systems
- ▶ Prompt for the software bundle or packages to install

Table 3-1 compares some of the useful commands used in Solaris installation with those used in AIX 5L.

Table 3-1 Installation command comparison

Tasks	Solaris	AIX 5L
Set bootlist on hardware	Boot “ok” prompt	Systems Maintenance Service menu
Automated live patch upgrade	Patch Manager	Service Update Management Assistant

Tasks	Solaris	AIX 5L
Install preserving user data	Live Upgrade	Preservation installation
Install operating system (OS) on another disk	Live Upgrade	alt_disk_install
Network installation	<ul style="list-style-type: none"> ▶ JumpStart™ ▶ Flash Install 	Network Install Manager
Create installation server	setup_install_server <i>install_dir_path</i>	nimconfig
Create a boot server for network install	setup_install_server -b	smitty nim_config_env
Set up a client for network installation	add_install_client	smitty nim_mkmac
Display current OS level	uname -a	oslevel -r
Display installed packages	pkginfo or kgparam	lslpp -L
Display installed patches	showrev -p	instfix -ia
Display term type	echo \$TERM	termdef

Figure 3-1 shows a flowchart outlining the steps involved in a Base Operating System (BOS) installation.

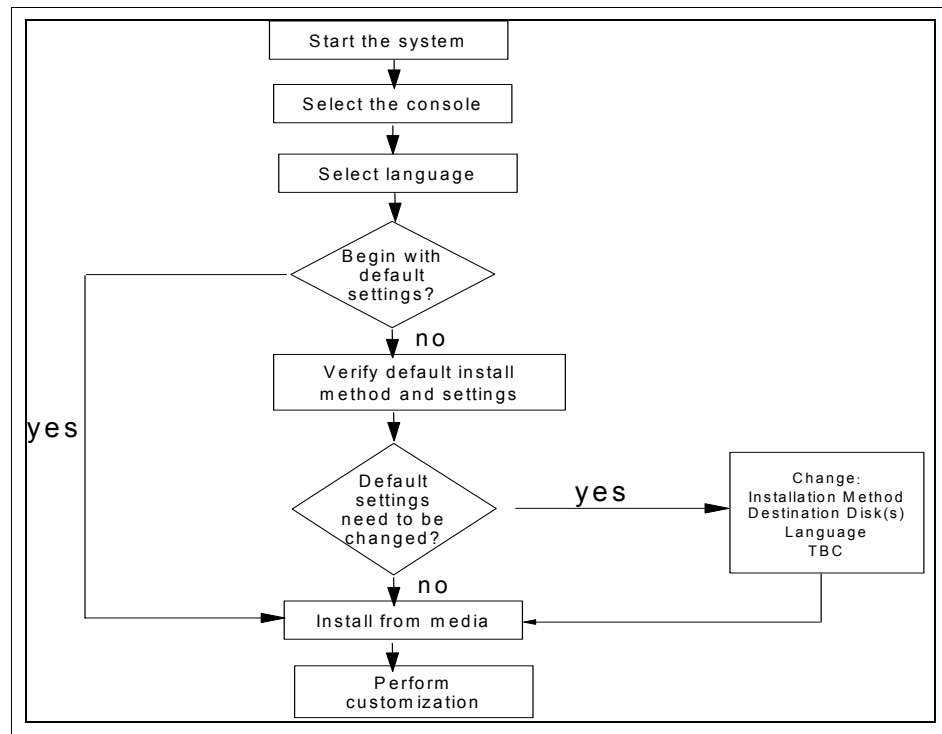


Figure 3-1 Flowchart outlining the steps involved in a BOS installation

3.2 Graphical installation or text installation

The previous section (3.1, “Basic system installation” on page 48) does not mention the console device being used. As with Solaris on some scalable processor architecture (SPARC) platforms, you have the choice of using a graphical console to perform the installation. Even if you are on a graphical console, you have the choice of selecting a text-based installation.

In Solaris, when installing from a CD set, the installation CD always starts a graphical installation and CD 1 starts a text-based installation. On a DVD, you will be prompted for the type of installation to use.

In AIX 5L, you can manage the install in the following ways:

- ▶ Connect remotely using Web-based System Manager Remote Client
- ▶ Connect directly using a laptop through the serial port

- ▶ Open a virtual terminal window on the Hardware Management Console (HMC) server through Secure Shell (SSH) using the `mkvterm` command.

For more information about the HMC management setup, refer to:

http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/hardware_docs/pdf/380590.pdf

To configure your system after the installation is complete, three methods are available:

- ▶ Configuration assistant application
- ▶ SMITTY
- ▶ Command line

To install the Web-based System Manager, perform the following tasks:

1. Enter the following URL in your browser:

`http://hmchostname/remote_client.html`

You will be prompted for the HMC root user name and password.

2. After the client is installed, you will have access to the available frames and partitions.
3. After you have the HMC and the partitions set up with the required devices, you are ready to start the installation:
 - a. Open a window by right-clicking the partition. Insert CD 1 from the AIX 5L OS Installation CD pack.
 - b. From the Web-based System Management Console restart the partition. When the partition restarts, the following line appears:
`memory keyboard network scsi speaker`

- c. Press F1 when you see this or Esc+ if you are working through the serial port. This brings you to the System Management Services screen (Figure 3-2).

```
Version SF220_051
SMS 1.5 (c) Copyright IBM Corp. 2000,2003 All rights reserved.
-----
Main Menu
 1. Select Language
 2. Setup Remote IPL (Initial Program Load)
 3. Change SCSI Settings
 4. Select Console
 5. Select Boot Options

-----

Navigation Keys:

                                     X = eXit System Management Services
-----
Type the number of the menu item and press Enter or select Navigation Key: █
```

Figure 3-2 System Management Services main menu

This section is important for setting up the initial program load (IPL) parameters because these are required for future network-based boots, installations, and upgrades. Here, things such as IP parameters, boot server parameters, network adapter configuration, bootlist order, and boot devices are set. For a CD-based installation, set the first boot device to your CD-ROM (Refer to Chapter 5, “Software management” on page 133).

- d. After all the configurations are completed, exit from the System Management Services screen. The server starts from the CD, and the OS installation begins.

There are three ways in which to install AIX 5L on your system:

- ▶ New and Complete Overwrite Installation
- ▶ Migration Installation
- ▶ Preservation Installation

Note: Preservation Installation is the default for a first-time installation because there are no file systems to preserve for a Migration installation.

Figure 3-3 shows the installation settings for the BOS installation.

```

                                Installation and Settings

Either type 0 and press Enter to install with current settings, or type the
number of the setting you want to change and press Enter.

  1 System Settings:
    Method of Installation.....Preservation
    Disk Where You Want to Install.....hdisk0

  2 Primary Language Environment Settings (AFTER Install):
    Cultural Convention.....English (United States)
    Language .....English (United States)
    Keyboard .....English (United States)
    Keyboard Type.....Default

  3 More Options (Desktop, Security, Kernel, Software, ...)

>>> 0 Install with the current settings listed above.

-----+-----
88 Help ? | WARNING: Base Operating System Installation will
99 Previous Menu | destroy or impair recovery of SOME data on the
                | destination disk hdisk0.
>>> Choice [0]: █
```

Figure 3-3 Installation settings for the BOS installation

3.3 New and complete overwrite installation

This method is generally used in the following situations:

- ▶ You have a new machine.
In this case, the hard disk or disks on which you are installing the BOS are empty, and this is the only possible installation method for a new machine.
- ▶ You want to install on a hard disk that already contains an existing root volume group that you want to overwrite.
This might, for example, occur if your root volume group is corrupted.
- ▶ You might want to reassign your root volume group to another disk, perhaps to a disk that is smaller.

Note: The new and complete overwrite installation overwrites all the data on the selected destination disk. This means that after the installation is complete, you must manually configure your system using the configuration assistant application, or smitty, or the command line.

3.4 Migration installation

Use the migration installation method to upgrade AIX 5L to a different version or release while preserving the existing root volume group. Following are some of the characteristics of migration installation:

- ▶ During a migration installation, the installation process determines the optional software products that must be installed on AIX 5L. Earlier versions of AIX 5L software that exist on the system are replaced by the new software in AIX 5L.
- ▶ This method preserves all the file systems (except /tmp), the root volume group, the logical volumes, and the system configuration files. In most cases, user configuration files from the earlier version of a product are saved.
- ▶ Nonsoftware products remain on the system.
- ▶ When migrating from AIX 5L V3.2, all the files in /usr/lib/drivers, /usr/lib/microcode, /usr/lib/methods, and /dev are removed from the system. Therefore, software support for non-IBM device drivers must be reinstalled.

3.5 Preservation installation

Use the preservation installation method when a version of BOS is installed on your system and you want to preserve user data in the root volume group. Following is a list of features pertaining to a preservation installation:

- ▶ The /etc/preserve.list file contains a list of system files to be copied and saved during a preservation BOS installation. The /etc/filesystems file is listed by default. Add the full path names of any additional files that you want to save during the preservation installation to the /etc/preserve.list file. Create the /etc/preserve.list file on an AIX 5L V3.1 machine. On an AIX 5L V4.1 or later system, this file already exists on your system, and can be directly edited.
- ▶ Ensure that you have sufficient disk space in the /tmp file system to store the files listed in the /etc/preserve.list file.
- ▶ This method overwrites the /usr, /tmp, /var, and /(root) file systems by default. Therefore, any user data in these directories is lost. These file systems are removed and recreated. Therefore, any other licensed program products (LPPs) or file sets that you installed on the system will also be lost. Think of a Preservation Installation as an overwrite installation for these file systems. System configuration must be performed after preservation installation is carried out.

3.6 Advanced installation options

The third option in the Installation and Settings menu (Figure 3-3 on page 53) allows you to modify more settings for system operations parameters. These are the three options that can be modified:

- ▶ Installation package set or desktop
- ▶ Enable trusted computing base
- ▶ Enable 64-bit kernel and JFS2

Installation package set or desktop

This allows you to configure the type of interface that the system uses at startup. The installation package set is the default and the only option when using an American Standard Code for Information Interchange (ASCII) console.

The desktop option is for graphical systems. You can select from the following options:

- ▶ Common Desktop Environment (CDE)
- ▶ K Desktop Environment (KDE)
- ▶ GNU Network Object Model Environment (GNOME)
- ▶ None

Note: If you select None, a minimal configuration is installed.

3.7 Other installation methods

The methods discussed so far pertained to the different ways in which to perform the BOS installation from CD or DVD. Solaris and AIX 5L both offer other ways to source the installation software.

In Solaris, you have the following additional choices:

- ▶ Custom JumpStart
- ▶ WebStart Flash
- ▶ Live Upgrade
- ▶ Factory JumpStart

In AIX 5L, you have the following options:

- ▶ Alternate Disk Installation
- ▶ Network Installation Management
- ▶ Install from System Backup
- ▶ Preinstallation option for a new system order

3.7.1 Alternate disk installation

Only AIX 5L V5.x has the ability to install a completely new OS on another disk or part of a disk when the production environment is up and running. The result is a significant reduction in downtime. It also allows large facilities to better manage an upgrade because systems can be installed over a longer period of time. While the systems are still running at the previous version, the switch to the newer version can happen at the same time. This concept is called *alternate disk installation*.

Benefits of alternate disk installation

If you already have an AIX 5L version installed, you can choose alternate disk installation to transition your site through the upgrade process more smoothly. Following are the benefits of alternate disk installation:

- ▶ It lets you install a new version of the OS when your current version is still running.
- ▶ You can retain the flexibility of reverting to the earlier version of AIX 5L if the new installation is not compatible with your existing applications or customizations.
- ▶ By using an alternate destination disk, you can install the new version to different machines over time, and later, when it is convenient, reboot to implement the new installations.
- ▶ You can test your applications against the new version on an alternate disk. With this option, you can stabilize your environment before implementing the installation on other machines.

The `mksysb` command creates a backup of the OS (the root volume group). You can use this backup to reinstall a system to its original state if gets corrupted. If you create the backup on tape, the tape is bootable and includes the installation programs required to install from the backup. This is an important and useful command.

System requirements

Table 3-2 shows the file sets that are required in order to run an alternate disk installation.

Table 3-2 System requirements

File set name	Description	Requisite® software
bos.alt_disk_install.rte	This file set ships the alt_disk_install command, which allows the cloning of the rootvg and the installation of an AIX 5L mksysb to an alternate disk.	bos.sysmgmt.sysbr
bos.alt_disk_install.boot_images	This file set ships the boot images required to install mksysb images to an alternate disk.	bos.alt_disk_install.rte

The bos.alt_disk_install package requires approximately 12 MB of disk space in /usr.

Although one additional disk is required, the system recommendation is that four disks should be used for alternate disk installation, two for the primary rootvg mirrored and two for the alt_disk_install implementation.

After you have installed these file sets, the alternate disk installation functions are available to you in the Software Installation and Maintenance menu. Use the following System Management Interface Tool (SMIT) fast path:

```
# smitty alt_install
```

Figure 3-4 shows the Alternate Disk Installation screen.

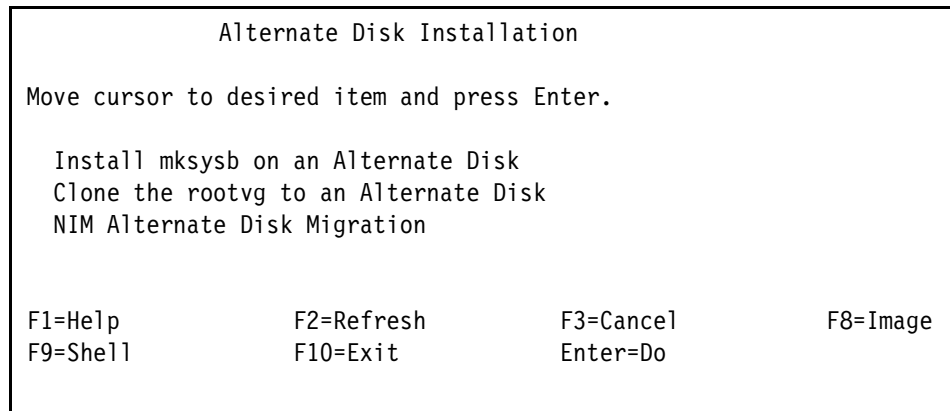


Figure 3-4 Alternate Disk Installation menu

Alternate disk installation can be used in one of following ways:

- ▶ Cloning the current running rootvg to an alternate disk
- ▶ Installing an mksysb image on another disk
- ▶ Upgrading the BOS to the current release

Cloning the current running rootvg to an alternate disk

Following are the advantages of cloning the rootvg to an alternate disk:

- ▶ Having an online backup available in case of a disaster
Keeping an online backup requires that an extra disk or disks be available on the system.
- ▶ Applying new maintenance levels or updates
A copy of the rootvg is made to an alternate disk, and then updates are applied to that copy. Finally, the boot list is updated to boot from the new device. The system runs uninterrupted during this time. When it is rebooted, the system boots from the newly updated rootvg for testing. If the updates cause problems, the old rootvg can be retrieved by resetting the boot list and rebooting.

Figure 3-5 shows how to use the alternate disk installation. With the primary rootvg currently running on hdisk0 and hdisk1, make a clone to the second set of drives, hdisk2 and hdisk3. Also upgrade the clone disks from AIX 5L V5.2 ML 2 to AIX 5L V5.2 ML 3. Figure 3-5 presumes the following facts:

- ▶ You are cloning to disks hdisk2 and hdisk3
- ▶ You are running an update_all operation installation of the software in /tmp/update. It is here that the new MLs are located.
- ▶ You are specifying that this operation must change the current boot list to hdisk2 and hdisk3 after completion.
- ▶ You are not asking the process to complete an immediate reboot on completion of the upgrade because this is something that you want to schedule in an appropriate maintenance window.

Perform the following tasks:

1. To start the clone procedure, use the following smit fast path:

```
# smitty alt_clone
```

Figure 3-5 shows the Clone the rootvg to an Alternate Disk screen.

```
Clone the rootvg to an Alternate Disk

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                     [Entry Fields]
* Target Disk(s) to install           [hdisk2 hdisk3]           +
Phase to execute                       all                       +
image.data file                         []
Exclude list                            []
Bundle to install                       [update_all]           +
  -OR-
Fileset(s) to install                   []
Fix bundle to install                   []
  -OR-
Fixes to install                        []
Directory or Device with images         [ /tmp/update ]
(required if filesets, bundles or fixes used)

installp Flags
COMMIT software updates?                yes                       +
SAVE replaced files?                     no                         +
AUTOMATICALLY install requisite software? yes                       +
EXTEND file systems if space needed?     yes                       +
OVERWRITE same or newer versions?       no                         +
VERIFY install and check file sizes?    no                         +

Customization script                     []
Set bootlist to boot from this disk
on next reboot?                          yes                       +
Reboot when complete?                    no                         +
Verbose output?                           no                         +
Debug output?                             no                         +

F1=Help      F2=Refresh      F3=Cancel    F4=List
F5=Reset     F6=Command    F7=Edit     F8=Image
F9=Shell     F10=Exit      Enter=Do
```

Figure 3-5 Cloning the rootvg

2. After completing the operation, verify the boot list with the following command:


```
bootlist -m normal -o
```
3. The boot list is set to hdisk2 hdisk3. Issuing an **lspv** command provides you with the output shown in Example 3-1.

Example 3-1 lspv output

```
# lspv
hdisk0      0001615fa41bf87a      rootvg
hdisk1      0001615fcbc1a83f      rootvg
hdisk2      0001615fcbc1a86b      altinst_rootvg
hdisk3      0001615fcbca5d16      altinst_rootvg
```

At this point, you have cloned and installed AIX 5L V5.2 ML 3. The changes are activated at the next reboot.

4. After the reboot, issue the **oslevel** command or complete the appropriate verifications to ensure that the upgrade is performed as expected. Issuing the **lspv** command provides you with the output shown in Example 3-2.

Example 3-2 lspv output

```
# lspv
hdisk0      0001615fa41bf87a      old_rootvg
hdisk1      0001615fcbc1a83f      old_rootvg
hdisk2      0001615fcbc1a86b      rootvg
hdisk3      0001615fcbca5d16      rootvg
```

You have booted AIX 5L V5.2 ML3 from hdisk2 and hdisk3, and the disks recognized as the new rootvg hdisks (0 and 1) now show a volume group of old_rootvg and are not active. The recommendation now is to leave disk 0 and disk 1 with AIX 5L V5.2 ML 2 in case you have to fall back on the old system.

5. To complete the process of cloning hdisk 2 and hdisk 3 back to hdisk 0 and 1, issue the following commands:
 - `alt_disk_install -W hdisk0 hdisk1`
This wakes up the old_rootvg.
 - `alt_disk_install -S`
This puts the old_rootvg back to sleep.

– `alt_disk_install -X altinst_rootvg`

This removes the `old_rootvg` volume group name associated with `hdisk0` and `hdisk1` from the Object Data Manager (ODM), and assigns them a value of “none”, which allows the cloning to recur perfectly.

– `smitty alt_clone`

This clones back to `hdisk0` and `hdisk1`.

Installing an mksysb image on another disk

An alternate mksysb install involves installing an mksysb image that is already created, from another system to an alternate disk of the target system. The mksysb image (AIX 5L V4.3 or later) is created on a system that either has the same hardware configuration as the target system, or has all the device and kernel support installed for a different machine type or platform or different devices.

1. To create the alternate mksysb system, use the following smit fast path:

```
# smitty alt_mksysb
```

2. In the alternate mksysb installation screen (Figure 3-6), enter the name of the disk on which you want to install the mksysb in the “Target Disk(s) to install”

field and the name of the device or the image name from which you will be restoring the mksysb in the “Device or image name” field. Press Enter.

```

                                Install mksysb on an Alternate Disk

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry
Fields]
* Target Disk(s) to install      []
+
* Device or image name          []
+
Phase to execute                 all
+
image.data file                  [] /
Customization script            [] /
Set bootlist to boot from this disk
on next reboot?                 yes
+
Reboot when complete?          no
+
Verbose output?                 no
+
Debug output?                   no
+
resolve.conf file               [] /

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit      Enter=Do
```

Figure 3-6 Installing mksysb

After the mksysb image is restored to the new disk, the system reboots from the new alternate rootvg. This completes your alternate mksysb installation.

3.7.2 Alternate disk migration installation

Alternate disk migration installation allows you to create a copy of rootvg to a free disk or disks, and simultaneously migrate it through Network Installation Management (NIM) to a new release level. Using alternate disk migration installation over a conventional migration provides the following advantages:

- ▶ Reduced downtime

The migration is performed when the system is up and running. There is no requirement to boot from install media, and the majority of processing occurs on the NIM master.
- ▶ Quick recovery in the event of migration failure

Because you are creating a copy of rootvg, all the changes are performed to the copy (altinst_rootvg). In the event of serious migration installation failure, the failed migration is cleaned up, and the administrator does not have to take further action. In the event of a problem with the new (migrated) level of AIX 5L, the system can be quickly returned to the premigration OS by booting from the original disk.
- ▶ High degree of flexibility and customization in the migration process

This is performed with the use of optional NIM customization resources, image_data, bosinst_data, exclude_files, premigration script, installp_bundle, and postmigration script.

Alternate disk migration installation has the following requirements:

- ▶ Configured NIM master running AIX 5L V5.3 or later with AIX 5L-recommended maintenance level 5300-04 or later.
- ▶ The NIM master must have bos.alt_disk_install.rte installed in its rootvg and the Shared Product Object Tree (SPOT) that will be used.
- ▶ The level of the NIM master rootvg, lpp_source, and SPOT must be at the same level.
- ▶ The client (the system to be migrated) must be at AIX 5L V4.3.3 or later.
- ▶ The client must have a disk or disks that are large enough to clone the rootvg and an additional 500 MB (approximately) of free space for the migration. The total amount of required space depends on the original system configuration and migration customization.
- ▶ The client must be a registered NIM client to the master.
- ▶ The NIM master must be able to execute remote commands on the client, using the rshd protocol.
- ▶ The client must have a minimum 128 MB of memory.

- ▶ A reliable network, which can facilitate large amounts of NFS traffic, must exist between the NIM master and the client.
- ▶ The client's hardware must support the level it is migrating to and meet all the other conventional migration requirements.

To create the alternate disk migration, use the following smit fast path:

```
# smitty nimadm_migrate
```

Figure 3-7 shows the NIM Alternate Disk Migration screen. For more information about the fields, go to `smitty nimadm_migrate` and press F1 or Esc+1.

```

Perform NIM Alternate Disk Migration

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                     [Entry Fields]
* Target NIM Client                                 +
* NIM LPP_SOURCE resource                           +
* NIM SPOT resource                                 +
* Target Disk(s) to install                         +
DISK CACHE volume group name                       +

NIM IMAGE_DATA resource                            +
NIM BOSINST_DATA resource                          +
NIM EXCLUDE_FILES resource                         +
NIM INSTALLP_BUNDLE resource                       +
NIM PRE-MIGRATION SCRIPT resource                  +
NIM POST-MIGRATION SCRIPT resource                  +

Phase to execute                          [all]          +
NFS mounting options                               +
Set Client bootlist to alternate disk?    yes            +
Reboot NIM Client when complete?         no             +
Verbose output?                           no             +
Debug output?                             no             +

ACCEPT new license agreements?           no             +
[BOTTOM]

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command          F7=Edit           F8=Image
F9=Shell         F10=Exit            Enter=Do

```

Figure 3-7 Alternate disk migration installation

3.8 Using the multibos utility

The *multibos* utility allows you, as root, to create multiple instances of AIX 5L on the same root volume group (rootvg).

The multibos setup operation creates a standby BOS that boots from a distinct Boot Logical Volume (BLV). This creates two bootable instances of BOS on a given rootvg. You can boot from either instance of a BOS by specifying the respective BLV as an argument to the **bootlist** command, or by using system firmware boot operations.

You can simultaneously maintain two bootable instances of a BOS. The instance of a BOS associated with the booted BLV is the active BOS. The instance of a BOS associated with the BLV that has not been booted is the standby BOS. Only two instances of BOS are supported per rootvg.

The multibos utility allows you to access, install, maintain, update, and customize the standby BOS either during setup or during any subsequent customization operations. Installing maintenance updates to the standby BOS does not change system files on the active BOS. This allows for concurrent update of the standby BOS, and the active BOS remains in production.

The multibos utility has the ability to copy or share logical volumes and file systems. By default, the multibos utility copies the BOS file systems (currently, the /, /usr, /var, /opt, and /home directories), the associated log devices, and the boot logical volume. You can make copies of additional BOS objects (see the **-L** flag). All the other file systems and logical volumes are shared between the instances of the BOS.

For more information, refer to the following Web site:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

3.9 Network Installation Manager

The NIM permits the installation, maintenance, and upgrade of AIX 5L, its basic OS, and additional software and fixes that might be applied over a period of time over token-ring, Ethernet, Fiber Distributed Data Interface (FDDI), and asynchronous transfer mode (ATM) networks. NIM also permits the customization of machines both during and after the installation. As a result, NIM has eliminated the reliance on tapes and CD-ROMs for software installation. The

bonus, in NIM's case, is in the network. NIM allows one machine to act as a master in the environment. This machine is responsible for storing information about the clients it supports, the resources that it or the other servers provide to these clients, and the networks on which they operate.

Following are some of the benefits of NIM:

- ▶ **Manageability**
It allows central localization of software installation images, thus making backup and administration easier.
- ▶ **Central administration**
Administrators can install remote AIX 5L machines without having to physically attend them.
- ▶ **Scalability**
You can install more than one machine at a time, implement a group strategy of machines and resources, and choose how many machines to install at a time.
- ▶ **Availability**
Where server down time means loss of profits, NIM provides you with a backup image of all your servers. A new server can be set up and running in just over an hour.
- ▶ **High availability of the NIM server**
AIX 5L V5.3 introduces a way to define a backup NIM master, take over to the backup master, and then fail back to the primary master. This helps to create more reliable NIM environments.
- ▶ **Nonprompted installation**
NIM provides a function to install systems without having to go to the machine.
- ▶ **Installations can be initiated by either the client or the master at a convenient time.**
If, for example, a client is unavailable at the time of the installation, you can initiate an installation when it is back online. Alternatively, if there is less traffic on your network at a certain time, you can have the installations occur at that time.
- ▶ **It is a relatively faster means of installation than tape or CD-ROM.**
NIM provides greater functionality than CD-ROM or tape. Among other things, it allows you to customize an installation, initiate a nonprompted installation, or install additional software.

3.9.1 Network Installation Management environments

A NIM environment is typical of any client/server environment. You have client machines accessing resources that are remotely held on servers. In the NIM environment, there is also the additional requirement that these resources bring stand-alone, dataless, and diskless machines to a running state. It is obvious then, that certain resources are required to support the operation of systems within the NIM environment. This capability is dependent on the functionality of the network.

All the information about the NIM environment is stored in three ODM databases (this data is located in the files in the `/etc/objrepos` directory):

- ▶ `nim_object`
Each object represents a physical entity in the NIM environment
- ▶ `nim_attr`
Stores individual characteristics of physical entities
- ▶ `nim_pdatr`
Contains predefined characteristics

The objects that comprise the ODM database are machines, networks, resources, and groups. Characteristics refer to their attributes that are a part of their initial definition. In this definition, objects are also assigned a name. This name is for NIM purposes only and might be completely different from any defining physical characteristic it may have. To have a functioning environment, the following conditions must be met:

- ▶ Network File System (NFS) and TCP/IP must be installed
- ▶ TCP/IP must be configured
- ▶ TCP/IP communications must be established between the machines
- ▶ Name resolution must be configured

3.9.2 Network Installation Management setup

Before you begin to set up a NIM server, a few important points must be considered. The NIM master must be running the highest version of AIX 5L that you are planning to install, for example, if your NIM master is running on AIX 5L V5.2, you can install AIX 5L V5.2, V5.1, and V4.3.3 on your client machines, but you cannot install AIX 5L V5.3 on any of the client machines until the NIM master is upgraded to AIX 5L V5.3. A quick startup guide for the NIM setup and BOS installation is provided here. For more information about NIM's latest features, refer to *NIM from A to Z in AIX 5L*, SG24-7296.

Network Installation Management Master

You must consider where and how to store the NIM resources. You might want to have separate file systems for each resource, create logical volumes for each resource, or even have your NIM resources on a separate volume group (refer to Chapter 4, “Disks and file systems” on page 91).

lpp_source

An `lpp_source` resource represents a directory in which software installation images are stored. If the `lpp_source` contains the minimum set of support images required to install a machine, it is given the `simages` attribute and can be used for BOS installation (`bos_inst`) operations.

NIM uses an `lpp_source` for an installation operation by first mounting the `lpp_source` on the client machine. The `installp` commands are then started on the client using the mounted `lpp_source` as the source for installation images. When the installation operation has completed, NIM automatically unmounts the resource.

In addition to providing images to install machines, `lpp_source` resources can also be used to create and update SPOT resources.

Shared Product Object Tree

SPOT is a fundamental resource in the NIM environment. It is required to install or initialize all machine configuration types. A SPOT provides an `/usr` file system for diskless and dataless clients, and network boot support for all the clients.

Everything that a machine requires in an `/usr` file system, such as the AIX 5L kernel, executable commands, libraries, and applications, are included in the SPOT. Machine-unique information or user data is usually stored on the other file systems. The SPOT can be located on any stand-alone machine within the NIM environment, including the master. The SPOT is created, controlled, and maintained from the master, even though it can be located on another system.

One way of configuring the NIM master is by using `eznim`. The `smitty eznim` menu helps the system administrator by organizing the commonly used NIM operations and simplifies frequently used advanced NIM operations.

Perform these tasks to set up NIM:

- ▶ Prepare the AIX 5L OS and install the CD-ROMs that are at the same levels as the ones that are currently installed.
- ▶ Configure the NIM master server. Execute the `smitty setup_eznm_master` fast path.

Figure 3-8 shows Easy NIM server configuration. You can select the software source to configure from, the volume group to use for the NIM resources, and the file system to use for the NIM resources. When the NIM master environment is configured, the basic NIM resources are created, for example, lpp_source and SPOT.

```

Easy NIM - Setup the NIM Master environment

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]
Select or specify software source          [cd0]
+
to initialize environment

Select Volume Group for resources         [rootvg]
+

Select Filesystem for resources           [/export/eznim]

Options
CREATE system backup image?              [yes]
+
CREATE new Filesystem?                   [yes]
+
DISPLAY verbose output?                  [no]
+

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit       Enter=Do

```

Figure 3-8 Easy NIM server configuration

To view the NIM resources created by **eznim**, select **Show the NIM environment** or run the **lsnim** command on the NIM Master.

Network Installation Management client

eznim also allows you to manage an NIM client. On a client system, use the **smitty setup_eznim_client** fast path (but only if your NIM client system is already installed). If not, you can install it from the CD by using the following command:

```
installp -aXgd /dev/cd0 bos.sysmgt.nim.client
```

If you have a new machine, it is necessary to configure the boot by network using the NIM Master. Figure 3-9 shows Easy NIM Client Configuration.

Select the host name of the NIM client, the primary network interface, and the host name of the NIM master. To determine the hardware platform, type the following command:

```
lscfg | grep Arch
```

The kernel to use for network boot is “up” (uniprocessor) for a single CPU system or “mp” (multiprocessor) for an SMP system.

Easy NIM - Client Configuration

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]	[Entry
* Machine Name	[]
* Primary Network Install Interface	[]
+	
* Host Name of Network Install Master	[]
Hardware Platform Type	chrp
Kernel to use for Network Boot	[mp]
+	

F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 3-9 Easy NIM client configuration

3.9.3 Installing Network Installation Management from a command line

If you prefer to use a command line instead of smitty to set up your NIM master, the necessary commands are provided here. This gives you greater flexibility in configuring your NIM master and allocating NIM resources across the system. Perform the following tasks:

1. Create your file systems and logical volumes for hosting the NIM resources, as shown in Example 3-3.

Example 3-3 Creating file systems for NIM install

```
crfs -v jfs -g nimvg -a size=$((2000*500)) -m /export/nim/lpp_source -A  
yes -p rw -t no -a frag=4096 -a compress=no  
crfs -v jfs -g nimvg -a size=$((2000*300)) -m /export/spot -A yes -p rw  
-t no -a frag=4096 -a compress=no
```

2. Check whether the NIM server file set is installed on your system:

```
ls/lpp -l | grep bos.sysmgt.nim
```

If it is not found, insert CD1 of the AIX 5L OS installation pack and type the following:

```
installp -aXgd /dev/cd0 bos.sysmgt.nim
```

3. Define the network for NIM:

```
nimconfig -a netname=domain -a pif_name=en0 -a platform=chrp \  
-a cable_type1='N/A'
```

4. Define lpp_source and SPOT (Example 3-4). Here, the resource names are the same as the directories that contain them.

Example 3-4 Defining lpp_source and SPOT for NIM install

```
nim -o define -t lpp_source =a source=/dev/cd0 -a server=master \  
-a location='/export/nim/lpp_source/aix530_cd_lpp' aix530_cd_lpp  
nim -o define -t spot=a source=aix530_cd_lpp -a server=master \  
-a location='/export/nim/spot/aix530_cd_spot' aix530_cd_spot
```

5. To allow the NIM master to successfully perform a network boot of its clients, you require two services to run BOOTP and TFTP. Put the following commands into the /etc/inetd.conf file on your NIM master if they do not already exist:

```
tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd  
bootps dgram udp wait root /usr/sbin/bootpd bootpd /etc/bootptab
```

6. Make inetd reread by running the following:

```
refresh -s inetd
```

7. (Optional) It is a good idea to set up Transmission Control Protocol (TCP) wrapper to increase security.

8. Set up your NIM client. Check whether the NIM client file set is installed on your client machine:

```
ls1pp -l | grep bos.sysmgmt.nim.client
```

If it is not found, insert CD1 of the OS installation pack into your CD-ROM and type the following:

```
installp -aXgd /dev/cd0 bos.sysmgmt.nim.client
```

9. The client must have remote shell running in order to allow the NIM operations to be performed. Add the following to the /etc/inetd.conf file of the client machine:

```
shell stream tcp6 nowait root /usr/sbin/rshd rsh
```

10. Make inetd reread by running the following:

```
refresh -s inetd
```

11. Now add the NIM master's root account name into the \$HOME/.rhosts file as follows (a short and fully qualified name is recommended):

```
masterhostname root  
masterhostname.domain.com root
```

12. You are now ready to define your first client machine. You can perform this action from the master, as shown in Example 3-5.

Example 3-5 Defining the first client for NIM

```
nim -o define -t standalone -a platform='chrp' -a netboot_kernel='up'  
-a if1='find_net hostname MACaddress' -a net_definition='ent netmask  
clientgateway servergateway' clientresourcename
```

13. To find the client's MAC address, use the following:

```
lscfg -vl ent0
```

In this case, the NIM Master is austin.ibm.com on gateway 9.1.200.1, the client is dublin.ibm.com with two CPUs and chrp architecture with Ethernet adapter MAC address 007123456JO, and will be on gateway 9.1.100.1 (Example 3-6).

Example 3-6 Example NIM client definition

```
nim -o define -t standalone -a platform='chrp' -a netboot_kernel='mp'
-a if1='find_net dublin 007123456JO' -a net_definition='ent
255.255.255.0 9.1.100.1 9.1.200.1' dublin
```

The same task can be performed from the client machine by using the **niminit** command:

```
niminit -a name='dublin' -a master=austin -a pif_name='en0' -a
cable_type1='N/A' -a platform='chrp' -a netboot_kernel='mp'
```

3.9.4 Installing the Base Operating System on a Network Installation Management client

In this method, using installation images to install BOS on a NIM client is similar to the traditional BOS installation from a tape or CD-ROM device, because the BOS image is installed from the installation images in the lpp_source resource.

Following are the prerequisites:

- ▶ The NIM Master must be configured, and the lpp_source and SPOT resources must be defined.
- ▶ The NIM client to be installed must already exist in the NIM environment. If your system does not exist in an NIM environment, it is necessary to configure the boot by network by using the NIM master.

Perform the following tasks to install the BOS on a NIM client:

1. Use the **smitty nim_bosinst** fast path from the NIM master.
2. Select the TARGET for the operation.
3. Select **rte** as the installation TYPE.
4. Select the SPOT to use for the installation.
5. Select the LPP_SOURCE to use for the installation.
6. In the displayed dialog fields, supply the correct values for the installation options or accept the default values. Use the Help information and the LIST option to help you.

7. If the client machine being installed is not already running a configured NIM client, NIM will not automatically reboot the machine over the network for installation. If the client is not rebooted automatically from SMIT, initiate a network boot from the client to install it.
8. After the machine boots over the network, the display on the client machine begins prompting for information about how the machine must be configured during installation. Specify the requested information to continue with the installation.

A command line can also be used for this procedure. For more information, refer to the operating system manual for NIM.

BOS installations can be initiated by the server (push installation) or by the client (pull installation).

3.9.5 Booting a machine over the network

When using NIM, one of the most common problems pertains to booting over the network. If your machine has problems getting a boot record, use the following checklist to determine the cause of your problem:

- ▶ The client's SMS menu already has IP addresses, netmask, and/or gateways defined that do not match the current environment. You can test the connection between the client and the master using the ping function as part of the SMS menu. For this test, put in entries for IP addresses. However, after successful testing, it is best to set all the fields to "0" (zero) again. This way, the values stored on the NIM master are used.
- ▶ The adapter speed is a critical parameter. If you have the adapter speed set to auto on your NIM client and master, you might need to change it. If possible, set your adapter speed to the desired level on both the machines. In our case, we used an I/O server, which meant using virtual Ethernet adapters, and so, auto was the only option available for the client adapter speed. However, it worked perfectly well, performing a network boot install of AIX 5L V5.3.
- ▶ Check the microcode level of your machine and your adapters. An old microcode level is often the cause for network problems between the NIM master and client. You might not even notice it during normal business on your AIX 5L machine, but the network boot requires successful initializing of the network card.

For more information about configuring your client to boot over the network, refer to 3.9.2, "Network Installation Management setup" on page 69.

3.10 AIX 5L installation in a partitioned environment

The AIX 5L Installation in a Partitioned Environment guide is found in the IBM pSeries and AIX 5L Information Center at:

<http://publib16.boulder.ibm.com/pseries/index.htm>

This guide provides system administrators with complete information about how to perform tasks such as installing, maintaining, and updating AIX 5L in a partition using CD-ROM, tape, and network installation. It also covers such topics as system backup, dump management, storage management, and remote management. This publication is available with the documentation CD that is shipped with the OS. The above Information Center reference applies to AIX 5L V5.3 and to all subsequent releases of this product until otherwise stated in the new editions.

The guide is available also available on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

3.10.1 Installing AIX 5L in a partitioned environment

For instructions about how to create a partition and allocate I/O resources to a partition, refer to *Hardware Management Console Installation and Operations Guide* (SA38-0590). To help you keep track of the LPAR environment system resources, refer to the tracking worksheets in the guide.

3.10.2 Configuring an initial partition as a NIM master

In this procedure, you set up an initial logical partition as a NIM master and server. This is particularly useful for the latest System p virtualization capabilities, for example, with a system capable of 256 logical partitions. The procedure described here refers to this initial logical partition as the *Master_LPAR*. It is assumed that AIX 5L is already installed and configured for network communication in the Master_LPAR.

The procedure is as follows:

1. Ensure that your network environment is already defined and working correctly before configuring the NIM environment.
2. After you verify that the correct level of AIX 5L OS has been installed on the Master_LPAR as the root user, set up the NIM environment using the `nim_master_setup` script. This script automatically installs the `bos.sysmgt.nim.master` file set, configures the NIM master, and creates the required resources for installation, including a `mksysb` system backup.

Note: The `nim_master_setup` script uses the `rootvg` volume group and creates an `/export/nim` file system by default. You can change these defaults using the `volume_group` and `file_system` options. The `nim_master_setup` script also allows you to optionally *not* create a generic system backup if you plan to use a `mksysb` image from another system.

3. Use the `nim_clients_setup` script to define your NIM clients, allocate the installation resources, and initiate a NIM BOS installation on the clients.
4. Then, using the HMC, activate the client partitions and configure them to boot off the network.

Prerequisites

Before beginning this procedure, ensure that you have already performed the following tasks:

- ▶ Use the HMC to create the `Master_LPAR` logical partition and partition profile. Ensure that the `Master_LPAR` partition has a network adapter, enough hard disk space for the NIM resources, and an assigned CD device. Set the boot mode for the `Master_LPAR` partition as Normal. After you successfully create the partition and the partition profile, leave the partition in the Ready state. Do not activate the partition yet.
- ▶ Use the HMC to create logical partitions and partition profiles for each NIM client. Be sure that each LPAR has a network adapter assigned. Set the boot mode for each partition as SMS. After you successfully create the partitions and the partition profiles, leave the partitions in the Ready state. Do not activate the partitions yet.
- ▶ Configure AIX 5L for network communication on the `Master_LPAR`. If AIX 5L is not currently installed on any of the disks in the system, refer to the CD-ROM device to install a partition with an HMC to obtain the details about the procedure.

To configure an initial partition as a NIM Master, perform the following tasks:

1. Activate the `Master_LPAR` (perform this step in the HMC interface). After you successfully create the `Master_LPAR`, it is in the Ready state. Use the HMC to activate the `Master_LPAR` partition. To activate the `Master_LPAR`, perform the following tasks:
 - a. Select the **Master_LPAR** partition.
 - b. Right-click the partition to open the menu, and select **Activate**.

- c. The Activate Partition menu opens with a selection of partition profiles. Check whether the correct partition profile is highlighted. Select **Open terminal** at the bottom of the menu to open a virtual terminal (vterm) window, and click **OK**.
 - d. A vterm window opens for the partition. After several seconds, the login prompt displays in the vterm window.
2. Configure NIM master and Initiate Installation of Partitions (perform these steps in the AIX 5L environment)

- a. Run the **oslevel** command as follows:

```
# oslevel -r
```

The output is similar to:

```
5300-04
```

The **oslevel** command reports the maintenance level of the OS, using a subset of all the file sets installed on your system.

- b. Verify the network configuration by running the following command:

```
# smitty mktcpip
```

- i. Select the Network Interface and press Enter.
- ii. Confirm or enter your host name, IP address, name server, domain name, default gateway, and the ring speed or cable type. Press Enter.
- iii. You can also test the network status by using the following **netstat** command options:

```
# netstat -C
```

The -C flag shows the routing table information.

- iv. Check to make sure your gateway information is correct:

```
# netstat -D
```

The -D flag shows the number of packets received, transmitted, and dropped in the communications subsystem.

- v. Check to make sure the network device is sending and receiving packet information.

- c. Insert the AIX 5L for POWER V5.3 Volume 1 in the CD device. Run the **nim_master_setup** command:

```
# nim_master_setup
```

This command configures the NIM environment on the AIX 5L system by installing the **bos.sysmgmt.nim.master** file set, configuring the NIM environment, and creating the **boot**, **nim_script**, **resolv_conf**, **bosinst_data**, **LPP_Source**, and **SPOT** resources. If you plan to use a **mksysb** image

from another system, the -B flag is used to prevent the creation of the mksysb resource. The nim_master_setup script uses the /dev/cd0 device as the default device. You can specify an alternate location using the -a device=full_path_name option.

The nim_master_setup script uses the rootvg volume group and creates an /export/nim file system by default. You can change these defaults by using the volume_group and the file_system options.

Note: The output from the nim_master_setup script is stored in the /var/adm/ras/nim.setup log file.

- d. If you are adding new client machines that cannot be resolved on the name server, edit the /etc/hosts file to add the IP addresses and the client host names.
- e. There are two ways to define the client systems and initiate the BOS installation.

The first method uses the SMIT interface to define the clients, and then uses the nim_clients_setup script to initiate the installation.

The second method allows you to manually edit the client.defs file, use the nim_clients_setup script to define the clients with this file, and then initiate the installation. This section describes both the methods:

Use SMIT and the nim_clients_setup script, as follows:

- i. Run the **smitty nim_mkclient** fast path (Figure 3-10) and the nim_clients_setup script to define the client partitions in the NIM environment.

```
# smitty nim_mkclient
```

- ii. Select **Add a NIM Client**.
- iii. Enter a host name and press Enter.

- iv. If the menu prompts you for the Type of Network Attached to Primary Network Install Interface, select the network adapter from the list and press Enter.

```
Define a Machine

Type or select a value for the entry field.
Press Enter AFTER making all desired changes.

* Host Name of Machine [Entry Fields]
  (Primary Network Install Interface)

F1=Help      F2=Refresh   F3=Cancel    F4=List
F5=Reset     F6=Command   F7=Edit      F8=Image
F9=Shell     F10=Exit     Enter=Do
```

Figure 3-10 smitty nim_mkclient

- v. In the Define a Machine screen (Figure 3-11), provide the necessary information by typing them into the entry fields or by using the F4 key to open a selection menu. Verify that all the information is correct, especially the Hardware Platform Type (chrp), Kernel to Use for Network Boot (mp), and Network Type. Press Enter when you are finished.

```

Define a Machine

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
* NIM Machine Name                    [lpar1]
* Machine Type                          [standalone]          +
* Hardware Platform Type                 [chrp]                 +
Kernel to use for Network Boot           [mp]                   +
Communication Protocol used by client    []                      +
Primary Network Install Interface
* Cable Type                             bnc                    +
  Network Speed Setting                   []                      +
  Network Duplex Setting                  []                      +
* NIM Network                             [ent-Network1]
* Network Type                             ent
* Ethernet Type                           Standard                +
* Subnetmask                               []

[MORE...9]

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command      F7=Edit       F8=Image
F9=Shell     F10=Exit         Enter=Do

```

Figure 3-11 Using smitty nim_mkclient to define a machine

- vi. Repeat for each client partition. Use the F3 key to return to the previous menu, and change the information for each client.

Run the `nim_clients_setup` script as follows:

```
# nim_clients_setup
```

The `nim_clients_setup` command creates a NIM machine group with the clients you just defined using the SMIT interface and then allocates the `LPP_Source`, `SPOT`, `mksysb`, `bosinst.data`, and `resolv.conf` resources, and finally, initiates a NIM `mksysb` installation. The NIM `mksysb` installation uses the `generic_sysb` resource that was created with the `nim_master_setup` script. If you want to use another `mksysb` image, use the `-m mksysb_path` option, and the script defines and uses it to install the partitions. The path must be local to the master.

Use a text editor to manually edit the `client.defs` file and use the `nim_clients_setup` script:

Use the vi editor to customize the /export/nim/client.defs file as follows:

```
# vi /export/nim/client.defs
```

Edit the client.defs file according to your environment. For more information, see the instructions and examples in the client.defs file. After you edit the client.defs file, save it and exit the vi editor.

Run the nim_clients_setup script to define the client partitions in the NIM environment as follows:

```
# nim_clients_setup -c
```

The -c option specifies using the client.defs file for your client definitions. The **nim_clients_setup** command creates a NIM machine group with all the resources created from the nim_master_setup script and initiates a NIM mkysyb installation. If you want to use another mkysyb image, use the -m mkysyb_path option, and the script defines and uses it to install the partitions. The path must be local to the master.

3. Activate and install the partitions (perform these steps in the HMC interface). To activate the partitions, perform the following tasks:
 - a. Select the partition or partition profile that you want to activate.
 - b. Right-click the partition or partition profile to open the menu. Select **Activate**.
 - c. The Activate Partition menu opens with a selection of partition profiles. Select a partition profile that is set to boot to the SMS menu. Select **Open terminal** at the bottom of the menu to open a virtual terminal (vterm) window, and click **OK**.
 - d. A vterm window opens for each partition. After several seconds, the SMS menu opens in the vterm window. In the SMS menu on the vterm window (Figure 3-12), perform the following tasks:
 - i. Press 5 to select 5 Bootoptions.
 - ii. Press 1 to select Install/B.oot Device..Press Esc to get to the Select Boot Device Order.

- iii. Select the network adapter as the first choice for boot device from the list of available boot devices.
- iv. Press Esc to set the remote initial program load setup.

```
Version SF22Q_051
SMS 1.5 (c) Copyright IBM Corp. 2000,2003 All rights reserved.
-----
Select Device Type
1. Diskette
2. Tape
3. CD/DVD
4. IDE
5. Hard Drive
6. Network
7. List all Devices

-----

Navigation keys:
M = return to Main Menu
ESC key = return to previous screen      X = eXit System Management Services
-----
Type the number of the menu item and press Enter or select Navigation Key: █
```

Figure 3-12 SMS menu: Selecting the install/boot device

- e. In the Set Remote Initial Program Load Setup screen (Figure 3-13):
 - i. Press 1 for IP parameters. Type the appropriate information for the Client IP address, Server IP address, Gateway IP address, and Subnet Mask.

- ii. Press 2 to set the adapter configuration. (If you are using a virtual Ethernet adapter, auto is the default setting.)

```
Version SF220_051
SMS 1.5 (c) Copyright IBM Corp. 2000,2003 All rights reserved.
-----
Network Parameters
Interpartition Logical LAN: U9113.550.104790E-V7-C2-T1
  1. IP Parameters
  2. Adapter Configuration
  3. Ping Test
-----
Navigation keys:
M = return to Main Menu
ESC key = return to previous screen      X = eXit System Management Services
-----
Type the number of the menu item and press Enter or select Navigation Key: █
```

Figure 3-13 SMS menu: Setting the IP parameters for remote IPL

4. After all the configurations are performed, check if they are correct by performing the ping test. If the ping is successful, proceed with the network boot.

3.10.3 Installing AIX 5L using a CD-ROM device

This section describes the procedure involved in installing the AIX 5L OS. For more information about the concepts and the considerations involved when performing a base OS installation of AIX 5L, or concepts and requirements involved when using the NIM to install and maintain AIX 5L, refer to the AIX 5L Installation Guide and Reference.

Note: For the installation method that you choose, ensure that you follow the sequence of steps described here. Within each procedure, use AIX 5L to complete some installation tasks, and the HMC interface for the other steps.

Under this procedure, perform a New and Complete BOS Installation on a logical partition using the partition's CD-ROM device. This procedure assumes that there is an HMC attached to the managed system.

Prerequisites

Before you begin this procedure, you must use the HMC to create a partition and partition profile for the client. Assign the SCSI bus controller attached to the CD-ROM device, a network adapter, and enough disk space for the AIX 5L OS to the partition. Set the boot mode for this partition as SMS. After you have successfully created the partition and the partition profile, leave the partition in Ready state.

For instructions about how to create a logical partition and partition profile, refer to the “Creating logical partitions and partition profiles” topic in the IBM eServer Hardware Information Center, which is available on the Web at:

<http://www-1.ibm.com/support/docview.wss?uid=pub1sk3t815905>

Activating and installing the partition

The following tasks must be performed in the HMC interface:

1. Activate the partition as follows:
 - a. Insert the AIX 5L Volume 1 CD into the CD device of the managed system.
 - b. Right-click the partition to open the menu and select **Activate**.
 - c. The Activate Partition menu opens with a selection of partition profiles. Ensure that the correct profile is highlighted. Select **Open a terminal window** or **console session** at the bottom of the menu to open a virtual terminal (vterm) window.
 - d. Select **Advanced** to open the Advanced options menu.
 - e. For the Boot mode, select **SMS**.
 - f. Click **OK** to close the Advanced options menu.
 - g. Click **OK** again. A vterm window opens for the partition.
2. In the SMS menu on the vterm, perform the following tasks:
 - a. Press 5 and press Enter to select 5 (Boot Options).
 - b. Press 1 and press Enter to select 1 (Install/Boot devices).
 - c. Select **CD/DVD** as the first boot device and **Hard drive** as the second boot device.
 - d. If you have more than one hard disk in your partition, determine which hard disk you will use to perform the AIX 5L installation. Select the media type that corresponds to that hard disk and press Enter.
 - e. Select the device number that corresponds to the hard disk and press Enter.
 - f. Press the X key to exit the SMS menu. Confirm that you want to exit SMS.

3. Boot from the AIX 5L Volume 1 as follows:
 - a. Select **Console** and press Enter.
 - b. Select the language for the BOS Installation menu, and press Enter to open the Welcome to Base Operating System Installation and Maintenance menu.
 - c. Type 2 to select **Change/Show Installation Settings** and **Install in the Choice field** and press Enter.
4. Verify or change the BOS installation settings as follows:
 - a. Type 1 in the Choice field to select the System Settings option.
 - b. Type 1 for a New and Complete Overwrite in the Choice field and press Enter.

Note: The installation methods available depend on whether your disk has an earlier version of AIX 5L installed.

- c. When the Change Disks screen displays, change the destination disk for the installation. If the default that is shown is correct, type 0 in the Choice field and press Enter. To change the destination disk, perform the following tasks:
 - i. Type the number for each disk you choose in the Choice field and press Enter. Do not press Enter a final time until you have finished selecting all the disks. If you must deselect a disk, type its number a second time and press Enter.
 - ii. After you have finished selecting the disks, type 0 in the Choice field and press Enter. The Installation and Settings screen displays, with the selected disks listed under System Settings.
 - d. If required, change the primary language environment. Perform the following tasks to change the primary language used by this installation and to select the language and cultural convention you want to use:
 - i. Type 2 in the Choice field on the Installation and Settings screen to select the **Primary Language Environment® Settings** option.
 - ii. Select the appropriate set of cultural convention, language, and keyboard options. Most of the options are a predefined combination. However, you can define your own combination of options.

Note: Changes to the primary language environment do not take effect until after the BOS installation is complete and your system is rebooted.

- e. After you have made all your selections, verify that the selections are correct. Press Enter to confirm your selections and to begin the BOS installation. The system automatically reboots after the installation is complete.
5. Switch the partition to Normal mode by performing the following tasks:
 - a. Right-click the partition profile to open the menu. Check whether the correct partition profile is highlighted.
 - b. Select **Properties**.
 - c. Select the **Settings** tab.
 - d. For the Boot mode, select **Normal**.
 - e. Select **OK** to close the Properties menu.
 - f. Right-click the partition to open the menu.
 - g. Select **Restart Partition**.
 - h. Select **Immediate** for the Restart Options.
 - i. When the partition has restarted, right-click the partition to open the menu.
 - j. Select **Open terminal window** to open a vterm window.
 6. Complete the BOS installation by performing the following tasks:
 - a. Type vt100 as the terminal type.
 - b. In the License Agreement menu, select **Accept License Agreements**.
 - c. Click **Yes** to accept the installed license agreements.
 - d. Press F10 (or Esc+0) to exit the License Agreement menu.
 - e. In the Installation Assistant main menu, select **Set Date and Time**. Set the correct date, time, and time zone. Press F3 (or Esc+3) to return to the Installation Assistant main menu.
 - f. Select **Set root Password**, and set a root password for the partition. Select **Configure Network Communications**. Select **TCP/IP Startup**. Select an option from the Available Network Interfaces and press Enter.
 - g. Enter the appropriate network information in the Minimum Configuration and Startup menu and press Enter. Use F3 (or Esc+3) to return to the Installation Assistant main menu.
 - h. Exit the Installation Assistant by pressing F10 (or Esc+0).
 - i. The vterm window displays a login prompt.

3.11 Installing AIX 5L on IBM BladeCenter

A useful and quick setup guide for the IBM BladeCenter JS20 is available on the DeveloperWorks Web site at:

<http://www-128.ibm.com/developerworks/linux/library/l-pow-js20quickstart>

For more detailed information about AIX 5L V5.3 installation and setup with virtual I/O Server on IBM BladeCenter JS21, refer to *IBM BladeCenter JS21: The POWER of Blade Innovation*, SG24-7273.



Disks and file systems

This chapter discusses the following topics:

- ▶ 4.1, “Disk administration” on page 92
- ▶ 4.4, “Storage area network administration” on page 94
- ▶ 4.5, “Logical Volume Manager administration on AIX 5L” on page 96
- ▶ 4.9, “File system types and management” on page 109
- ▶ 4.10, “Migration from physical disks partition to AIX 5L” on page 127
- ▶ 4.11, “Migration from Solaris Volume Manager to AIX 5L” on page 128
- ▶ 4.12, “Migration from Veritas Volume Manager” on page 130

4.1 Disk administration

In Solaris, slices and partitions are used interchangeably to mean the same thing. In AIX 5L, the concepts are totally different because the disks are under a Logical Volume Manager (LVM), which is responsible for reserving the necessary disk areas. For more information about LVM on AIX 5L, refer to 4.5, “Logical Volume Manager administration on AIX 5L” on page 96.

4.2 Disk recognition

In Solaris 9, disk recognition depends on hardware, drivers, and the available infrastructure. In general, the disks that are managed by Sun drivers, which are called QLC drivers, can be managed online without file modifications or reboots. In this case, the commands used to perform this task are **cfgadm** and **devfsadm**.

For other vendor-acquired drivers, it is common to change some files on the `/kernel/drv` directory, such as the `sd.conf` file and the vendor file, and reboot the system with the reconfigure option after the modification.

On AIX 5L, disk recognition is always online without reboots. The command for a new device recognition is **cfgmgr**. The **cfgmgr** command configures the devices and optionally installs device software into the system. It is a good practice to use option `-v` for verbose during any **cfgmgr** execution.

Table 4-1 shows a comparison of disk management in Solaris and AIX 5L.

Table 4-1 Disk management

Task	Solaris	AIX 5L
Disk identification	echo format	lsdev -Cc disk
Vendor information	format / inquire	lscfg -vl
Disk analysis	format / analyse	diag

Example 4-1 shows a disk recognition in the AIX 5L environment after the **cfgmgr** command is run.

Example 4-1 Disk recognition after using the cfgmgr command

```
# lsdev -Cc disk
hdisk0 Available Virtual SCSI Disk Drive
# cfgmgr
# lsdev -Cc disk
hdisk0 Available Virtual SCSI Disk Drive
hdisk1 Available Virtual SCSI Disk Drive
```

Example 4-2 shows the lsdev output on the same system.

Example 4-2 lsdev output

```
#lsdev -Cc disk
hdisk0 Available 3b-08-00-8,0 16 Bit LVD SCSI Disk Drive
hdisk1 Available 3b-08-00-10,0 16 Bit LVD SCSI Disk Drive
#
```

4.3 Multipath I/O

Some of the differences between the multipath I/O options are described here.

Solaris

In Solaris 9, it is common to use the disk multipath solution under Veritas Dynamic Multi-Pathing (DMP) or the Solaris Traffic Manager to provide failover services, without load balance. For total solutions on disk multipath, it is common to use third-party tools such as EMC PowerPath.

Thus, the multipath solution is related to hardware infrastructure and the software acquired from vendors.

AIX 5L

There is a complete solution in the AIX 5L OS called Multipath I/O (MPIO), which has been available since AIX 5L V5.2. MPIO is an enhancement to the base OS environment that provides support for multipath fibre channel storage subsystems and AIX 5L servers configured with multiple fibre channel host bus adapter (HBA) on a storage area network (SAN). MPIO automatically discovers, configures, and makes available every storage device path. The storage device paths are managed by MPIO to provide high availability and load balancing of storage I/O.

For more information, refer to the MPIO sections of the System p and AIX 5L Information Center, which is available on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?>

4.4 Storage area network administration

On operating systems in general, the function that is performed before SAN management is setting up a SAN device called HBA for devices recognition. Usually the devices on SAN are disks or tapes.

On Solaris servers, there are many third-party adapters with different kinds of products for configuration.

On AIX 5L, the administration is centralized on HBA settings.

Use the smit fast path, `smit fcsdd`, for menu administration, as shown in Figure 4-1.

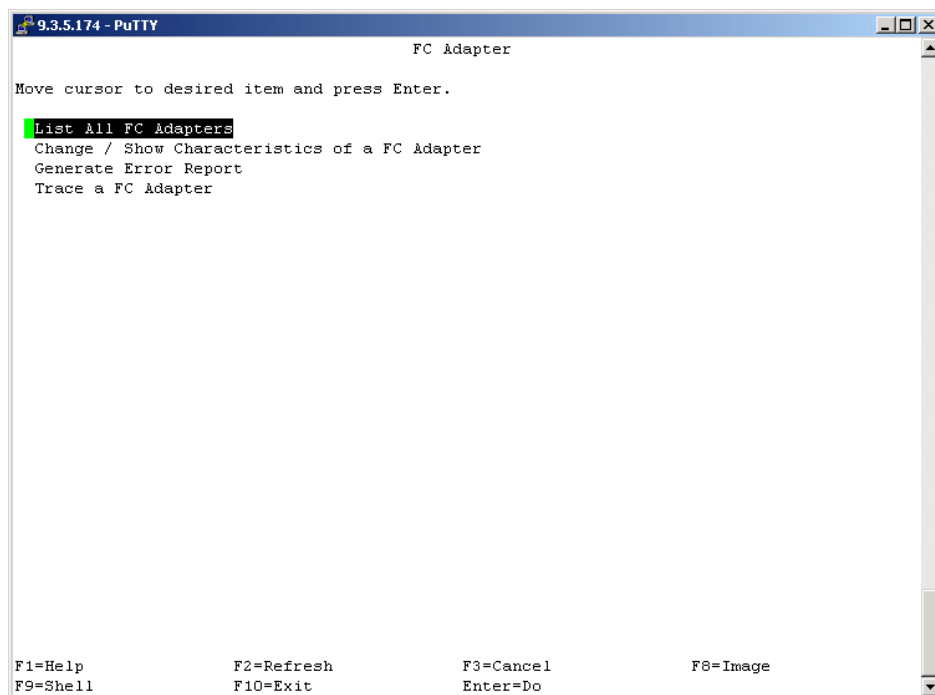


Figure 4-1 SAN management with smit

Alternately, you can use the commands shown in Table 4-2.

Table 4-2 AIX 5L SAN management using command line

Command	Task
<code>lsparent -C -k iocb;lsparent -C -k qiocb</code>	List fibre channel adapters
<code>lsparent -C -k fcp</code>	List fibre channel Small Computer System Interface (SCSI) protocol adapters
<code>chdev</code>	Change adapter characteristics
<code>lsattr -El adapter name</code>	List adapter attributes

4.4.1 SAN command-line examples on AIX 5L

This section provides SAN command-line examples on AIX 5L.

Example 4-3 shows the command for listing fibre channel (FC) adapters.

Example 4-3 Listing FC adapters

```
mail_1:/#lsparent -C -k iocb;lsparent -C -k qiocb
fcs0 Available 2V-08 FC Adapter
fcs3 Available 2Y-08 FC Adapter
fcs1 Available 2k-08 FC Adapter
fcs2 Available 31-08 FC Adapter
```

Example 4-4 shows the command for listing FC SCSI protocol adapters.

Example 4-4 Listing FC SCSI protocol adapters

```
mail_1:/#lsparent -C -k fcp
fscsi0 Available 2V-08-01 FC SCSI I/O Controller Protocol Device
fscsi3 Available 2Y-08-01 FC SCSI I/O Controller Protocol Device
fscsi1 Available 2k-08-01 FC SCSI I/O Controller Protocol Device
fscsi2 Available 31-08-01 FC SCSI I/O Controller Protocol Device
```

Example 4-5 shows the commands for listing adapter attributes.

Example 4-5 Listing adapter attributes

```
mail_1:/#lsattr -El fcs0
bus_intr_lvl 35          Bus interrupt level
False
```

bus_io_addr	0x1000	Bus I/O address
False		
bus_mem_addr	0xe0040000	Bus memory address
False		
init_link	a1	INIT Link flags
True		
intr_priority	3	Interrupt priority
False		
lg_term_dma	0x800000	Long term DMA
True		
max_xfer_size	0x100000	Maximum Transfer Size
True		
num_cmd_elems	200	Maximum number of COMMANDS to queue to the adapter
True		
pref_alpa	0x1	Preferred AL_PA
True		
sw_fc_class	2	FC Class for Fabric
True		

4.5 Logical Volume Manager administration on AIX 5L

This section provides a summary of Logical Volume Manager (LVM) on AIX 5L V5.3. This information is an important reference for the future chapters relating to migration scenarios.

The fundamental concepts used by LVM are physical volumes, volume groups, physical partitions, logical volumes, logical partitions, file systems, and raw devices. It is necessary to understand more components for a thorough knowledge about how LVM works on AIX 5L.

Figure 4-2 shows a summary of the basic LVM units on AIX 5L. The sections that follow provide a detailed explanation about the components.

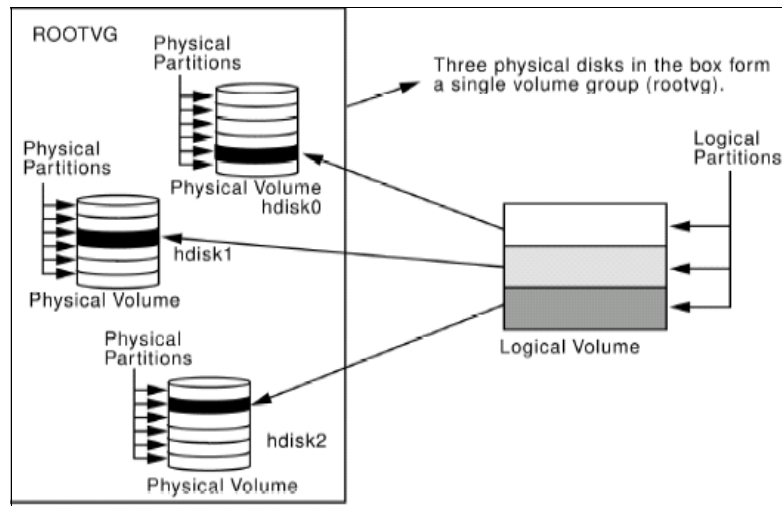


Figure 4-2 Relationship between the logical storage components

4.5.1 Logical Volume Manager configuration data

The data that describes the components of the LVM is not kept in one place. It is important to understand that this descriptive data about volume groups, logical volumes, and physical volumes is kept in several places.

Object Data Manager database

The Object Data Manager (ODM) database is the place where most of the AIX 5L system configuration data is kept. The ODM database contains information about all the configured physical volumes, volume groups, and logical volumes. This information mirrors the information found in the Volume Group Descriptor Area (VGDA). The process of importing a VGDA, for example, involves the automatic copying of VGDA data for the imported volume group into the ODM. When a volume group is exported, the data held in the ODM about that volume group is removed from the ODM database. The ODM data also mirrors the information held in the Logical Volume Control Block (LVCB).

Volume Group Descriptor Area

The VGDA, located at the beginning of each physical volume, contains information that describes all the logical volumes and all the physical volumes that belong to the volume group of which that physical volume is a member. The VGDA is updated by almost all the LVM commands. The VGDA makes each

volume group self-describing. An AIX 5L system can read the VGDA on a disk, and from that, can determine what physical volumes and logical volumes are a part of that volume group.

Each disk contains at least one VGDA. This is important at vary on time. The time stamps in the VGDA are used to determine which VGDA correctly reflect the state of the volume group. VGDA can get out of sync when, for example, a volume group of four disks has one disk failure. The VGDA on that disk cannot be updated when it is not operational. Therefore, a method to update this VGDA when the disk comes online is required, and this is what the vary on process does.

The VGDA is allocated when the disk is assigned as a physical volume (with the command `mkdev`). This reserves a space for the VGDA at the start of the disk. The actual volume group information is placed in the VGDA when the physical volume is assigned to a volume group (using the `mkvg` command or the `extendvg` command).

When a physical volume is removed from the volume group (using the `reducevg` command), the volume group information is removed from the VGDA.

Volume Group Status Area

The Volume Group Status Area (VGSA) contains state information about physical partitions and physical volumes, for example, the VGSA knows if one physical volume in a volume group is unavailable. Both the VGDA and the VGSA have beginning and ending time stamps that are important. These time stamps enable the LVM to identify the most recent copy of the VGDA and the VGSA at vary on time. The LVM requires that the time stamps for the chosen VGDA be the same as those for the chosen VGSA.

VGSA is used for monitoring and maintained data copies synchronization.

The VGSA is essentially a bitmap, and its architecture and location on the disk depends on the type of the volume group.

Logical Volume Control Block

The LVCB contains important information about the logical volume, such as the number of the logical partitions or the disk allocation policy. Its architecture and location on the disk depends on the type of the volume group it belongs to. For standard volume groups, the LVCB resides on the first block of user data within the LV. For big volume groups, there is additional LVCB information in VGDA on the disk. For scalable volume groups, all the relevant logical volume control information is kept in the VGDA as part of the LVCB information area and the LV entry area.

Example 4-6 shows the use of the **getlvcb** command to display the information held in the LVCB of logical volume hd2.

Example 4-6 getlvcb from Logical Volume Control Block

```
# getlvcb -TA hd2
  AIX LVCB
  intrapolicy = c
  copies = 1
  interpolicy = m
  lvid = 00c4790e00004c0000000005491642c0.5
  lvname = hd2
  label = /usr
  machine id = 4790E4C00
  number lps = 33
  relocatable = y
  strict = y
  stripe width = 0
  stripe size in exponent = 0
  type = jfs2
  upperbound = 32
  fs =
  time created = Sun Sep 20 17:50:40 1970
  time modified = Sun Sep 20 18:41:17 1970
#
```

Disk quorum

Each physical disk in a volume group has at least one VGDA or VGSA. The number of VGDA's contained in a single disk varies according to the number of disks in the volume group, as shown in Table 4-3.

Table 4-3 VGDA allocation

Condition	VGDA allocation
Single physical volume (PV) in a volume group	Two VGDA's on one disk
Two PV's in a volume group	Two VGDA's on the first disk, one VGDA on the second disk
Three or more PV's in a volume group	One VGDA on each disk

A quorum is a state in which 51 per cent or more of the physical volumes in a volume group are accessible. A quorum is a vote of the number of VGDA and VGSA that are active. A quorum ensures data integrity in the event of a disk failure.

When a volume group is created on a single disk, it initially has two VGDA/VGSA combinations residing on the disk. If a volume group consists of two disks, one disk still has two VGDA/VGSA combinations, but the other disk has one VGDA/VGSA combination. When the volume group is made up of three or more disks, each disk is allocated just one VGDA/VGSA combination.

Figure 4-3 shows that the quorum is lost when enough disks and their VGDA/VGSA combinations are unreachable, so that a 51 per cent majority of VGDA/VGSA area no longer exists.

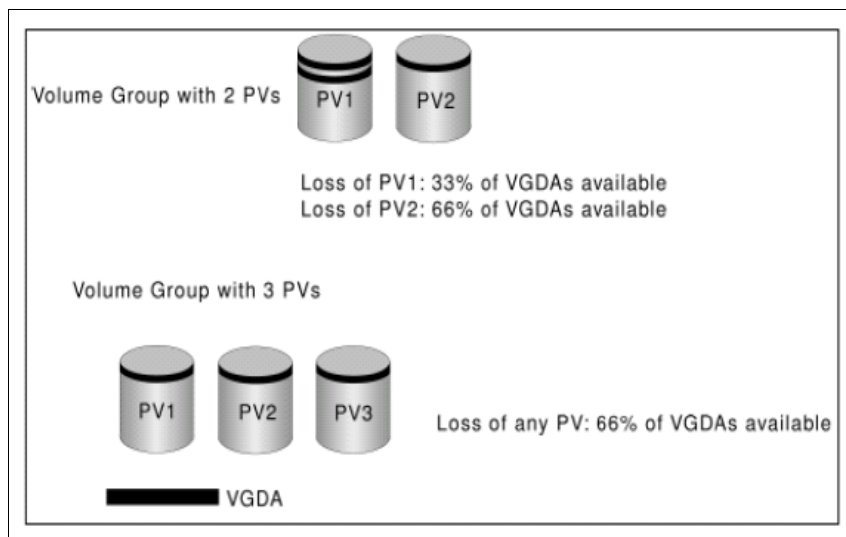


Figure 4-3 Disk quorum

When a quorum is lost, the volume group varies itself off so that the disks are no longer accessible by the LVM. This prevents further disk I/O to that volume group so that data is not lost or assumed to be written when physical problems occur. Additionally, as a result of the vary off, the user is notified in the error log that a hardware error has occurred and service must be performed.

This has implications when you want to use disk mirroring to ensure high availability. In a two disk mirrored system, if the first disk fails, you have lost 66 per cent of your VGDA's, and the entire volume group becomes unavailable. This defeats the purpose of mirroring. For this reason, three or more (generally an odd number) disk units provide a higher degree of availability and are highly recommended where mirroring is desired.

Note: The ability to turn off disk quorum protection on any volume group exists. Turning off quorum protection allows a volume group to remain online even when a quorum or majority of its VGDA's are not online. This allows the volume group to remain online in the situation described earlier. This capability provides for a less expensive mirroring solution, but does carry the risk of data loss because, after a disk failure, data is accessible, but is no longer mirrored.

4.6 Physical volumes

Following are some of the characteristics of physical volumes:

- ▶ Each individual disk drive is a named PV, and has a name such as hdisk0 or hdisk1.
- ▶ One or more PVs can make up a volume group (VG). A PV can belong to a maximum of one VG.
- ▶ You cannot assign a fraction of a PV to one VG. A PV is assigned entirely to a VG.
- ▶ PVs can be assigned to the same VG even though they are of different types, such as SCSI or Serial Storage Architecture (SSA).
- ▶ Storage space from PVs is divided into physical partitions (PPs).
- ▶ The size of the physical partitions is identical on all the disks belonging to the same VG.

Table 4-4 shows the PV commands.

Table 4-4 PV commands

Command	Smit fast path	Description
lspv	smit lspv	Lists information about a physical volume
chpv	smit chpv	Changes the characteristics of a physical volume

Example 4-7 shows how to list all the PVs on AIX 5L.

Example 4-7 Physical volume information using lspv

```
# lspv
hdisk0          00c4790ea0a455f0          rootvg
active
hdisk1          00c4790ecc77fd19          rootvg
active
```

Example 4-8 shows how to list details about a physical volume.

Example 4-8 Detailed physical volume information using lspv

```
# lspv hdisk0
PHYSICAL VOLUME:  hdisk0          VOLUME GROUP:  rootvg
PV IDENTIFIER:    00c4790ea0a455f0 VG IDENTIFIER
00c4790e00004c00000000005491642c0
PV STATE:         active
STALE PARTITIONS: 0          ALLOCATABLE:   yes
PP SIZE:          32 megabyte(s) LOGICAL VOLUMES: 10
TOTAL PPs:        639 (20448 megabytes) VG DESCRIPTORS: 2
FREE PPs:         572 (18304 megabytes) HOT SPARE:     no
USED PPs:         67 (2144 megabytes)  MAX REQUEST:   128
kilobytes
FREE DISTRIBUTION: 127..128..61..128..128
USED DISTRIBUTION: 01..00..66..00..00
```

4.7 Volume groups

The LVM layer for AIX 5L V5.3 provides an increased level of flexibility in disk management. However, there are limitations, as shown in Table 4-5.

Note: Within each VG, one or more LVs can be defined.

Table 4-5 LVM limitations

VG type	Maximum PVs	Maximum LVs	Maximum PPs per LV	Maximum PP size
Normal VG	32	256	32512	1Gb
Big VG	128	512	130048	1Gb
Scalable VG	1024	4096	2097152	128Gb

Table 4-6 shows a summary of commands used in VG management.

Table 4-6 VG commands

Command	Smit fast path (menu management)	Task
lsvg	smit lsvg	Displays information about VGs
mkvg	smit mkvg	Creates a VG
chvg	smit chvg	Sets the characteristics of a VG
extendvg	smit extendvg	Adds a new disk on a VG
reducevg	smit reducevg	Removes a disk from a VG
varyonvg	smit varyonvg	Activates a VG
varyoffvg	smit varyoffvg	Deactivates a VG
exportvg	smit exportvg	Exports the definition of a VG from a set of PVs
importvg	smit importvg	Imports a new VG definition from a set of PVs

The examples provided here pertain to volume group management. Check the man pages for more information about the command options.

Example 4-9 shows the command for listing all the VGs.

Example 4-9 Listing all the VGs

```
# lsvg
rootvg
altinst_rootvg
```

Example 4-10 shows the command for listing a VG's features.

Example 4-10 Listing a VG's features

```
# lsvg rootvg
VOLUME GROUP:      rootvg                VG IDENTIFIER:
00c4790e00004c0000000005491642c0
VG STATE:          active                PP SIZE:        32
megabyte(s)
VG PERMISSION:    read/write            TOTAL PPs:     1278
(40896 megabytes)
```

MAX LVs:	256	FREE PPs:	1202
(38464 megabytes)			
LVs:	13	USED PPs:	76 (2432
megabytes)			
OPEN LVs:	10	QUORUM:	2
TOTAL PVs:	2	VG DESCRIPTORS:	3
STALE PVs:	0	STALE PPs:	0
ACTIVE PVs:	2	AUTO ON:	yes
MAX PPs per VG:	32512		
MAX PPs per PV:	1016	MAX PVs:	32
LTG size (Dynamic):	128 kilobyte(s)	AUTO SYNC:	no
HOT SPARE:	no	BB POLICY:	
relocatable			

The command for creating a VG is as follows:

```
# mkvg -y new_vg hdisk1
new_vg
```

The command for changing a VG for BIG VG is as follows:

```
/usr/sbin/chvg -a y -Q y -B itso
```

The command for extending a VG is as follows:

```
# extendvg -f new_vg hdisk2
0516-1254 extendvg: Changing the PVID in the ODM.
```

The command for reducing a VG is as follows:

```
# reducevg -f new_vg hdisk2
#
```

When you remove the last disk that is part of a VG, the VG is automatically removed from AIX 5L. The command for removing the disks and the LVs at the same time, is as follows:

```
# reducevg -df new_vg hdisk1
ldeletepv: Volume Group deleted since it contains no physical volumes.
```

Example 4-11 is about exporting and importing a VG. Note that on import and export tasks, it is necessary to activate and deactivate the VG.

Example 4-11 Exporting and importing a VG

```
# lsvg
rootvg
itsovg
# varyoffvg itsovg
```

```

# exportvg itsovg
# lsvg
rootvg

# importvg -y itsovg -f hdisk1
itsovg
# varyonvg itsovg
# lsvg
rootvg
itsovg

```

4.8 Logical volumes

LVs consist of one or more logical partitions (LPs). Each LP has at least one corresponding physical partition. An LP and a physical partition are always the same size. You can have up to three copies of the data located on different physical partitions. Usually, physical partitions storing identical data are located on different physical disks for redundancy purposes.

Data from an LV can be stored in an organized manner, having the form of files located in the directories. This structured and hierarchical form of organization is called a *file system*.

Data from an LV can also be seen as a sequential string of bytes. These types of LVs are called raw logical volumes. It is the responsibility of the application that uses this data to access and interpret it correctly.

Physical volumes and VGs are normally not addressed directly by users and applications to access data, and they cannot be manipulated to provide disk space for use by users and applications. However, LVs provide the mechanism to make disk space available for use, giving users and applications the ability to access the data stored on them.

Table 4-7 shows a summary of commands used in VG management.

Table 4-7 LV commands

Command	Smit fast path	Description
lslv	smit lslv	Lists information about an LV
mklv	smit mklv	Creates an LV
chlv	smit chlv	Changes the characteristics of an LV

Command	Smit fast path	Description
<code>rmlv</code>	<code>smit rmlv</code>	Deletes an LV
<code>extendlv</code>	<code>smit extendlv</code>	Extends an LV

The command for creating a new jfs2 LV is:

```
## mklv -t jfs2 itsvg 1G
fslv00
```

Example 4-12 shows the command for checking the LV.

Example 4-12 Checking the LV

```
## lslv fslv00
LOGICAL VOLUME:      fslv00                VOLUME GROUP:      itsvg
LV IDENTIFIER:      00c4790e00004c000000010acd6f6546.1  PERMISSION:
read/write
VG STATE:           active/complete        LV STATE:          closed/syncd
TYPE:               jfs2                   WRITE VERIFY:      off
MAX LPs:            512                     PP SIZE:           32
megabyte(s)
COPIES:             1                       SCHED POLICY:     parallel
LPs:                32                       PPs:              32
STALE PPs:          0                       BB POLICY:         relocatable
INTER-POLICY:       minimum                  RELOCATABLE:      yes
INTRA-POLICY:       middle                   UPPER BOUND:      32
MOUNT POINT:        N/A                     LABEL:            None
MIRROR WRITE CONSISTENCY: on/ACTIVE
EACH LP COPY ON A SEPARATE PV ?: yes
Serialize IO ?:     NO
```

Following is the command for increasing an LV size:

```
# /usr/sbin/extendlv fslv00 10M
#
```

Example 4-13 shows the command for removing an LV.

Example 4-13 Removing an LV

```
# rmlv fslv00
Warning, all data contained on logical volume fslv00 will be destroyed.
rmlv: Do you wish to continue? y(es) n(o)? y
rmlv: Logical volume fslv00 is removed.
```

4.8.1 File system

File systems represent a convenient way of storing and accessing data from an LV. A file system comprises files, directories, and other data structures. File systems maintain information and identify the location of a file or a directory's data.

Details about file system types and management examples on AIX 5L are available in "File system journaling on AIX 5L" on page 123.

4.8.2 Disk mirroring

Disk mirroring is the association of two or three physical partitions with each LP in an LV. When the data is written on the LV, it is also written to all the physical partitions that are associated with the LP. Thus, mirroring data increases the availability of data.

AIX 5L and Logical Volume Manager provide a disk mirroring facility at an LV level. If mirroring is established, this can be performed when an LV is created.

The **mk1v** command allows you to select one or two additional copies for each LV. Mirroring can also be added to an existing LV using the **mk1vcopy** command.

The following mirroring factors further improve data availability:

- ▶ The number of copies of the data

It is more reliable to keep three copies of the data rather than two copies.

- ▶ Location of the copies

Allocating the copies of a logical partition on different physical volumes is more reliable than allocating the copies on the same physical volume. This is because one of the most common error modes for disk subsystems is the loss of an individual physical disk. Copies can also be located across different disk adapters to further enhance isolation from failures.

The **mirrorvg** command mirrors all the LVs on a given volume group. The same function can also be accomplished manually if you run the **mk1vcopy** command for each individual LV in a volume group. As with **mk1vcopy**, the target physical drives to be mirrored with data must already be members of the volume group.

Table 4-8 shows the mirroring commands.

Table 4-8 *Mirroring commands*

Command	Smit fast path	Task
mk1vcopy	smit mk1vcopy	Provides copies of data within an LV

Command	Smit fast path	Task
rmlvcopy	smit rmlvcopy	Removes copies from an LV
mirrorvg	smit mirrorvg	Mirrors all the LVs that exist on a given volume group
unmirrorvg	smit unmirrorvg	Removes the mirrors that exist on volume groups or specified disks
syncvg	smit syncvg	Synchronizes LV copies that are not current

Example 4-14 shows the command for mirroring rootvg on hdisk1.

Example 4-14 Mirroring rootvg on hdisk1

```

# lspv
hdisk0          00c4790ea0a455f0          rootvg
active
hdisk1          00c4790ecc77fd19          None
hdisk2          00c4790ecd611578          altinst_rootvg
hdisk3          00c4790ecd54055d          itso
active
#
# extendvg -f rootvg hdisk1
# lspv
hdisk0          00c4790ea0a455f0          rootvg
active
hdisk1          00c4790ecc77fd19          rootvg
active
hdisk2          00c4790ecd611578          altinst_rootvg
hdisk3          00c4790ecd54055d          itso
active
#
# /usr/sbin/mirrorvg rootvg hdisk0 hdisk1
0516-1124 mirrorvg: Quorum requirement turned off, reboot system for
this
        to take effect for rootvg.
0516-1126 mirrorvg: rootvg successfully mirrored, user should perform
        bosboot of system to initialize boot records. Then, user must
modify
        bootlist to include: hdisk0 hdisk1.
# bosboot -ad /dev/hdisk1

bosboot: Boot image is 25166 512 byte blocks.
bootlist -m normal hdisk0 hdisk1

```

4.9 File system types and management

This section discusses different methods to manage a disk-based file system on Solaris and AIX 5L.

4.9.1 Basic administration and concepts

The basic administration is similar in Solaris and AIX 5L. The main commands and differences are shown in Table 4-9.

Table 4-9 File system management

File system management	Solaris	AIX 5L
Create a file system on disk	<code>newfs</code> or <code>mkfs</code>	<code>mkfs</code> or <code>crfs</code>
Check the file system space used	<code>df -k</code>	<code>df -k</code>
Check the file system i-nodes used	<code>df -o i</code>	<code>df -k</code>
Check the file system for consistency	<code>fsck</code>	<code>fsck</code>
Check the file system type	<code>df -n</code>	<code>lsfs</code> , <code>lslv</code> , <code>lsvg</code>
Check the file with basic file system settings	<code>cat /etc/vfstab</code>	<code>cat /etc/filesystems</code>

Basic administration examples on AIX 5L

This section provides examples pertaining to basic administration in AIX 5L.

Example 4-15 shows the command for checking the size and i-nodes occupation.

Example 4-15 Checking the size and i-nodes occupation

```
#df -k
Filesystem      1024-blocks    Free %Used   Iused %Iused Mounted on
/dev/hd4         65536         45996  30%     1235   4% /
/dev/hd2        737280         56984  93%    19525  11% /usr
/dev/hd9var     32768         29776  10%      304   4% /var
/dev/hd3        32768         17244  48%      126   2% /tmp
/dev/hd1        16384         15656   5%       30   1% /home
/dev/lv00       16384         15828   4%       17   1% /test
```

To get a similar Solaris file system occupation, see Example 4-16. This information is useful for scripts migration.

Example 4-16 df command output using “-kI”

```
# df -kI
Filesystem    1024-blocks    Used    Free %Used Mounted on
/dev/hd4      65536         19540   45996  30% /
/dev/hd2      737280        680296  56984  93% /usr
/dev/hd9var   32768         2992    29776  10% /var
/dev/hd3      32768         15524   17244  48% /tmp
/dev/hd1      16384         728     15656  5% /home
/dev/lv00     16384         556     15828  4% /test
```

Example 4-17 shows a file system creation. The -A yes option enables the file system to be mounted on the next boot. In other words, the /etc/filesystems file will be changed automatically.

Example 4-17 Creating a file system

```
# /usr/sbin/crfs -v jfs2 -g rootvg -a size=80M -m itso -A yes
File system created successfully.
98096 kilobytes total disk space.
New File System size is 196608
# mkdir /itso
mkdir: 0653-358 Cannot create /itso.
/itso: Do not specify an existing file.
# mount /itso
# df -kI /itso
Filesystem    1024-blocks    Used    Free %Used Mounted on
/dev/fslv00   98304          344    97960  1% /itso
```

4.9.2 File system types on Solaris and AIX 5L

Natively, Solaris only supports the UNIX file system (UFS) for hard disks. The **newfs** command or the **mkfs** command is used to create the file system and the **fsck** command is used to check and fix the file system for consistency.

It is common to see Solaris with Veritas File System (vxfs). This is a third-party product.

The other types of disk-based file systems are High Sierra File System (HSFS) (for CD-ROM), PC File System (PCFS) (for diskettes), and Universal Disk Format (UDF) (for DVD).

AIX 5L natively supports the journaled file system (JFS) and journaled file system 2 (JFS2) file systems. Both are journalized, and no third-party file systems are necessary. For more information about JFS and JFS2, refer to 4.9.7, “File system journaling” on page 122.

Table 4-10 shows a summary of file system types on Solaris and AIX 5L OS.

Table 4-10 File system types

File system types	Solaris	AIX 5L
Native file system	ufs	jfs and jfs2
CD-ROM file system	nsfs	cdrfs
DVD file system	udf	cdrfs
MSDOS file system	pcfs	cifs
Win95+ file system	pcfs	cifs
Network file system	nfs	nfs

4.9.3 Network File System

The Network File System (NFS) is a distributed file system that allows users to access files and directories of remote servers as though they are local, for example, you can use OS commands to create, remove, read, write, and set file attributes for remote files and directories. NFS is independent of machine types, OS, and network architectures because of its use of remote procedure calls (RPC) for these services.

On Solaris, the daemon that converts RPC program numbers into port numbers is called *rpcbind*. On AIX 5L, the same daemon is called *portmap*.

On Solaris and AIX 5L, the command **rpcinfo** is used to report RPC information.

The NFS is available for Solaris and AIX 5L, and you can use it in heterogeneous networks with Solaris and AIX 5L OS, with each of them being an NFS server or client or both.

AIX 5L V5.3 was the first version of AIX 5L to introduce support for NFSv4, even as it continued to support for NFSv2 and NFSv3. The default NFS protocol version used in server exports and client mounts under AIX 5L V5.3 is still V3. This decision was made to permit an easier migration to AIX 5L V5.3 from the earlier versions because few sites were prepared to implement the features provided by NFSv4.

To enjoy the new features available on NFSv4, refer to *Implementing NFSv4 in the Enterprise: Planning and Migration Strategies*, SG24-6657.

In any version, for successful implementation of an NFS environment, the following points must be considered:

- ▶ The NFS daemons must be running on the server and the clients.
- ▶ The file systems that have to be remotely available must be exported.
- ▶ The exported file systems must be mounted on the remote (client) systems.

Daemon control

An NFS difference between Solaris and AIX 5L pertains to daemon control. By default, on AIX 5L, the NFS daemons are not started on a newly installed system. When a system is first installed, all the files are placed on the system, but the steps to activate NFS are not taken. The daemons can be started by using one of the following methods:

- ▶ By using the following smit fast path:

```
smit mknfs
```
- ▶ By using the **mknfs** command to start the NFS daemons immediately. This must produce the result shown in Example 4-18.
 - Option **-B** of the **mknfs** command configures the daemons to be started now and on the next boot.
 - Option **-l** of the **mknfs** command configures the daemons to be started only on the next boot.

Example 4-18 Using mknfs

```
# mknfs -N
0513-029 The portmap Subsystem is already active.
Multiple instances are not supported.
Starting NFS services:
0513-029 The biod Subsystem is already active.
Multiple instances are not supported.
0513-029 The rpc.statd Subsystem is already active.
Multiple instances are not supported.
0513-029 The rpc.lockd Subsystem is already active.
Multiple instances are not supported.
Completed NFS services.
```

- By using Resource Controller, as shown in Example 4-19.

Example 4-19 Starting NFS daemons

```
# startsrc -g nfs
0513-059 The biod Subsystem has been started. Subsystem PID is 204914.
0513-059 The nfsd Subsystem has been started. Subsystem PID is 233628.
0513-059 The rpc.mountd Subsystem has been started. Subsystem PID is
245896.
0513-059 The nfsrgyd Subsystem has been started. Subsystem PID is
348338.
0513-059 The gssd Subsystem has been started. Subsystem PID is 344244.
0513-059 The rpc.lockd Subsystem has been started. Subsystem PID is
348340.
0513-059 The rpc.statd Subsystem has been started. Subsystem PID is
278690.
```

After the daemons are started on the client and the server, perform the NFS tasks, as shown in Example 4-20.

Exporting the file systems

In AIX 5L, you can edit the configuration file (*/etc/exports*) and issue the `exportfs` command. If you want to export a directory that is not explicitly defined in the configuration file, see Example 4-20.

Example 4-20 Exporting the file systems

```
aixlab: /> exportfs
exportfs: 1831-182 nothing exported
aixlab: /> exportfs -i /test
aixlab: /> exportfs
/test -rw
```

Mounting the Network File System

Example 4-21 shows how to mount an NFS using a command line.

Example 4-21 Mounting an NFS

```
# mount 10.20.1.18:/test /test
# df -k /test
```

Filesystem	1024-blocks	Free	%Used	Iused	%Iused	Mounted on
10.20.1.18:/test	672676	329640	51%	23118	7%	/test

Summary of differences

Table 4-11 shows a summary of NFS differences between Solaris and AIX 5L.

Table 4-11 NFS differences

Task and configuration file	Solaris	AIX 5L
Start NFS daemons	<ul style="list-style-type: none">▶ /etc/init.d/nfs.client start and▶ /etc/init.d/nfs.server start	startsrc -g nfs
Stop NFS daemons	<ul style="list-style-type: none">▶ /etc/init.d/nfs.client stop and▶ /etc/init.d/nfs.server stop	stopsrc -g nfs
Mount a resource on an NFS client	mount -F nfs <i>server://resource /mntpoint</i>	mount <i>server://resource /mntpoint</i>
Share file systems from a configuration file	shareall exportfs -a	exportfs -a
Share a new file system	share -F nfs ... <i>directory</i>	exportfs -i <i>directory</i>
Config file of shared file systems	/etc/dfs/dfstab	/etc/exports
File that contains NFS is to be mounted at booting	/etc/vfstab	/etc/filesystems
Command to share a directory or file system	<ul style="list-style-type: none">▶ share or▶ exportfs	<ul style="list-style-type: none">▶ mknfsexp or▶ exportfs

For detailed information about NFS on AIX 5L, refer to *Securing NFS in AIX An Introduction to NFS v4 in AIX 5L Version 5.3*, SG24-7204.

4.9.4 Autofs automounter

An *automounter* is a facility used to manage the mounting activity of a file system. When you access a file or directory under the automounter control, the automounter transparently mounts the required file system. When there has been no activity on this file system for some predetermined amount of time, the automounter unmounts the file system.

Automounters are typically used with the NFS, which is a distributed file system that allows you to access files and directories located on remote systems and treats those files and directories as if they were local. When performing the mounting activity for an NFS, the automounter uses the NFS mounting facilities. The automounter reduces the period of time that a file system is actively mounted, thereby minimizing local system hangs due to NFS server outages.

Solaris

Automount is configured in the `/etc/auto_master` file (and its other corresponding files) and is activated by the startup script `/etc/rc2.d/S74autofs`, which runs during the server boot to run level 2 or level 3. After automount is run as a daemon, all the NFS mounting and unmounting are automatically handled.

AIX 5L

The AIX 5L automount daemon reads automount map files to determine which directories to support. Typically, there is one map file for each file system to be controlled by the automounter. The map file contains entries for each directory supported within the file system, the host name where the directory resides, and the specific mount information for that directory. The automount map files are kept in the `/etc/auto/maps` directory by default. The list of all the map files to be used by the automount daemon is specified in the master map file `/etc/auto.master`. This master map file contains entries for each file system to be controlled by the automounter, the name of the map file containing the directory information, and the optional default mount information.

Table 4-12 compares autofs in Solaris and AIX 5L.

Table 4-12 Autofs

Task	Solaris	AIX 5L
Automount daemon	automountd	automountd
Default map file	<code>/etc/auto_master</code>	<code>/etc/auto_master</code>
Stop automount	<code>/etc/init.d/autofs stop</code>	<code>startsrc -s automountd</code>
Start automount	<code>/etc/init.d/autofs start</code>	<code>stopsrc -s automountd</code>

4.9.5 Virtual file systems

These types of file systems (except CacheFS™) do not have a 1:1 corresponding disk slice or volume that it uses to store the data, but instead uses the system random access memory (RAM) to store information. Anything that gets stored in here will not be persistent across a reboot.

Solaris

There are several different types of virtual file systems in Solaris, with each type being used for a specific purpose:

▶ /tmp

Based on the tmpfs, this is used for storing the temporary files generated by the OS and the applications. When this space fills up to a certain level, the physical swap is used as the backing store where these files are moved. This space is also used as a buffer space for file system reads and writes in order to increase access time.

▶ /var/run

Provides a place to store the temporary system files that are currently in use, but is not required across a reboot. This space also provides access to special kernel information and facilities.

▶ CacheFS

Used for caching slow devices on a local hard drive, such as simple or double-speed CD-ROMs or NFS over slow networks.

▶ Loopback file system

Provides a way to create a virtual file system by using a different path to access the files within this file system.

▶ /proc

Contains all the active processes in the system according to process number.

/proc on AIX 5L

As with the Solaris environment, AIX 5L too has the /proc file system. /proc on AIX 5L contains information about each process, about the running kernel, devices, networking stack, and so on.

Table 4-13 compares /proc management in Solaris and AIX 5L.

Table 4-13 /proc management

Task	Solaris	AIX 5L
Process credentials	pcred	proccred
File descriptor information	pfiles	procfiles
Flags trace	pflags	procflags
Dynamic libraries loaded by process	p1dd	procldd
Address space map of processes	pmap	procmap

Task	Solaris	AIX 5L
Start the stopped processes	prun	procrun
List the signal actions	psig	procsig
Process stacks	pstack	procstack
Stop the process on the PR_REQUESTED event	pstop	procstop
Print the process tree by ID or users	ptree	proctree
Wait for all the specified processes to terminate	pwait	procwait
Current work directory of a process	pwdx	procpwdx

CacheFS on AIX 5L

The CacheFS on AIX 5L is a general purpose file system caching mechanism that improves NFS server performance and scalability by reducing server and network load. Designed as a layered file system, CacheFS provides the ability to cache one file system on another. In an NFS environment, CacheFS increases the client-per-server ratio, reduces server and network loads, and improves performance for clients on slow links, such as Point-to-Point Protocol (PPP).

Create a cache on the client so that the file systems that you specify to be mounted in the cache can be accessed by the user locally instead of across the network. When a user first requests access to these files, they are placed in the cache. The cache does not get filled until the user requests access to a file or files. Initial file requests might be slow, but subsequent use of the same files are faster.

To perform any CacheFS task on AIX 5L, the product bos.net.nfs must already be installed on the OS.

Table 4-14 describes the main commands and smit fast paths for CacheFS management.

Table 4-14 CacheFS on AIX 5L

Task	Smit fast path	Command line
Set up a cache	cachefs_admin_create	cfsadmin -c MountDirectoryName1

Task	Smit fast path	Command line
Specify files for mounting	<code>cachefs_mount</code>	<ul style="list-style-type: none"> ▶ <code>mount -F cachefs -o backfstype=FileSysType</code> ▶ <code>cachedir=CacheDirectory[,options]Back FileSystem MountDirectoryName2 or</code> ▶ <code>edit /etc/filesystems</code>
Modify the cache	<code>cachefs_admin_change</code>	Remove the cache and then recreate it using the appropriate mount command options
Display cache information	<code>cachefs_admin_change</code>	<code>cfsadmin -l MountDirectoryName</code>
Remove a cache	<code>cachefs_admin_remove</code>	<ul style="list-style-type: none"> ▶ Unmount the file system with <code>umount MountDirectoryName</code> ▶ Determine the cache ID with <code>cfsadmin -l MountDirectoryName</code> ▶ Delete the file system with <code>cfsadmin -d CacheID CacheDirectory</code>
<code>cachefs_admin_check</code>	<code>cachefs_admin_check</code>	<code>fsck_cachefs CacheDirectory</code>

4.9.6 Swap space

On Solaris, the swap space is related to the /tmp file system.

On AIX 5L, the swap area is always related to a logical volume.

Overview of Solaris

The only swap configuration command on Solaris is **swap**. You can add, remove and list the available swaps. A swap can be defined in dedicated disk slices, which is the preferred way, or as files within file systems, which is usually performed for emergency and temporary purposes.

Overview of AIX 5L

A page is a unit of virtual memory that holds 4 KB of data and can be transferred between real storage and auxiliary storage.

A paging space, also called a swap space, is a logical volume with the attribute “type equal to paging”. This type of logical volume is referred to as a paging space logical volume or paging space. When the amount of free real memory in the system is low, programs or data that have not been used recently are moved from real memory to paging space in order to release real memory for other activities. The installation creates a default paging logical volume (hd6) on drive hdisk0, also referred to as primary paging space.

Table 4-15 shows swap area management in Solaris and AIX 5L.

Table 4-15 Swap management

Task	Solaris	AIX 5L
List total and usage swap area	<code>swap -l</code>	<ul style="list-style-type: none"> ▶ <code>swap -l</code> or ▶ <code>lsps</code>
Increase page space	<code>swap -a</code>	<ul style="list-style-type: none"> ▶ <code>mkps</code> ▶ <code>chps -s</code>
Reduce swap area	<code>swap -r</code>	<ul style="list-style-type: none"> ▶ <code>chps -d</code> ▶ <code>rmpps</code>
Activate page space	<code>swap -a</code>	<ul style="list-style-type: none"> ▶ <code>swap -a</code> ▶ <code>swapon</code>
Deactivate page space	<code>swap -d</code>	<ul style="list-style-type: none"> ▶ <code>swap -d</code> ▶ <code>swapoff</code>
Migrate page space between different disks	<code>vxevac</code> (available only if the page space area is under Veritas Volume Manager)	<code>migratepv</code>

Swap management examples on AIX 5L

This section provides swap management examples on AIX 5L.

Example 4-22 shows swap information.

Example 4-22 Swap information

```
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
hd6             hdisk0          rootvg         512MB    1  yes
yes    lv
```

Example 4-23 shows how to increase the swap area size.

Example 4-23 Increasing swap area size

```
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
hd6             hdisk0          rootvg         512MB    1  yes
yes    lv
# chps -s 2 hd6
# lsps -a
```

Page Space Auto Type	Physical Volume	Volume Group	Size	%Used	Active
hd6 yes lv	hdisk0	rootvg	576MB	1	yes

Example 4-24 shows how to shrink swap area size.

Example 4-24 Shrinking the swap area size

```
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
hd6             hdisk0          rootvg          576MB  1  yes
yes            lv
# chps -d 2 hd6
shrinkps: Temporary paging space paging00 created.
shrinkps: Dump device moved to temporary paging space.
shrinkps: Paging space hd6 removed.
shrinkps: Paging space hd6 recreated with new size.
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
hd6             hdisk0          rootvg          512MB  1  yes
yes            lv
```

Example 4-25 shows how to create a new swap area.

Example 4-25 Creating a new swap area

```
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
hd6             hdisk0          rootvg          512MB  1  yes
yes            lv
# mkps -s 10 rootvg
paging00
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
paging00       hdisk0          rootvg          320MB  0  no
no            lv
hd6             hdisk0          rootvg          512MB  1  yes
yes            lv
```

Example 4-26 shows how to activate the swap area.

Example 4-26 Activating the swap area

```
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
paging00        hdisk0           rootvg          320MB  0  no
no             lv
hd6             hdisk0           rootvg          512MB  1  yes
yes           lv
# swapon /dev/paging00
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
paging00        hdisk0           rootvg          320MB  1  yes
no             lv
hd6             hdisk0           rootvg          512MB  1  yes
yes           lv
```

Example 4-27 shows how to deactivate the swap area.

Example 4-27 Deactivating the swap area

```
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
paging00        hdisk0           rootvg          320MB  1  yes
no             lv
hd6             hdisk0           rootvg          512MB  1  yes
yes           lv
# swapoff /dev/paging00
# lsps -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
paging00        hdisk0           rootvg          320MB  0  no
no             lv
hd6             hdisk0           rootvg          512MB  1  yes
yes           lv
```

Example 4-28 shows how to remove a swap area.

Example 4-28 Removing a swap area

```
# lsvg -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
paging00        hdisk0           rootvg          320MB  0   no
no             lv
hd6             hdisk0           rootvg          512MB  1   yes
yes           lv
# rmps paging00
rmlv: Logical volume paging00 is removed.
# lsvg -a
Page Space      Physical Volume  Volume Group    Size %Used Active
Auto Type
hd6             hdisk0           rootvg          512MB  1   yes
yes           lv#
```

The other important feature of swap management in AIX 5L is that it works with smit. The fast path to swap management on smit is **smit pgsd**.

4.9.7 File system journaling

File system journaling is a way of storing the transactions before they are written to the file system itself. After it is stored, the transaction can be applied to the file system at a later time. When a hard reboot is encountered, the OS only has to check and replay the journal log and does not have to check the entire file system, thereby reducing the time it takes to perform the checks at boot up.

File system journaling on Solaris

The Solaris Volume Manager (SVM) default is logging-enabled for any UFS unless specifically disabled by itself because of available free space, or specifically disabled by the system administrator.

SVM's logging is all internal to the mounted file system and does not make use of any external device to keep log entries.

For the Veritas file system, the journaling is default-enabled.

File system journaling on AIX 5L

AIX 5L V5.1 introduced the JFS2, which is an enhanced and updated version of the JFS on AIX 5L V4.3 and earlier releases. JFS2 is recommended only for systems that are running the 64-bit kernel. In AIX 5L V5.3, JFS2 is the default file system that is created.

JFS provides the following features:

- ▶ Journaling

Journaling is the process of storing transactions (changes that make up a complete journaled file system (JFS) operation) in a journal log before the transactions are applied to the JFS. After a transaction is stored, the transaction can be applied to the file system later.

- ▶ Extent-based allocation

When data is stored in a JFS2, it is grouped in extents instead of one block at a time.

- ▶ Snapshots

AIX 5L V5.2 introduced the JFS2 snapshot image. The JFS2 snapshot image provides a consistent block-level image of a file system at a given point in time. The snapshot stays stable even if the file system that the snapshot was taken from continues to change. The snapshot can then be used to create a backup of the file system at the time the snapshot was taken. The snapshot also provides the capability to access files or directories as they were at the time of the snapshot.

- ▶ Large file system capacity (see Table 4-16)

- ▶ Large files

Table 4-16 AIX 5L JFS and JFS2

Function	JFS	JFS2
Architectural maximum file system size	1 terabyte (TB)	4 petabyte (PB)
Architectural maximum file size	64 GB	4 PB
Number of i-nodes	Fixed, set at file system creation	Dynamic
i-node size	128 bytes	512 bytes
Fragment size	512 bytes	512 bytes
Block size	4096 bytes	4096 bytes
Directory organization	Linear	B-Tree

Function	JFS	JFS2
Compression	Yes	No
Default ownership at creation	sys.sys	root.system
Set Group ID (SGID) of default file mode	SGID=on	SGID=off
Quotas	Yes	Yes

JFS and JFS2 can coexist on the same systems.

If you migrate data from a JFS to a JFS2, back up the JFS and restore the data in JFS2.

Creating, changing, and removing the file systems

This section provides examples for creating, changing, and removing the file systems.

Example 4-29 shows how to create a new file system.

Example 4-29 Creating a new file system

```
# crfs -v jfs2 -g itsovg -m /test -a size=100M
File system created successfully.
130864 kilobytes total disk space.
New File System size is 262144
# mount /test
# df -k /test
Filesystem      1024-blocks      Free %Used      Iused %Iused Mounted on
/dev/fslv00      131072           130724    1%           4      1% /test
```

Example 4-30 shows how to change the file system size.

Example 4-30 Changing a file system size

```
# df -k /test
Filesystem      1024-blocks      Free %Used      Iused %Iused Mounted on
/dev/fslv00      131072           130724    1%           4      1% /test
# chfs -a size=50M /test
Filesystem size changed to 131072
# df -k /test
Filesystem      1024-blocks      Free %Used      Iused %Iused Mounted on
/dev/fslv00      65536            65196    1%           4      1% /test
```

Example 4-31 shows how to remove a file system.

Example 4-31 Removing a file system

```
# umount /test
# rmfs -r /test
rmlv: Logical volume fslv00 is removed.
```

Checking file system consistency

The **fsck** command checks file system consistency and interactively repairs the file system. Do not run the **fsck** command on a mounted file system. You must be able to read the device file on which the file system resides. The **fsck** command tries to repair file system metadata structures, displays information about the inconsistencies found, and prompts you for permission to repair them.

It does not, however, recover data from the data blocks. If you have lost data, you must restore it from a backup.

Orphaned files and directories detected by the **fsck** command are placed under the `lost+found` directory located in the root directory of the file system.

When the system boots, the **fsck** command is called to verify the `/`, `/usr`, `/var`, and `/tmp` file systems. An unsuccessful result prevents the system from booting.

Example 4-32 shows how to check the file system for consistency.

Example 4-32 Checking the file system consistency

```
#df -k /test
Filesystem      1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/lv00        16384           15828    4%         17     1% /test
#umount /test
#fsck /test
** Checking /dev/r1v00 (/test)
** Phase 1 - Check Blocks and Sizes
** Phase 2 - Check Pathnames
** Phase 3 - Check Connectivity
** Phase 4 - Check Reference Counts
** Phase 5 - Check Inode Map
** Phase 6 - Check Block Map
8 files 1112 blocks 31656 free
#mount /test
#df -k /test
Filesystem      1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/lv00        16384           15828    4%         17     1% /test
```

Defragmenting file systems

Use the **defragfs** command to improve or report the status of contiguous space within a file system. Example 4-33 shows an example of using **defragfs** to defragment the /home file system.

Example 4-33 File system defragmenting

```
#defragfs /home
statistics before running defragfs:
number of free fragments 31318
number of allocated fragments 1450
number of free spaces shorter than a block 1
number of free fragments in short free spaces 1

statistics after running defragfs:
number of free spaces shorter than a block 1
number of free fragments in short free spaces 1

other statistics:
number of fragments moved 11
number of logical blocks moved 11
number of allocation attempts 11
number of exact matches 0
#
```

File system organization

The file system or directory structure for OS files is similar on Solaris and AIX 5L. Table 4-17 shows a summary of this organization on a default installation.

Table 4-17 Directories organization

File system or directory	Solaris	AIX 5L
/	Root file system	Root file system
/etc	Configuration files	Configuration files
/dev	Special device files	Special device files
/var	Logs and spool area	Logs and spool area
/opt	Application and Solaris packages area	Application area
/tmp	Temporary files and swap area	Temporary files

File system or directory	Solaris	AIX 5L
/usr/bin	OS commands and shell scripts	OS commands and shell scripts
/bin	Symbolic link for /usr/bin	Symbolic link for /usr/bin
/sbin	Files used on initialization process	Files used on initialization process
/export/home	Home area	N/A
/home	N/A	Home area
/proc	Virtual file system for processes management	Virtual file system for processes management
/lib	Symbolic link for /usr/lib	Symbolic link for /usr/lib
/u	N/A	Symbolic link for /home

4.10 Migration from physical disks partition to AIX 5L

If you work with only physical disk partitions on Solaris without Solaris Volume Manager or Veritas Volume Manager, you will see a new and powerful environment on AIX 5L.

Table 4-18 shows the basic advantages in LVM administration.

Table 4-18 Physical disk and LVM management

Task	Solaris with physical disk partition	LVM on AIX 5L
Concat and stripe volume management	N/A	Available
Online file system management for size extension and reduction	N/A	Available
Mirror management	N/Z	Available

For information about migration from physical partition to LVM on AIX 5L, and about detailed LVM documentation, refer to 4.5, “Logical Volume Manager administration on AIX 5L” on page 96.

4.11 Migration from Solaris Volume Manager to AIX 5L

Solaris Volume Manager is a new implementation of the Solstice™ DiskSuite™. The main difference is that Sun Volume Manager works with soft partitions.

4.11.1 Concepts

This section discusses two concepts.

Replicas

In Solaris Volume Manager, all the information about the volumes' structures are saved on a disk area called replica.

On AIX 5L, the LVM information is saved automatically in different places during LVM administration. The disk area that we can compare with replicas on Solaris is called VGDA, VGSA, and LVCB on AIX 5L. For more information about these areas on AIX 5L, refer to 4.5.1, "Logical Volume Manager configuration data" on page 97.

Import and export

On Sun Volume Manager, there are no import and export concepts as on AIX 5L.

In a storage migration between different servers, it is a good practice to save the meta devices configuration in a file, and re-create on the new host.

The disk names on a new server must be exactly the same. Otherwise, you must edit the file before a new initialization.

For more information, refer to Appendix A, "Tasks reference" on page 457, and "Disk and file system management" on page 484.

4.11.2 Commands

To compare commands, refer to Table 4-19.

Table 4-19 Solaris VM and LVM on AIX 5L

Volume management task	Solaris VM	AIX 5L
Create a volume group	N/A	mkvg
Create a logical volume	metainit volumename raidtype devices...	mklv

Volume management task	Solaris VM	AIX 5L
Enable the volume or volume group	N/A	varyonvg
Disable the volume or volume group	N/A	varyoffvg
Export a volume group	N/A	exportvg
Delete the volume or volume group	metaclear	rmlv
Add a device to the volume or volume group	metattach or metainit	extendvg
Delete a device from the volume or volume group	metadetach	reducevg
Create a soft partition or logical volume (no Redundant Array of Independent Disks (RAID))	metainit -p	mklv (see options on man pages)
Create a soft partition or logical volume (RAID 0)	metainit with RAID 0 on devices first, then metainit -p to create the soft partition volume	mklv (see options on man pages)
Create a soft partition or logical volume on a specific device	Same as above, but the 2nd metainit -p will have the devicename at the end of the command line	mklv (see options on man pages)
Delete a soft partition or logical volume	metaclear	rmlv
Extend a volume or logical volume	metadetach Volname devicename	extendlv
Extend a file system after volume has been grown	growfs	chfs
Reduce a volume or logical volume	metadetach Volname devicename	chfs

4.12 Migration from Veritas Volume Manager

In this scenario, you work with a tool for volume management and you have two options for migration.

The first is to install the VxVM on AIX 5L. This is useful because the management is similar in AIX 5L and Solaris. In this case, you must have more facilities for data migration without copies (depending on the version and the configuration on VxVM).

VxVM is a part of the Veritas Foundation Suite. For more information about the Veritas Foundation Suite on AIX 5L, refer to *Introducing VERITAS Foundation Suite for AIX*, SG24-6619.

The second possible scenario is a migration for VxVM to AIX 5L Volume Manager. For this migration, it is crucial that you refer to 4.12.1, “Concepts” on page 130.

4.12.1 Concepts

LVM and VxVM use the terms shown in Table 4-20 to specify their various components.

Table 4-20 Veritas and LVM terminology

AIX 5L LVM	VxVM
Physical Volume	Disk Media
Volume Group	Disk Group
Physical Partition	Subdisks
Logical Partition	Plex
Logical Volume	Volume
Logical Volume Mirror	Logical Partition Copies

Disk or Physical Volume

The disks on the VxVM are disks or dm. When you initialize one disk on VxVM, the disk name is changed, and the new name is used for Veritas tasks.

Disk Group or Volume Group

People who work with VxVM use the term disk group. However, in AIX 5L, this concept is referred to as a VG. These two terms mean the same thing.

On AIX 5L LVM, the disks are called physical volumes.

Subdisk or Physical Partition

The VxVM works with subdisks that are the regions of a physical disk. The reference on AIX 5L are Physical Partitions. These are different from Veritas. On AIX 5L LVM, you specify the Physical Partition size on VG creation.

Logical Partition or Plex

On Veritas, a Plex is a series of Subdisks linked together in an address space. The equivalent layer in AIX 5L is called Logical Partition.

Volume or Logical Volume

In the VxVM, the term Volume specifies a separated group of Logical Partitions that belong to a VG. On AIX 5L, this component is called Logical Volume, and is usually associated with a file system.

4.12.2 Commands

To compare commands, refer to Table 4-21.

Table 4-21 VxVM and LVM on AIX 5L

Task	VxVM	LVM on AIX 5L
Administration tool	<code>vxdiskadm</code> or <code>vea</code>	<code>smit lvm</code> or <code>wsm</code>
Check license	<code>vxlicrep</code>	No licence required
See disks	<code>vxdisk list</code>	<code>lspv</code>
Add a new disk	<code>vxdiskadd</code>	<code>extendvg</code>
Migrate a disk	<code>vxevac</code>	<code>migratepv</code>
Migrate a logical partition to another disk	N/A	<code>migratelp</code>
Start a volume	<code>vxvol start</code>	You put the VG online with <code>varyonvg</code>
Stop a volume	<code>vxvol stop</code>	You put the VG offline with <code>varyoffvg</code>

Task	VxVM	LVM on AIX 5L
List disk groups or volume groups	<code>vxvg list</code>	<code>lsvg</code>
Display information about disk group	<code>vxprint</code>	<code>lsvg</code>
Create a disk group	<code>vxvg init</code>	<code>mkvg</code>
Export a disk group or volume group	<code>vxvg deport</code>	<code>exportvg</code>
Import a disk group or volume group	<code>vxvg import</code>	<code>importvg</code>
Remove a disk from a disk group	<code>vxvg -g dname rmdisk</code>	<code>reducevg</code>
Add a disk to a disk group	<code>vxdiskadd</code>	<code>extendvg</code>
Display information about logical volume	<code>vxprint</code>	<code>lslv</code>
Create a logical volume	<code>vxassist make</code>	<code>mklv</code>
Extend a logical volume	<code>vxassist growto</code> or <code>vxassist growby</code>	<code>extendlv</code>
Change a logical volume setting	<code>vxedit set</code>	<code>chlv</code>
Remove a logical volume	► <code>vxassist remove</code> ► <code>vxedit rm</code>	<code>rm1v</code>
Report statistics for volumes	<code>vxstat</code>	<code>lvmstat</code>
Extend a file system	<code>vxresize</code>	<code>chfs</code>
Shrink a file system	<code>vxresize</code>	<code>chfs</code>
Mirror a logical volume	<code>vxassist</code> or <code>vxmirror</code>	<code>mk1vcopy</code> or <code>mirrorvg</code>



Software management

This chapter describes how to manage software packages and patches in AIX 5L. In this context, software management includes the operating system (OS) and any software that runs on the OS.

This chapter discusses the following topics:

- ▶ 5.1, “Packages” on page 134
- ▶ 5.3, “Patching” on page 146
- ▶ 5.5, “Dependencies” on page 150
- ▶ 5.5.3, “Package distribution methods” on page 151
- ▶ 5.6, “Automated software management” on page 151
- ▶ 5.7, “Activating the fixes after updating” on page 154
- ▶ 5.8, “Software management in clustered environments” on page 154

5.1 Packages

.A package is a collection or group of program files and subdirectories that make up a software product. A package can be a part of an OS or an add-on software for a specific functionality.

Task table

Table 5-1 shows the package management commands.

Table 5-1 Package management commands

Package management task	Solaris	AIX 5L
Install package	<code>pkgadd</code>	<code>installp -a</code>
Display installed package	<ul style="list-style-type: none">▶ <code>pkginfo</code> or▶ <code>pkgparam</code>	<code>lslpp -a</code>
Remove software package	<code>pkgrm</code>	<code>installp -u</code>
Upgrade or install package	<code>pkgadd</code>	<code>install_all_updates</code>
Verify correct installation	<code>pkgchk</code>	<code>lppchk -v</code>
List the contents of an installed package	Look in <code>/var/sadm/install/contents</code>	<code>lslpp -f fileset</code>
Check which file belongs to which package	<code>/usr/sbin/pkgchk -lp somefile</code>	<code>lslpp -w /pathname/filename</code>
Check package information	<code>pkginfo -l</code>	<code>lslpp -a grep fileset</code>

Beginning AIX 5L V5.1, you can install RPM Package Manager (RPM) and InstallShield MultiPlatform formatted packages in addition to the `installp` formatted packages. You can use the Web-based System Manager, `smitty`, or the `geninstall` command to install and uninstall these type of packages. The `geninstall` command can detect the format type of a specified package and run the appropriate installation command. If you use the `geninstall` command from the command line to install the RPM or the InstallShield MultiPlatform packages, use the prefix type to indicate to the `geninstall` command the type of package that you are installing. Following are the package prefix types:

- ▶ I: `installp` format
- ▶ R: RPM format
- ▶ J: InstallShield MultiPlatform (ISMP) format
- ▶ E: interim fix format

To install the `cdrecord` package and the `bos.games` package, for example, use the following:

```
# geninstall -d/dev/cd0 R:cdrecord I:bos.games
```

Note: For RPM-based packages, the sysadmin can also use the `rpm` commands on AIX 5L.

5.1.1 Package management in Solaris

The Solaris package format is based on the System V Interface Definition for application binary interface (ABI) and has tools for managing these packages. These management tools include the ability to add and remove packages, check for consistency, and display package information. If system administrators use the `pkgadd` and `pkgrm` tools to manage packages, the tools update the software product database accordingly.

5.1.2 Package management in AIX 5L

As with Solaris, AIX 5L too has a specific terminology related to installable software. AIX 5L uses the Berkeley Software Distribution (BSD) standard. It also has the option of using the System V standard for initialization files startup. This section describes the AIX 5L terminology for installable software.

Under packaging terminology, there are four basic package concepts in AIX 5L, file set, package, LPP, and bundle.

File set

A file set is the smallest individually installable unit. It is a collection of files that provide a specific function, for example, the `bos.net.tcp.client` is a file set in the `bos.net` package.

File set naming convention

File sets follow this standard naming convention:

```
LPP.msg[.lang].package.fileset
```

LPP is the first part of every file set name, for example, all the file sets within the Base Operating System (BOS) program product will have `bos` at the beginning of their name.

If a package has only one installable file set, the file set name might be the same as the package name, for example, `bos.INed`.

Following is a list of the standard file set suffixes:

- ▶ .adt
Application Development Toolkit for the licensed program product
- ▶ .com
Common code between two similar file sets
- ▶ compat
Compatibility code that will be removed in a future release of the licensed program product
- ▶ .data
/usr/share portion of a file set
- ▶ .dev
Device support for the licensed program product
- ▶ .diag
Diagnostics for a file set
- ▶ .fnt
Font portion of a file set
- ▶ .help[lang]
Translated help files for the licensed program product
- ▶ .loc
Locale for the licensed program product
- ▶ .mp
Multiprocessor-specific code for a file set
- ▶ .msg[lang]
Translated messages
- ▶ .rte
Runtime or minimum set
- ▶ .smit
SMIT tools and dialogs for a file set
- ▶ .ucode
Microcode for a file set
- ▶ .up
Uniprocessor-specific code for a file set

With the message libraries associated with LPPs, the language is also a part of the naming convention.

Package names

Following are the examples of the major packages in the AIX 5L BOS:

- ▶ **bos.acct**
Accounting services. Contains accounting services that support or enhance the BOS.
- ▶ **bos.adt**
Base Application Development Toolkit. Contains commands, files, and libraries that are required to develop software applications.
- ▶ **bos.diag**
Hardware diagnostics. Contains the Diagnostic Controller for the hardware diagnostics package.
- ▶ **bos.docregister**
Documentation registration tools. Contains the utilities used in the administration of the Hypertext Markup Language (HTML) documentation options and their associated search indexes.
- ▶ **bos.docsearch**
Documentation library service. Provides functions that allow users to navigate, read, and search HTML documents that are registered with the library service.
- ▶ **bos.dosutil**
Disk operating system (DOS) utilities. Contains DOS file and disk utilities for handling DOS diskettes.
- ▶ **bos.iconv**
AIX 5L language converters. Converts data from one code set designation to another code set. This can be used to represent data in a given locale.
- ▶ **bos.INed**
INed editor. Contains a full-screen text editor that supports viewing, entering, and revising text at any location in the editor window.

- ▶ `bos.loc`
AIX 5L localization. Contains support for applications to run using the cultural conventions of a specific language and territory. These conventions include date and time formatting, collation order, monetary and numeric formatting, language for messages, and character classification. Where applicable, additional software such as input methods and fonts that are required to display and process characters of a specific language are also included.
- ▶ `bos.mh`
Mail handler. Contains commands to create, distribute, receive, view, process, and store mail messages.
- ▶ `bos.net`
BOS network facilities. Provides network support for the OS. Includes TCP/IP, Point-to-Point Protocol (PPP), Network File System (NFS), Cache File System (CacheFS), Automount File System (AutoFS), Network Information Services (NIS), Network Information Services+ (NIS+), UNIX-to-UNIX Copy (UUCP), and Asynchronous Terminal Emulator (ATE).
- ▶ `bos.perf`
Base performance tools. Contains two file sets for identifying and diagnosing performance problems.
- ▶ `bos.powermgt`
Power management software. Controls electric power consumption features such as system standby, device idle, suspend, and hibernation on models that support these features.
- ▶ `bos.rte`
BOS runtime. Contains the set of commands that are required to start, install, and run AIX 5L.
- ▶ `bos.sysmgt`
System management tools and applications. Contains system management functions relating to installation, system backup, error logging, and trace.
- ▶ `bos.terminfo`
Base AIX 5L terminal function. Contains description files used by curses libraries for various terminals.
- ▶ `bos.txt`
Text formatting services. Contains services for formatting and printing documents.

Licensed program product

This is a complete software product collection, including all the packages and file sets that are required. Licensed program products (LPP) are separately orderable products that run on the AIX 5L OS, for example, IBM DB2®, IBM CICS®, IBM Tivoli Storage Manager, and so on.

File set names are designed to describe the contents of a file set, for instance, all the file sets within the BOS program product will have *bos* at the beginning of their name.

Bundles

It is a difficult task to figure out which individual file set you want to install on your machine. For this, AIX 5L offers a collection of file sets as a bundle that match a particular purpose, for example, if you are developing applications, the App-Dev bundle is the logical choice to install.

A bundle is a collection of packages and file sets suited for a particular environment. AIX 5L bundles are quite similar to AIX 5L bundles.

Following are the predefined system bundles in AIX 5L V5.3:

- ▶ App-Dev
- ▶ Common Desktop Environment (CDE)
- ▶ GNU Network Object Model Environment (GNOME)
- ▶ KDE
- ▶ Media-defined
- ▶ Netscape
- ▶ Devices
- ▶ wsm-remote

When you install a bundle, some of the file sets are installed if the prerequisite hardware is available, for example, a graphic adapter is required to run CDE.

In some cases, bundles are equivalent to product offerings. Often, however, they are a subset of a product offering or a separate customized bundle. The bundles available might vary from configuration to configuration.

The standard bundle definitions that control what selections appear in the System Management Interface Tool (SMIT) or the Web-based System Manager, are stored in `/usr/sys/inst.data/sys_bundles`.

5.2 AIX 5L Base Operating System

The AIX 5L BOS licensed program includes the AIX 5L OS, languages, device drivers, system management tools, utilities, and other file sets.

The AIX 5L V5.3 OS is delivered on multiple CDs or on DVDs. These include:

- ▶ AIX 5L BOS
- ▶ Bonus pack
- ▶ Expansion pack
- ▶ AIX 5L documentation
- ▶ AIX 5L toolbox for Linux applications

5.2.1 Bonus pack and expansion pack

The contents of the bonus pack and the expansion pack vary from time to time. The main purpose of these packs is to acquaint users with the tools and products that may be valuable in their business environment. The AIX 5L V5.3 expansion and bonus packs, for example, contain tools to build secure Java application Data Encryption Standard (DES) library routines, software security, and encryption support, network authentication aervice, IBM HTTP Server, and so on.

5.2.2 Software updates

As new software is created for AIX 5L, you will want to upgrade your system to maintain the latest features and functionality.

A *maintenance level* consists of one file set update for each file set that has changed since the base level of AIX 5L V5.3. Each of these file set updates is cumulative, containing all the fixes for that file set since the time AIX 5L V5.3 was introduced, and supersedes all the earlier updates for the same file set.

With the `oslevel` command, you can obtain the OS level you are running, for example:

```
# oslevel
5.3.0.0
```

This outputs indicates that the current maintenance level is Version 5, Release 3, Modification 0, and Fix 0.

The `oslevel -r` command tells you which maintenance level you have:

```
# oslevel -r
5300-02
```


The output shows that you are at maintenance level 2.

Note: All the versions and release levels must be bought. However, modification and fix-level upgrades are available at no charge.

To learn about version and release upgrades, refer to Chapter 3, “Operating system installation” on page 47.

5.2.3 Software states under AIX 5L

In an AIX 5L environment, it is important to know about the different software states.

Applied state

When a service update is installed or applied, it enters the applied state and becomes the currently active version of the software. When an update is in the applied state, the earlier version of the update is stored in a special save directory. The applied state provides you the opportunity to test the newer software before committing to its use. If it works as expected, you can commit the software, which will remove the earlier version from the disk.

Commit state

When you commit a product update, the saved files from all the earlier versions of the software product are removed from the system, thereby making it impossible to return to an earlier version of the software product. This means that there is only one level of that software product installed on your system.

With committed (or applied) software products, you can also remove them. This causes the product's files to be deleted from the system. Requisite software (software dependent on this product) will also be removed unless it is required by some other software product on your system. If you want to use the software again, you will have to reinstall it.

5.2.4 Installing software under AIX 5L using smitty

This section describes how to install additional software in the AIX 5L environment.

Use the **smitty install_update** fast path to access the screen shown in Figure 5-1.

```
Install and Update Software

Move cursor to desired item and press Enter.

Install Software
Update Installed Software to Latest Level (Update All)
Install Software Bundle
Update Software by Fix (APAR)
Install and Update from ALL Available Software

F1=Help          F2=Refresh      F3=Cancel      F8=Image
F9=Shell        F10=Exit       Enter=Do
```

Figure 5-1 The Install and Update Software screen

Following is a description of two of the options provided in this screen:

► Install software

Selecting this option enables you to install all the latest software, or selectively install some or all the individual software products that exist on the installation media (or directory). You can also use this menu if you are reinstalling a currently installed software product. If a product is reinstalled at the same level or at an earlier level, only the base product (no updates) is installed. This is commonly used to install optional software that is not currently installed on your system.

► Install and update from all available software

Selecting this option enables you to install or update software from all the software available on the installation media. Use this menu when none of the other menus that limit the available software in some way fit your requirements. In general, the software list in this menu is longer than in the menus that are tailored to a specific type of installation.

On selecting **Install Software**, the screen shown in Figure 5-2 opens.

```

                                Install Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry
Fields]
* INPUT device / directory for software          /dev/cd0
* SOFTWARE to install                            [_all_latest]
+
  PREVIEW only? (install operation will NOT occur)  no
+
  COMMIT software updates?                          yes
+
  SAVE replaced files?                              no
+
  AUTOMATICALLY install requisite software?         yes
+
  EXTEND file systems if space needed?              yes
+
  OVERWRITE same or newer versions?                 no
+
  VERIFY install and check file sizes?              no
+
  Include corresponding LANGUAGE filesets?          yes
+
  DETAILED output?                                  no
+
  Process multiple volumes?                          yes
+
  ACCEPT new license agreements?                     no
+
  Preview new LICENSE agreements?                   no
+

F1=Help          F2=Refresh          F3=Cancel        F4=List
F5=Reset         F6=Command         F7=Edit          F8=Image
F9=Shell         F10=Exit           Enter=Do
```

Figure 5-2 Install Software screen

Specify the software to be installed either by choosing the default setting (`_all_latest`) or by selecting from a list. Press F4 to access the list, provided the CD-ROM is inserted into the CD drive. It is also possible to install software from a disk.

The Preview option indicates whether you want to preview the installation of the selected software products and updates without actually performing software installation. A preview identifies the requirements for a software installation to be successful.

Committing software has two effects, it frees up the disk space used to store earlier versions of that software, and eliminates the possibility of being able to reject the update and go back to the earlier version.

Selecting **no** instructs the system *not* to commit the software updates you are installing. The software you are installing will be applied. When the software is applied to the system, it becomes the active version of the software. If it is replacing an earlier version of the software, the earlier version is saved in a special directory on the disk. The earlier version can be retrieved, if necessary, by rejecting the current version. After you are satisfied with the updates, commit them in order to free up the disk space used by the saved files. If you select **no**, select **SAVE replaced files**.

5.2.5 Installing optional software using the Web-based System Manager

This section provides information about using the Web-based System Manager to install the optional software.

The graphic interface provides access to the Web-based System Manager options for installing the following:

- ▶ Optional software
- ▶ Service updates
- ▶ Software bundles

The Web-based System Manager allows you to install software and to change the system's default install settings and specify other options. By default, the Web-based System Manager applies and commits any software updates you are installing. However, you can change this default setting and have the software updates only applied.

Note: Base software applications are always committed. If an earlier version of the software is installed, it cannot be saved.

Perform the following tasks to install the optional software, using the Web-based System Manager (Figure 5-3):

1. Start the Web-based System Manager by typing `wsm` in the command line.
2. Expand the machine name.
3. Expand **Software** in the Navigation area.
4. Select **Overview and Tasks**.
5. Select **Install Software**.

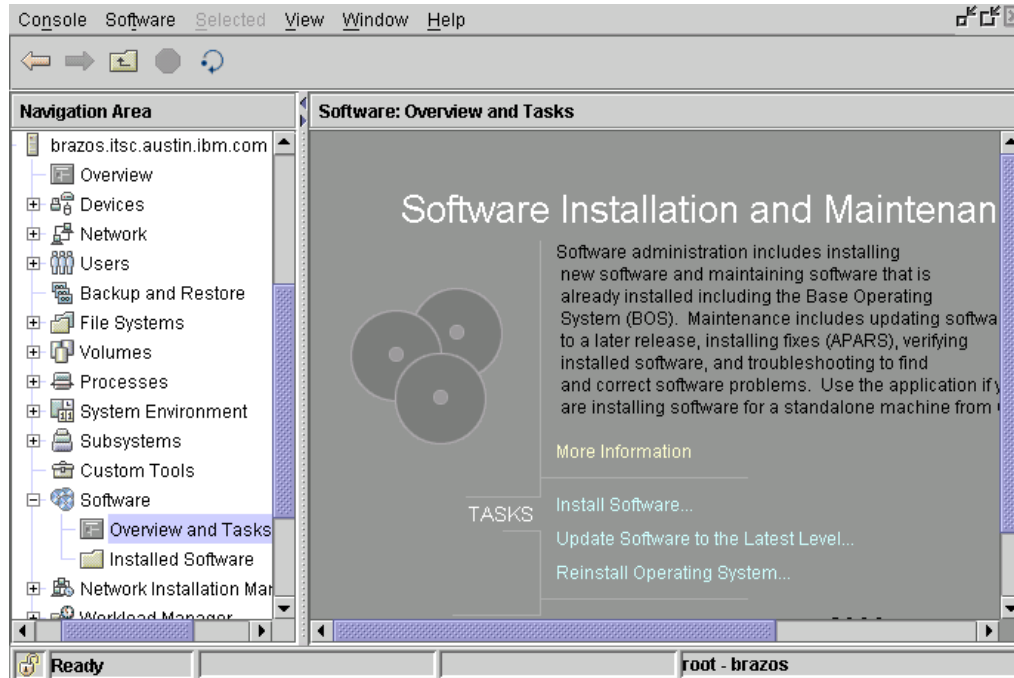


Figure 5-3 Installing optional software with the Web-based System Manager

Installing service updates with Web-based system Manager

Repeat the steps described in the previous section (5.2.5, “Installing optional software using the Web-based System Manager” on page 144), and after completing step 5, select **Update Software to the latest level**.

Installing software bundles with Web-based System Manager

Perform the following tasks:

1. Follow the steps 1, 2, and 3 described in the section 5.2.5, “Installing optional software using the Web-based System Manager” on page 144.
2. Select **Installed Software**.

3. From the Software menu, select **New Software (Install/Update)** → **Install Bundles (Easy)**.

Tip: To perform software and patch installation and updates without manually transferring the packages to each system, configure one server as a Network Installation Manager (NIM) Master. You can then define the machines as clients of this Master. With the appropriate configuration, you can use the NIM Master as a single push or pull point for installation of software packages or patches. This eliminates the requirement to manually move the installation media from machine to machine, either physically or through direct NFS.

5.3 Patching

A patch is a subset of a package that adds new functionality to a package or fixes a problem with the installed package.

Table 5-2 shows the patch management commands.

Table 5-2 Patch management commands

Patch management task	Solaris	AIX 5L
Install a patch	<code>patchadd</code>	<code>instfix -i</code>
Remove a patch	<code>patchrm</code>	<code>installp -r</code> (if applied but not committed) or <code>smitty reject</code>
Display installed patches	<code>showrev -p</code>	<code>instfix -ia</code>

5.3.1 Patching in Solaris

Patches in Solaris are handled using the `patchadd`, `patchrm`, and `showrev` commands.

The last two digits of the patch file name show the revision level.

5.3.2 Patching in AIX 5L

As new software is created for AIX 5L, upgrade your system to maintain the latest features and functionalities.

The numerical information that shows the level of software you have currently installed is broken into four parts, version, release, modification, and fix. You can see this information using the `oslevel` command, for example, 5. 3. 0. 0 means Version 5, Release 3, Modification 0, Fix 0.

Note: Version and release upgrades must be bought. Modification and fix-level upgrades are available at no charge.

5.4 Maintenance levels

A maintenance level consists of one file set update for each file set that has changed since the base level of AIX 5L V5.x. Each of these file set updates is cumulative, containing all the fixes for that file set since AIX 5L V5.x was introduced, and supersedes all the earlier updates for the same file set.

You can determine which maintenance level is installed, by using the `oslevel -r` command. At the time of writing this IBM Redbook, the maintenance level for AIX 5L V5.3 was 5300-04.

Recommended maintenance level

A recommended maintenance level is a set of file set updates that apply to the last maintenance level. Recommended maintenance packages are made up of field-tested file set updates, and provide a mechanism for delivering preventive maintenance packages between full maintenance levels.

Obtaining maintenance level

For AIX 5L, download the fixes from the following IBM Web site:

<http://www-03.ibm.com/servers/eserver/support/unixservers/aixfixes.html>

Installing maintenance levels and fixes

There are two ways to install maintenance levels and fixes. The easiest way to install them is to use the SMIT.

To install the maintenance levels and fixes, use the following procedure:

1. Download the fix from the following Web site:

<http://www-03.ibm.com/servers/eserver/support/unixservers/aixfixes.html>

2. Uncompress and untar the software.
3. Type **smitty update_all**.
4. From this point, follow the instructions on the screen to install the fix (Figure 5-4).

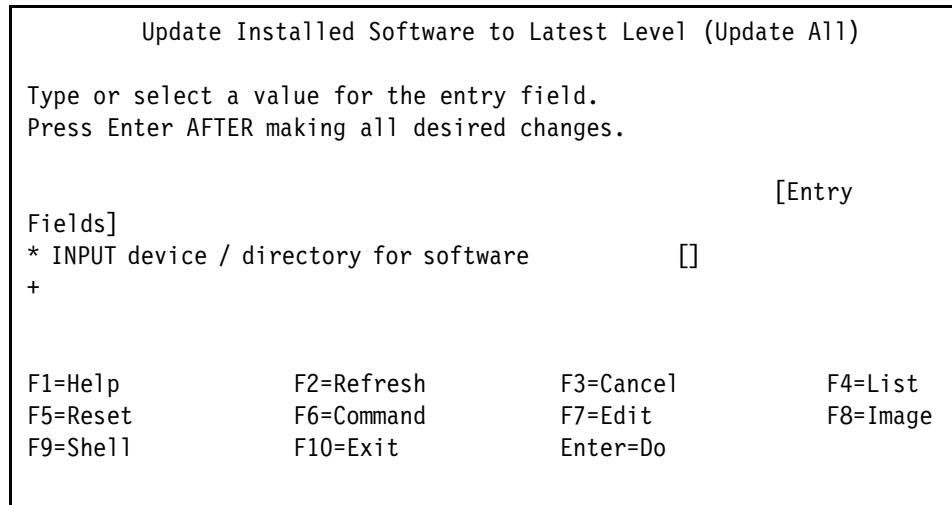


Figure 5-4 Update Installed

A second option to install the fixes is to use the **instfix** command. The **instfix** command allows you to install a fix or a set of fixes without knowing any information other than the Authorized Program Analysis Report (APAR) number or other unique key words that identify the fix.

Any fix can have a single file set or multiple file sets that comprise that fix. Fix information is organized in the Table of Contents (TOC) on the installation media. After a fix is installed, fix information is kept on the system in a fix database.

The **instfix** command can also be used to determine if a fix is installed on your system.

To install a patch with the **instfix** command, perform the following tasks:

1. Download the fix from the IBM Web site:
<http://www-03.ibm.com/servers/eserver/support/unixservers/aixfixes.html>
2. Uncompress and untar the software archive.
3. From the current directory, type the following command:

```
# instfix -T -d . | instfix -d . -f -
```


If you want to install only a specific fix, type the following command:

```
# instfix -k <Fileset> -d
```

Removing a fix

On AIX 5L, you can either use the **installp -r** command or the **smitty reject** fast path (Figure 5-5).

When you reject an applied service update, the update files are removed from the system and the earlier version of the software is restored. Only service updates in the applied state can be rejected.

To reject a service update using SMIT, type the **smitty reject** fast path on the command line.

```
Reject Applied Software Updates (Use Previous Version)

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]
* SOFTWARE name                []
+
  PREVIEW only? (reject operation will NOT occur)    no
+
  REJECT dependent software?                        no
+
  EXTEND file systems if space needed?              yes
+
  DETAILED output?                                  no
+

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command          F7=Edit           F8=Image
F9=Shell         F10=Exit            Enter=Do
```

Figure 5-5 *Reject Applied Software Updates screen*

In the input field, specify the package, for example, IY19375, and press Enter. This brings up another screen, from where you can control the deletion process.

You can also use the `installp -r` command to remove a fix, but this is a complex command, and if you are not familiar with AIX 5L, it is not recommended.

Interim fixes

When resolution to a problem cannot wait for a generally available fix, IBM will provide corrections in the form of an interim fix. The interim fix management solution allows users to track and manage interim fixes on systems running AIX 5L. The solution consists of the interim fix manager, the interim fix packager, and the associated SMIT screens.

Following are the benefits:

- ▶ Uses a common installation procedure. No more unique installation procedures per fix.
- ▶ The system keeps track of the applied fixes and prevents accidental overwriting of the interim fix by a generally available fix.
- ▶ Easy-to-use preview, installation, list, verification, and removal services
- ▶ Option to install the interim fix so that it is automatically unavailable at reboot.

For more information, refer to the following Web site:

<http://www14.software.ibm.com/webapp/set2/sas/f/aix.efixmgmt/home.html>

5.5 Dependencies

In certain situations, a package or patch will have a dependency on one or more packages or patches before it can be installed.

5.5.1 Dependency management in Solaris

A Solaris system administrator has several options for resolving package dependencies:

- ▶ Manual, that is, an individual package or patch
- ▶ A patch cluster that already contains most of what is required for the core OS
- ▶ An automated patch manager (refer to 5.6, “Automated software management” on page 151).

Each of these options has certain considerations that must be taken into account according to the requirements of the system administrator, for example, to target a specific issue, only downloading the required patches and its prerequisites is

required. However, consider a cluster patch when there is a requirement to ensure that the key components of the OS are all up to date.

5.5.2 Package dependencies in AIX 5L

If an AIX 5L system administrator uses the `installp` command with the `-g` flag specified, it automatically installs or commits respectively, any software products or updates that are the requisites of the specified software product. When used to remove or reject software, this flag automatically removes or rejects dependents of the specified software. The `-g` flag is not valid when used with the `-F` flag.

Note: The `-g` flag also automatically pulls in a superseding update that is present in the media if the specified update is not present. This flag causes the newest update to be installed for a given file set when there are multiple superseding updates for the same file set on the installation media.

5.5.3 Package distribution methods

Solaris has the SunSolve Web site for retrieving distributed packages and patches.

AIX 5L too has Web sites that provide the necessary facilities for package distribution:

- ▶ <http://www-03.ibm.com/servers/eserver/support/unixservers/syp5/downloadingwaix.html>
- ▶ <http://www-03.ibm.com/servers/eserver/support/unixservers/aixfixes.html>

5.6 Automated software management

Automated software management is an easy way of updating a system without having to individually check through each patch or package for dependencies and requirements.

5.6.1 Automated software management in Solaris

There are several options available from the SunSolve Web site for automated software management. The software in this context refers only to patches, and not packages. The options include:

- ▶ Patch Manager for Solaris 8 and 9

- ▶ PatchPro Interactive
- ▶ PatchPro Expert

These tools generate a complete list of patches based on your current system, which includes patches for software components that are installed on the system, but are not being used. Some of these tools enable you to select from the generated list so that you can target only specific software components.

5.6.2 Automated software management in AIX 5L

In AIX 5L V5.3, there are a number of ways in which to automate software management:

- ▶ Service Update Management Assistant (SUMA)
- ▶ NIM

Service Update Management Assistant

The SUMA moves the system administrator away from the manual task of retrieving maintenance updates from the Web. SUMA, which is included in the base AIX 5L V5.3 OS, provides clients with flexible policy-based options, allowing them to perform unattended downloads of all AIX 5L updates from the IBM eServer support Web site:

<http://www-03.ibm.com/servers/eserver/support/unixservers/aixfixes.html>

It allows automation of common tasks such as downloading a specific update when it becomes available, downloading the latest security updates, or downloading an entire maintenance level. A scheduling model is utilized to allow policies to be run at various intervals in order to conform to a client's maintenance window.

SUMA policies can be run without extensive configuration. Filtering options allow comparisons against an installed software inventory, a fix repository, or a maintenance level to ensure that only the required fixes are downloaded. SUMA provides the option to send an e-mail notification containing a list of what is available for download and the detailed summary statistics of a download. The technology offered by SUMA assists in moving clients toward an autonomic maintenance strategy by automating the download of software maintenance updates that allow clients to take advantage of the increased security and reliability benefits of having correct fixes, and the cost benefits that result from spending less time on system administration.

For more information, visit the following Web site:

<http://www-03.ibm.com/servers/aix/whitepapers/suma.pdf>

Network Installation Manager

If you have a large number of servers, instead of running SUMA on them individually, consider using NIM for custom software installation. If, for example, you have a NIM Master server set up, and 20 other servers that are defined NIM clients are running AIX 5L V5.3 ml03, and you want to upgrade all 20 clients from maintenance level 03 to level 04, perform the following tasks:

1. Download the maintenance level files to the NIM server, for example, `/mnt/patches/aix/530/ml0304`.
2. Create an `lpp_source` from the downloaded maintenance level files (Example 5-1). The `packages` attribute must be used for defining the resources that do not contain enough file sets to have the `simages` attribute (refer to the NIM manual for more information). (`installp` and `awk` are used to list the file sets that are available in the source directory.)

Example 5-1 Creating an lpp_source

```
nim -o define -t lpp_source -a server=master -a \  
source=/mnt/patches/aix/530/ml0304 -a \  
location=/export/nim/lpp_source/aix530_ml0304_lpp -a \  
packages="" installp -L -d /mnt/patches/aix/530/ml4fixes | awk -F: \  
{print $1}' "" aix530_ml0304_lpp
```

3. Use the `cust` operation to install from the `lpp_source`:

```
nim -o cust lpp_source=aix530_ml4fixes -a filesets='all' client1 \  
client2 ...
```

Installing RPM packages using NIM

To install an RPM package using NIM, perform the following tasks:

1. Take an rpm package and add it to an existing `lpp_source`, for example, copy the `vnc rpm` package into `/export/nim/lpp_source/aix530_cd_lpp/RPMS/ppc`.
2. Let NIM know about this new package by using the following:

```
nim -o check aix530_cd_lpp
```

3. Run the installation of the rpm package from the `lpp_source` to the client:

```
nim -o cust -a lpp_source=aix530_cd_lpp -a \  
filesets='R:vnc-3.3.3r1-2'
```

To learn more about using NIM, refer to *NIM from A to Z in AIX 5L*, SG24-7296.

5.7 Activating the fixes after updating

Certain packages and patches require a reboot to activate the update or fix, especially for kernel and library patches.

5.7.1 Patch activation in Solaris

Occasionally, a system has to regenerate its devices during the reboot if the fix is for driver components. In most kernel or library patches, Sun recommends installation in single-user mode. This allows the system to be immediately rebooted after applying the update, which in turn minimizes the chances of losing user data.

5.7.2 Patch activation in AIX 5L

Usually, when patches are applied to the AIX 5L system, it is sufficient to apply the `installp -c` flag. This commits the applied updates. To commit all the updates, for example, use the following command:

```
# installp -cgX all
```

Running this command commits all the updates and removes the file sets for the earlier version.

If an installation fails, the `onstallp` command cannot install the same software until you remove the file sets that succeeded in installing before the failure. Use the `installp cleanup` command as follows:

```
# installp -C
```

This removes all the file sets installed in the failed installation.

5.7.3 Verifying the integrity of the operating system

After the updates are applied, use the `lppchk` command. This determines whether or not the system is in a consistent state.

5.8 Software management in clustered environments

For clustered systems, both Solaris and AIX 5L offer software management solutions to integrate the System Administrator's jobs from multiple nodes to one central location.

5.8.1 Solaris

Solaris offers Sun Cluster software. For more information, refer to the following Web site:

<http://www.sun.com/software/cluster/index.xml>

5.8.2 AIX 5L

AIX 5L has a number of different software packages available to help organizations efficiently build, manage, and expand cluster environments, using IBM eServer pSeries servers running AIX 5L or Linux, IBM eServer xSeries® servers running Linux, or a combination. Cluster-ready software from IBM enables collections of eServer hardware to behave as a single high-performance system for users and system administrators.

Cluster systems management

Cluster systems management is designed to minimize the cost and complexity of administering clustered and partitioned systems by enabling comprehensive management and monitoring of the entire environment from a single point of control. Cluster systems management provides the following:

- ▶ Software distribution, installation, and update (OS and applications)
- ▶ Comprehensive system monitoring with customizable automated responses
- ▶ Distributed command execution
- ▶ Hardware control
- ▶ Diagnostic tools
- ▶ Management by group
- ▶ A graphical interface and a fully scriptable command-line interface

In addition to providing all the key functions for the administration and maintenance of distributed systems, Cluster systems management is designed to deliver the parallel execution that is required to manage clustered computing environments effectively. Cluster systems management supports homogeneous or mixed environments of IBM servers running AIX 5L or Linux.

For more information, refer to the following Web site:

<http://www-03.ibm.com/servers/eserver/clusters/software/csm.html>

IBM LoadLeveler

Used for dynamic workload scheduling, IBM LoadLeveler® is a distributed network-wide job management facility designed to dynamically schedule tasks

such as maximize resource utilization and minimize job completion time. Jobs are scheduled based on job priority, job requirements, resource availability, and user-defined rules to match processing requirements with resources. LoadLeveler provides consolidated accounting and reporting and supports IBM servers, including IBM eServer pSeries and IBM RS/6000 systems.

Parallel Environment for AIX 5L

Parallel Environment for AIX 5L is a comprehensive development and execution environment for parallel applications (distributed-memory, message-passing applications running across multiple nodes). It is designed to help organizations develop, test, debug, tune, and run high-performance parallel applications in C, C++, and FORTRAN on pSeries clusters. Parallel Environment runs on AIX 5L V5.2 and V5.3.

High Availability Cluster Multiprocessing for AIX 5L

High Availability Cluster Multiprocessing (HACMP) is designed to provide high availability for critical business applications and data through system redundancy and failover. HACMP constantly monitors the status of servers, networks, and applications to detect failures or performance degradation and can respond by automatically restarting a troubled application on designated backup hardware, taking care of all the network or storage connections in the process. With HACMP, customers can scale up to 32 nodes and mix and match system sizes and performance levels and network adapters and disk subsystems to satisfy specific application, network, and disk performance requirements.

High Availability Cluster Multiprocessing/Extended Distance

High Availability Cluster Multiprocessing/Extended Distance (HACM/ED) extends HACMP's high availability capabilities across geographic sites with remote data mirroring (replication) and failover using this mirrored data. This combination can maintain application and data availability even if an entire site is disabled by a disaster. HACMP/XD provides IP-based data mirroring and supports hardware-based mirroring products such as IBM Enterprise Storage Systems Metro-Mirror (earlier called "PPRC").



Device management

This chapter provides a description of common tasks for managing devices in AIX 5L.

This chapter includes the following topics:

- ▶ 6.1, “Device access and configuration” on page 158
- ▶ 6.3, “Listing device information” on page 160
- ▶ 6.4, “Adding a device” on page 165
- ▶ 6.5, “Modifying a device” on page 170
- ▶ 6.6, “Removing a device” on page 173
- ▶ 6.7, “Alternate disk paths (multipathing)” on page 174
- ▶ 6.8, “Device management summary” on page 180

For more information about device management in AIX 5L, refer to the IBM System p and AIX 5L Information Center, which is available on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

6.1 Device access and configuration

This section discusses the Solaris and AIX 5L name and access devices.

6.1.1 Device naming and access

AIX 5L is only a little different from Solaris in the way it represents devices on the system. Solaris uses both logical and physical names for its devices, and AIX 5L uses only a single name for each of its devices.

Table 6-1 shows device naming and access in Solaris and AIX 5L.

Table 6-1 Device naming and access: Solaris and AIX 5L

Solaris	AIX 5L	Description
/dev	/dev	Contains logical device files
/devices	Stored in the Object Data Manager (ODM) custom device class	Contains physical device files
devfsadm	<ul style="list-style-type: none">▶ cfgmgr▶ rmdev▶ mkdev	Commands that create and manage the device files

6.1.2 Solaris logical disk devices

Solaris administrators refer to disk devices by selecting the subdirectory that it is linked to (either /dev/rdisk or /dev/dsk), followed by a string of information that indicates the specific controller, disk, and slice:

```
/dev/dsk/c[1]t[2]d[3]s[4]
```

In this:

- ▶ 1 refers to the logical controller number
- ▶ 2 refers to the physical bus target number
- ▶ 3 refers to the disk number
- ▶ 4 refers to the slice or partition number

6.1.3 AIX 5L disk devices

AIX 5L administrators refer to a disk device by its *hdisk* name.

`/dev/hdisk[x]`

In this, x is the number of the hard disk.

AIX 5L device naming does not include the controller, target, or disk number in the disk device name. AIX 5L does not use a slice or partition number as Solaris does. For more information about how AIX 5L manages the disks and the file systems, refer to Chapter 4, “Disks and file systems” on page 91.

To determine the controller that an `hdisk` is on, use the `lspath` command.

6.2 Accessing devices

In Solaris, there is the concept of having a raw device logical interface name (`rdsk`) and a block device logical interface name (`dsk`) for the same device. The name that a system administrator uses depends on the task. In AIX 5L, only one type of logical device name scheme is used. Table 6-2 differentiates between the commonly used commands for accessing devices by Solaris and AIX 5L.

Table 6-2 Commonly used logical device access commands in Solaris and AIX 5L

Solaris	AIX 5L
<code>df /dev/dsk/c1t0d0s0</code>	<code>df /dev/hd1^a</code>
<code>fsck /dev/rdsk/c1t3d0s4</code>	<code>fsck /dev/hd1</code>
<code>mount /dev/dsk/c1t1d0s0 /mnt/1</code>	<code>mount -v jfs2 -o log=/dev/log1v00 /dev/fs1v00 /mnt</code>
<code>newfs /dev/rdsk/c0t0d1s1</code>	<code>mkfs /dev/1v01</code>
<code>prtvtoc /dev/dsk/c1t1d0s0</code>	N/A because AIX 5L does not use disk slices

a. Under AIX 5L Logical Volume Manager (LVM), devices are used for the creation of file systems, not the `hdisk` devices. Refer to Chapter 4, “Disks and file systems” on page 91.

Refer to the man pages for more information about these commands.

6.3 Listing device information

This section discusses the listing information about the devices.

6.3.1 Solaris

Following are the Solaris commands for displaying system and device configuration information:

- ▶ **prtconf**
- ▶ **sysdef**
- ▶ **dmesg**
- ▶ **prtdiag**
- ▶ **kstat**

6.3.2 AIX 5L

The **prtconf** command displays the system configuration information. This includes hardware and volume group configuration, and comprises lscfg, lspvs, lsvg -p <vg's>, and more.

A section of the **prtconf** command is shown in Example 6-1.

Example 6-1 prtconf command output

```
# prtconf | head -25
System Model: IBM,7038-6M2
Machine Serial Number: 10197AA
Processor Type: PowerPC_POWER4
Number Of Processors: 4
Processor Clock Speed: 1200 MHz
CPU Type: 64-bit
Kernel Type: 32-bit
LPAR Info: 1 NULL
Memory Size: 8192 MB
Good Memory Size: 8192 MB
Platform Firmware level: 3K041029
Firmware Version: IBM,RG041029_d79e00_r
Console Login: enable
Auto Restart: true
Full Core: false

Network Information
  Host Name: alexander
  IP Address: 22.1.1.199
```

```
Sub Netmask: 255.255.255.0
Gateway: 22.1.1.1
Name Server: 22.21.16.7
Domain Name: thelab.ibm.com
```

The other main command that is used is **lsdev**. This command queries the ODM, and is used to locate the customized devices or the predefined devices. Example 6-2 is an example of this command.

Example 6-2 lsdev output

```
# lsdev -Cc disk
hdisk0 Available 20-60-00-8,0 16 Bit LVD SCSI Disk Drive
hdisk1 Available 20-60-00-9,0 16 Bit SCSI Disk Drive
hdisk2 Available 20-60-00-10,0 16 Bit SCSI Disk Drive
hdisk3 Available 20-60-00-11,0 16 Bit SCSI Disk Drive
hdisk4 Available 20-60-00-13,0 16 Bit SCSI Disk Drive
```

In this example, the **-C** (upper case) option means that you want to query the customized section of the ODM, and the **-c** (lower case) option is used to query a class under the customized section of ODM. Following are the columns:

▶ First column

This is the name of the logical device, for example, `hdisk0`.

▶ Second column

This column shows the state of the device, for example, available or defined.

▶ Third column

This column specifies the location code for the device. The location codes consist of up to four fields of information, and they differ, based on model type. The format of the location code is `AB-CD-EF-GH`. The location code that is described here is for the Configurable High Rate Processing (CHRP) architecture, which means any multiprocessor PCI bus system. To find the architecture type for your system, use the `# bootinfo -p` command.

In the CHRP architecture, the location codes are:

– AB

This defines the bus type:

- 00 for processor bus
- 01 for ISA buses
- 04 for PCI buses

– CD

This defines the slot in which the adapter is located. If you find letters in this field instead of numbers, it means that the adapter is built-in or integrated with the system planar.

– EF

This field defines the connector ID. It is used to identify the adapter connector to which a resource is attached, for example, a Small Computer System Interface (SCSI) adapter with two ports. In adapters with only one port, this value is always 00.

– GH

This defines a port, address, memory module, or device of field-replaceable unit (FRU). GH has several meanings, depending on the resource type.

- For memory cards, this value defines a memory module. Values are 1 - 16. For modules plugged directly to the system planar, the values look as 00-00-00-GH.
- For L2 Cache, GH defines the cache value.
- For async devices, GH defines the port on the fanout box. The possible values are 0 - 15.
- For diskette drives, H defines which diskette drive (1 or 2). G is always 0.
- For SCSI devices, the location code is exactly the same for AB-CD-EF values. The only difference is in G and H, where G defines the control unit address of the device (SCSI ID) with possible values of 0 - 15, and H defines the logical unit number (LUN) for the device with possible values of 0 - 255.

All the adapters and cards are identified with only AB-CD.

Note: As mentioned earlier, the actual values in the location codes vary from model to model. For specific values, refer to the Service Guide for your model:

http://www.ibm.com/servers/eserver/pseries/library/hardware_docs/index.html

► Fourth column

This last column contains the description for the device.

As shown in Example 6-3, we query in the customized section of the ODM, looking into the adapter class. If you look at the second column, you will find that the location code only has two or three fields, instead of four. This is because it only defines the adapter slot.

Example 6-3 lsdev device descriptions

```
# lsdev -Cc adapter
sa0     Available 01-S1   Standard I/O Serial Port
sa1     Available 01-S2   Standard I/O Serial Port
sa2     Available 01-S3   Standard I/O Serial Port
siokma0 Available 01-K1     Keyboard/Mouse Adapter
fda0    Available 01-D1   Standard I/O Diskette Adapter
scsi0   Available 10-60    Wide SCSI I/O Controller
mga0    Available 20-58    GXT120P Graphics Adapter
scsi1   Available 20-60    Wide/Fast-20 SCSI I/O Controller
scsi2   Available 30-58    Wide SCSI I/O Controller
sioka0  Available 01-K1-00  Keyboard Adapter
ppa0    Available 01-R1     Standard I/O Parallel Port Adapter
tok0    Available 10-68     IBM PCI Tokenring Adapter (14101800)
ssa0    Available 10-70    IBM SSA Enhanced RAID Adapter (14104500)
ent0    Available 10-78     IBM 10/100/1000 Base-T Ethernet PCI Adapter
ent1    Available 10-80     IBM PCI Ethernet Adapter (22100020)
scraid0 Available 30-60     IBM PCI SCSI RAID Adapter
sioma0  Available 01-K1-01  Mouse Adapter
```

The other useful options for the **lsdev** command are:

► -P

This queries the predefined section of the ODM.

► -H

This flag can be used with -C or -P. It provides a long listing output with headers of all the configured or predefined (supported) devices (**# lsdev -PH**).

► -s

This can be used with -C or -P to query a specific subclass (**# lsdev -Cs scsi**).

► -l

This flag can be used to query a logical device (**# lsdev -Cl scsi0**).

AIX 5L V5.3 has two more commands to list more information about the devices:

► **lsattr**

This command is used to obtain the specific configuration attributes for a device, for example, to get the attributes of a tape drive, use the command as shown in Example 6-4.

Example 6-4 lsattr -el command and output

```
# lsattr -el rmt0
mode          yes    Use DEVICE BUFFERS during writes      True
block_size    1024  BLOCK size (0=variable length)        True
extfm         no     Use EXTENDED file marks               True
ret           no     RETENSION on tape change or reset     True
density_set_1 39    DENSITY setting #1                    True
density_set_2 39    DENSITY setting #2                    True
compress      yes    Use data COMPRESSION                  True
size_in_mb    20000 Size in Megabytes                     False
ret_error     no     RETURN error on tape change or reset  True
```

The first column of the **lsattr** command specifies the attribute for the device, the second column specifies the actual value for that attribute, the third column provides a brief description, and the last column specifies if the value for that attribute can be changed (true) or not (false).

► **lscfg**

This list configuration command displays information about the vendor name, serial number, type, and the model of the device. All this information is known in AIX 5L as the Vital Product Data (VPD). To get the VPD for the tape drive `rmt0`, for example, use the command as shown in Example 6-5.

Example 6-5 lscfg -vl command and output

```
# lscfg -vl rmt0
DEVICE          LOCATION          DESCRIPTION
rmt0           10-60-00-5,0     SCSI 8mm Tape Drive (20000 MB)
Manufacturer.....EXABYTE
Machine Type and Model.....IBM-20GB
Device Specific.(Z1).....38zA
Serial Number.....60089837
Device Specific.(LI).....A0000001
Part Number.....59H2813
FRU Number.....59H2839
EC Level.....E30279
Device Specific.(Z0).....0180020283000030
Device Specific.(Z3).....
```

Note: `lsattr` and `lscfg` can be run *only* with configured devices.

6.4 Adding a device

The process of adding a device (excluding hot-pluggable and dynamic reconfiguration devices) involves shutting down the system, physically connecting the device, and powering the system backup. If the device contains its own power source, make sure that the power is turned on *before* powering up the system.

6.4.1 Solaris

The procedure for adding a device to a Solaris system varies, depending on the device that is to be added. There are three general categories of device addition on Solaris:

- ▶ Non-hot plug, requiring the system to be shut down
- ▶ Hot plug
- ▶ Dynamic reconfiguration

The specific procedure varies from device to device and the documented procedure for the particular device must be followed. The generic procedure for adding a device to a Solaris system is as follows:

1. Become a Superuser
2. Install any required device drivers
3. Create or reconfigure the device:¹
 `# touch /reconfigure`
4. Shut down and power off the system
 `# init 5`
 or
 `# shutdown -i5 -y -g0`
5. Attach the device to the system
6. Power on and boot the system
7. Verify that the new device is correctly attached to the system and is operational

¹ This step can be skipped if a `boot -r` is performed when the system is booted.

6.4.2 AIX 5L

In AIX 5L, all the devices are self-configurable, except serial and parallel devices. The command that is used to configure the devices is the configuration manager (**cfgmgr**).

This command is run automatically at system boot, but you can run it at any time on a running system. For SCSI devices, you only have to set a unique SCSI ID on the device before attaching it. If you are going to attach a new device to a running system, be sure that the device is hot-swappable. Otherwise, you must power off the system before performing the attachment.

If **cfgmgr** does not find a device driver, you will be asked to install it. Study Figure 6-1 to understand the **cfgmgr**'s function.

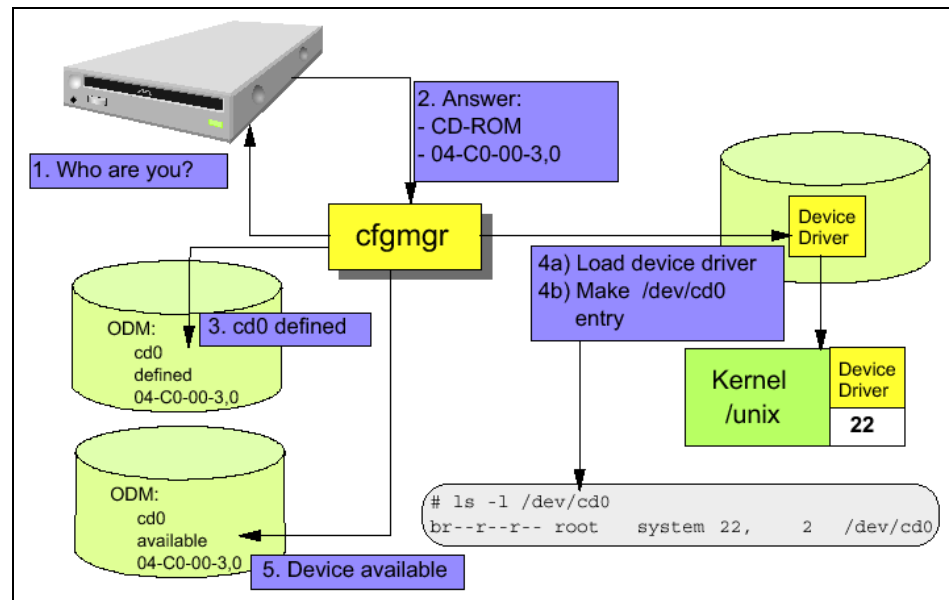


Figure 6-1 The configuration manager

Device configuration is not a difficult task in AIX 5L. In fact, more and more systems are supporting the hot plugging of a device into a running machine.

To install or replace a hot swappable card into a hot swap capable slot, follow the steps described here:

1. Verify that both the slot and the card are indeed hot pluggable.
2. If you are replacing a faulty device, unconfigure it first with **rmdev**.

3. Enter either **smitty** or **diag** to initiate the appropriate task (remove, add, or replace).

- **smitty devdrpci** (for the PCI hot plug manager)
- **diag -T identifyRemove** (for either PCI or SCSI hot plug managers)

4. When you have completed this task the installation is complete. If you have, for example, just added a new PCI device and performed a **lsslot -c pci**, you will see the following:

```
# Slot      Description                               Device(s)
U0.1-P2-I1  PCI-X capable, 64 bit, 133MHz slot  Unknown
```

Notice that the device is “Unknown” at this stage. This is due to the fact that there is no driver configured for it.

5. Run the configuration manager (**cfgmgr**) to configure the device driver for the newly added card. **lsslot -c pci** should now show something similar to the following:

```
# Slot      Description                               Device(s)
U0.1-P2-I1  PCI-X capable, 64 bit, 133MHz slot  fcs0
```

SMIT and adding devices

There are many SMIT screens that are used to change the device configuration or to add devices. Figure 6-2 shows the smitty menu in the Devices screen.

Run the following command to view the menu:

```
# smitty devices
```

```

                                Devices
Move cursor to desired item and press Enter.
[TOP]
  Install/Configure Devices Added After IPL
  Printer/Plotter
  TTY
  Asynchronous Adapters
  PTY
  Console
  Fixed Disk
  Disk Array
  CD ROM Drive
  Read/Write Optical Drive
  Diskette Drive
  Tape Drive
  Communication
  Graphic Displays
  Graphic Input Devices
  Low Function Terminal (LFT)
[MORE...12]
F1=Help      F2=Refresh   F3=Cancel    F8=Image
F9=Shell     F0=Exit     Enter=Do
```

Figure 6-2 Main menu for devices in smitty

For more information, refer to the details within the individual device types.

Other commands relating to adding devices

As with many other tasks in AIX 5L, you can also configure a device using the command line. The command that is to be used is **mkdev**. Following is an example of the command used to configure an additional tape drive into a system:

```
# mkdev -c tape -s scsi -t scsd -p scsi0 -w 5,0
rmt0 Available
```

To configure any device with **mkdev**, you must know the following information:

- ▶ **-c**
The class of the device
- ▶ **-s**
The subclass of the device
- ▶ **-t**
The type of the device. This is a specific attribute for the device.
- ▶ **-p**
The parent adapter of the device. You have to specify the logical name.
- ▶ **-w**
You must know the SCSI ID that you are going to assign to your new device. If it is a non-SCSI device, you must know the port number on the adapter.

The **mkdev** command also creates the ODM entries for the device and loads the device driver. Following is an example of the **mkdev** command for a non-SCSI device:

```
# mkdev -c tty -t tty -s rs232 -p sa1 -w 0 -a login=enable -a  
term=ibm3151  
tty0 Available
```

In this example, a new serial terminal is added to the parent adapter sa1, using port 0 in the adapter. The **-a** option is used to assign specific characteristics for the device, such as the terminal type and log in attributes.

If the **-a** option is omitted (for SCSI and non-SCSI devices), the default values are taken from the ODM (the PdAt “predefined attributes” file).

lsslot shows the list of dynamic slots and what is in them (Example 6-6).

Example 6-6 Using lsslot to list the slots

```
lsslot -c pci
```

# Slot	Description	Device(s)
U0.1-P2-I1	PCI-X capable, 64 bit, 133MHz slot	fcs1
U0.1-P2-I2	PCI-X capable, 64 bit, 133MHz slot	scsi2 scsi3
U0.1-P2-I3	PCI-X capable, 64 bit, 133MHz slot	Empty
U0.1-P2-I4	PCI-X capable, 64 bit, 133MHz slot	Empty
U0.1-P2-I5	PCI-X capable, 64 bit, 133MHz slot	ent1
U0.1-P2-I6	PCI-X capable, 64 bit, 133MHz slot	fcs0
U0.1-P2-I7	PCI-X capable, 32 bit, 66MHz slot	Empty

6.5 Modifying a device

This section discusses the modification of device attributes under Solaris and AIX 5L.

6.5.1 Solaris

The configuration settings for devices in Solaris are determined by the settings of the driver for the device, for example, the SCSI timeout on disk devices is determined by the SCSI drivers and will be the same for all the SCSI disks that are managed by a given driver. On AIX 5L, it is possible to change the time-out on each disk individually.

6.5.2 AIX 5L

This section describes how to use the smitty screens to change the values for a device. It is important to remember that in most cases, when you are going to change a device, the device must not be in use. You might have to put it into the defined state by running the following command:

```
rmdev -l device_name
```

This section provides an example of the smitty screen that is used to change the attributes of a network interface:

1. Use the following fast path to access this smitty screen:

```
# smitty chgenet
```

2. The screen shown in Figure 6-3 is displayed. Use this to select the Ethernet adapter that you want to use.

```

                                Ethernet Adapter

Move cursor to desired item and press Enter. Use arrow keys to
scroll.

    ent1 Available 10-80 IBM PCI Ethernet Adapter (22100020)
    ent0 Available 10-78 IBM 10/100/1000 Base-T Ethernet PCI Adapter
(1410

F1=Help           F2=Refresh       F3=Cancel
F8=Image          F0=Exit          Enter=Do
/=Find            n=Find Next
```

Figure 6-3 Selecting the Ethernet adapter

On selecting the adapter, the screen shown in Figure 6-4 is displayed. Change some attributes, such as the Hardware Receive queue size and Hardware Transmit queue size. These values have a performance impact when they are increased.

```

Change / Show Characteristics of an Ethernet Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]
Ethernet Adapter          ent1
Description              IBM PCI
Ethernet Adapt>
Status                   Available
Location                 10-80
HARDWARE TRANSMIT queue size [64]
                          +#
HARDWARE RECEIVE queue size [32]
                          +#
Full duplex              no
+
Enable ALTERNATE ETHERNET address no
+
ALTERNATE ETHERNET address
[0x000000000000] +
Apply change to DATABASE only no
+

F1=Help      F2=Refresh  F3=Cancel   F4=List
F5=Reset     F6=Command  F7=Edit     F8=Image
F9=Shell     F0=Exit     Enter=Do

```

Figure 6-4 Changing the attributes for a network interface

Example 6-7 shows the command for AIX 5L to change the default timeout on an hdisk.

Example 6-7 Equivalent AIX 5L command to change the default timeout

```

# lsattr -El hdisk5 -a rw_timeout
rw_timeout 30 READ/WRITE time out value True
# chdev -l hdisk5 -a rw_timeout=120

```



```
hdisk5 changed
# lsattr -El hdisk5 -a rw_timeout
rw_timeout 120 READ/WRITE time out value True
```

6.6 Removing a device

The process of removing a device (excluding hot-pluggable and dynamic reconfiguration devices) involves shutting down the system, physically disconnecting the device, and powering the system backup.

6.6.1 Solaris

Removal of devices in Solaris varies depending on the type of device that is being removed from the system. The recommended procedure for the removal of the specific device must be followed.

Removal of a device from a Solaris system might require a reboot to clear the device from the memory driver.

To remove the device files of a removed device from a Solaris system, the `devfsadm -C` command is used.

6.6.2 AIX 5L

The task of removing a device is performed with the `rmdev` command. This command removes all the ODM entries for a configured device (Example 6-8).

Example 6-8 Making a device unavailable

```
# lsdev -Cc tape
rmt0 Available 10-60-00-5,0 SCSI 8mm Tape Drive

# rmdev -l rmt0
rmt0 Defined

# lsdev -Cc tape
rmt0 Defined 10-60-00-5,0 SCSI 8mm Tape Drive
```

In Example 6-8, the tape drive configured in the system when the **rmdev** command is used is listed. Only the **-l** option, which indicates the logical device name, is used. This command changes only the device state, from available to defined, and it does not delete the ODM or **/dev** entries. To remove them from the system, you must also use the **-d** flag. Example 6-9 shows how to remove the tape drive from a system.

Example 6-9 Removing a device

```
# ls -l /dev/*hdisk5*
brw----- 1 root    system    41,  1 Jun 23 10:22 /dev/hdisk5
crw----- 1 root    system    41,  1 Jun 23 10:22 /dev/rhdisk5
# rmdev -l hdisk5 -d
hdisk5 deleted
# lsdev -Cl hdisk5
# ls -l /dev/*hdisk5*
#
```

6.7 Alternate disk paths (multipathing)

Alternate disk pathing is a technology for providing redundant (alternate path) access to disk devices. It is used in SAN or direct arbitrated loop fibre channel environments where there are multiple hardware-based connections to the array.

Disk multipathing, which provides redundancy, can also improve performance with the use of load balancing across the redundant links.

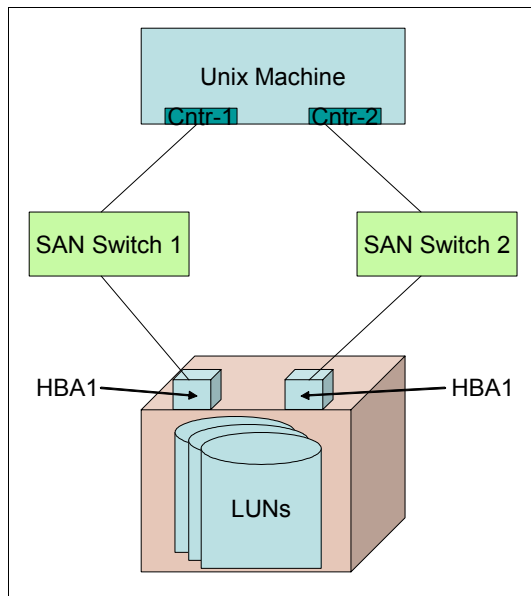


Figure 6-5 A multipath scenario

6.7.1 Solaris

To provide for alternate disk path access, Solaris requires the installation of additional software. A number of different pieces of software are available to provide this functionality. They are commonly provided by storage vendors and are sometimes designed to work with that particular vendor's disk array product, while others work with any vendor's disk array.

Following are the examples of additional software that can be used to provide multipath disk access on Solaris:

- ▶ EMC PowerPath
<http://www.emc.com>
- ▶ Veritas Dynamic Multi-Pathing (DMP)
<http://www.veritas.com>

- ▶ Sun StoreEdge Traffic Manager
<http://www.sun.com>
- ▶ IBM Redundant Disk Array Controller (RDAC)
<http://www.ibm.com>

6.7.2 AIX 5L

AIX 5L V5.2 and later provide native (multipath IO) MPIO support for certain storage subsystems, for example, the IBM TotalStorage® Enterprise Storage Server® (ESS) range, some Hitachi systems, and Symmetrix. MPIO support is configured on supported subsystems at device discovery time.

Certain vendors also provide additional software, for example, RDAC for IBM FAStT Storage Manager and PowerPath for EMC, with their disk subsystems that also provide differing capabilities with regard to multipath redundancy.

For a detailed description of the capabilities of MPIO, refer to Chapter 4, Section 4.1 of *AIX 5L Differences Guide Version 5.2*, SG24-5765. This IBM Redbook has indepth descriptions of the reservation policy, algorithms, and the commands modified for use with MPIO devices.

MPIO is installed and configured as part of BOS installation. Although no further configuration is required, you can add, remove, reconfigure, enable, and disable devices or device paths using SMIT, the Web-based System Manager, or the command-line interface. Refer to Table 6-3 on page 179 for the commands used to manage MPIO.

When using MPIO, the disk is managed by a unique name and ID, as shown in Example 6-10.

Example 6-10 Unique ID

PCM	PCM/friend/scsiscsd	Path Control Module	False
algorithm	fail_over	Algorithm	True
dist_err_pcnt	0	Distributed Error Percentage	True
dist_tw_width	50	Distributed Error Sample Time	True
hcheck_interval	0	Health Check Interval	True
hcheck_mode	nonactive	Health Check Mode	True
max_transfer	0x40000	Maximum TRANSFER Size	True
pvid	0001813f1a43a54d0000000000000000	Physical volume identifier	False
queue_depth	3	Queue DEPTH	False
reserve_policy	single_path	Reserve Policy	True
size_in_mb	9100	Size in Megabytes	False

MPIO in AIX 5L provides two different algorithms for multipathing:

- ▶ `fail_over`
Only the highest priority path is used. If this fails, the next highest priority path is used.
- ▶ `round_robin`
All the paths are used relative to their weighted priority. If one path fails, the others take over the load.

Taking Figure 6-5 on page 175 as an example environment, if you had one LUN assigned to the machine, you will end up with only one `/dev/dsk/hdiskX` device. However, underneath that, there will be two *paths* to the disk (Example 6-11).

Example 6-11 LUN-redundant paths

```
#lspath -l hdisk4
Enabled hdisk4 fscsi0
Enabled hdisk4 fscsi1
```

Thus, `hdisk4` in Example 6-11 has redundancy through `fscsi0` and `fscsi1`. At this point, you cannot tell which MPIO algorithm is being used. To be able to do that, look at the device attributes with `lsattr`, as shown in Example 6-12.

Example 6-12 Checking device attributes with the lsattr command

```
lsattr -El hdisk4
PCM                PCM/friend/fcpothe Path Control Module
False
algorithm          fail_over          Algorithm
True
clr_q              no                Device CLEARS its Queue on error
True
dist_err_pcmt     0                Distributed Error Sample Time
True
dist_tw_width     50              Distributed Error Sample Time
True
hcheck_cmd        test_unit_rdy    Health Check Command
True
hcheck_interval  0                Health Check Interval
True
hcheck_mode       nonactive        Health Check Mode
True
location          Location Label
True
```

lun_id	0x5211000000000000	Logical Unit Number ID
False		
max_transfer	0x40000	Maximum TRANSFER Size
True		
node_name	0x5005076300c09589	FC Node Name
False		
pvid	none	Physical volume identifier
False		
q_err	yes	Use QERR bit
True		
q_type	simple	Queuing TYPE
True		
queue_depth	1	Queue DEPTH
True		
reassign_to	120	REASSIGN time out value
True		
reserve_policy	single_path	Reserve Policy
True		
rw_timeout	30	READ/WRITE time out value
True		
scsi_id	0x650b00	SCSI ID
False		
start_timeout	60	START unit time out value
True		
ww_name	0x5005076300c19589	FC World Wide Name
False		

Example 6-12 shows that the algorithm is set to *fail_over*. This means that only one path will be in use at a time.

If you want to change this, the disk must not be in active use. Although you do not have to move the device to *Defined*, if it is in use by the Logical Volume Manager (LVM), you will not be able to modify it.

If the disk is assigned to a volume group, vary off that volume group before performing any changes.

To change the algorithm to *round_robin*, use three different methods, **smitty mpio**, Web-based System Manager, or **chdev** (Example 6-13).

Example 6-13 Changing the MPIO algorithm

```
# chdev -a reserve_policy=no_reserve -a algorithm=round_robin -l hdisk4
hdisk4 changed
# lsattr -El hdisk4 | grep -E "^PCM|^algorithm|reserve_policy"
```

PCM	PCM/friend/fcpothor	Path Control Module
False		
algorithm	round_robin	Algorithm
True		
reserve_policy	no_reserve	Reserve Policy
True		

Add extra paths to devices with the **mkpath** command, as shown in Example 6-14.

Example 6-14 mkpath example²

To define and configure an already defined path between scsi0 and the hdisk1 device at SCSI ID 5 and LUN 0 (i.e., connection 5,0), enter:

```
mkpath -l hdisk1 -p scsi0 -w 5,0
```

Remove a device path with the **rmpath** command, as shown in Example 6-15.

Example 6-15 rmpath example³

To unconfigure the path from scsi0 to hdisk1 at connection 5,0, type:

```
rmpath -l hdisk1 -p scsi0 -w "5,0"
```

To enable or disable paths to a device, use the **chpath** command. Example 6-16 shows the disable option.

Example 6-16 chpath example⁴

To disable the paths between scsi0 and the hdisk1 disk device, enter:

```
chpath -l hdisk1 -p scsi0 -s disable
```

AIX 5L MPIO command summary

Table 6-3 shows the disk multipath commands.

Table 6-3 Disk multipath commands

Command	Function
mkpath	Adds another path to a device

² Example from the **mkpath** man page

³ Example from the **rmpath** man page

⁴ Example from the **chpath** man page

Command	Function
<code>rmpath</code>	Removes a path from a device
<code>chpath</code>	Changes status or attribute associated with a path
<code>lspath</code>	Displays information about paths to a MPIO-capable device
<code>iostat -m</code>	Displays statistics for each path on each disk
<code>smitty mpio</code>	Provides you with all the options you might want for MPIO maintenance, including disabling all the activity down a particular parent adapter, enabling or disabling all the paths (although you can never disable the last path to a device), changing path priorities, and so on
<code>lsattr -E1</code>	Displays the attributes of a device
<code>chdev</code>	Changes the attributes of a device

6.8 Device management summary

AIX 5L has different ways in which to manage devices. Figure 6-6 shows a summary of device commands, device states, and the related ODM database.

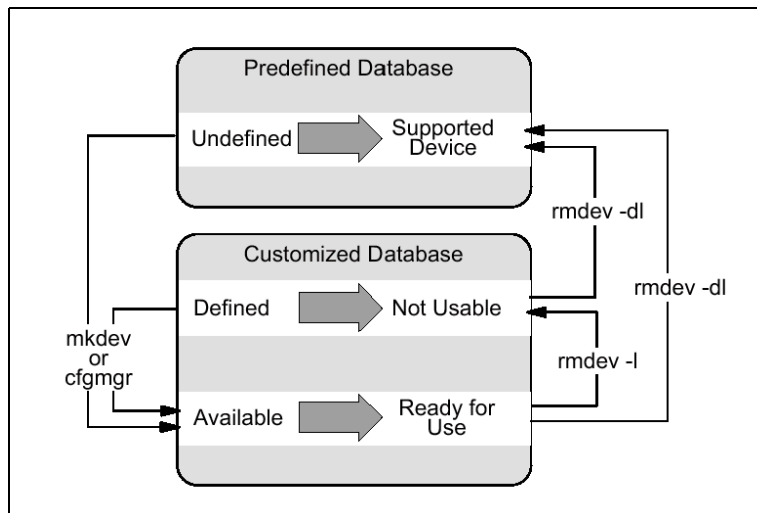


Figure 6-6 AIX 5L device states and ODM

Table 6-4 provides the quick reference for device management.

Table 6-4 Quick reference for device management

Task	AIX 5L	Solaris 9
Run multiple tasks in a graphical user interface (GUI) environment	<ul style="list-style-type: none"> ▶ smit ▶ Web-based System Manager 	smc
Configure a device (dynamic reconfiguration)	cfgmgr	<ul style="list-style-type: none"> ▶ cfgadm ▶ devfsadm
Add a device with the command line	mkdev	devfsadm
Remove an SCSI device	rmdev^a	<ul style="list-style-type: none"> ▶ luxadm (for Sun storage only) ▶ devfsadm -C
Change attributes for a device	chdev	No equivalent
List devices	<ul style="list-style-type: none"> ▶ lsdev^b ▶ prtconf ▶ lscfg 	<ul style="list-style-type: none"> ▶ prtconf ▶ sysdef ▶ dmesg ▶ prtdiag ▶ kstat
List the configuration attributes for devices	lsattr -El	No equivalent
List vital product data (serial number, model, vendor, part number) of a device	lscfg -v1	No equivalent

a. It can change the state of a device from “available” to “defined”, or it can delete the ODM entries for a device.

b. It can be used to query the configured devices if used with the -C (upper case) option, or supported devices if used with the -P option.



Network services

This chapter discusses the differences in networking and networking services between Solaris, specifically, Solaris 9, and AIX 5L, specifically, AIX 5L V5.3. This chapter does not describe what a TCP/IP is or how to plan for your networking services because this is the same for both the operating systems (OS). The initial configuration-at-installation methods for both Solaris and AIX 5L are discussed in Chapter 3, “Operating system installation” on page 47.

This chapter covers manual configuration and reconfiguration of networking services and includes the following topics:

- ▶ 7.1, “Network configuration changes” on page 184
- ▶ 7.2, “Differences between Internet Protocol V4 and Internet Protocol V6” on page 191
- ▶ 7.3, “Mixed IPv4 and IPv6 networks” on page 192
- ▶ 7.4, “Network load balancing and failover solutions” on page 195
- ▶ 7.5, “Static and dynamic routing” on page 198
- ▶ 7.6, “IP network services” on page 201
- ▶ 7.7, “Simple Network Management Protocol” on page 210

7.1 Network configuration changes

Configuration changes are handled somewhat differently on Solaris and AIX 5L. Chapter 1, “AIX 5L and Solaris: Approaches to administration” on page 3 discusses the fundamental differences between the two OS.

An example of a networking-related task that a Solaris or AIX 5L system administrator might routinely have to perform is defining a new network interface for an existing system. This can be a new *physical* interface (a new Network Information Card (NIC)) or a *virtual* interface.

7.1.1 Instructions for Solaris

This task must include the following steps:

1. Assign a host name to the new interface (if it is different from the host name associated with the primary interface) by creating a file called `/etc/hostname.interface`, and putting the host name into this file.
2. Ensure that the host name and IP of the new interface is in the `/etc/hosts` file.
3. If a different router is required for the new interface, use the **route** command to add it.
4. Use **ifconfig** to establish and open the interface.
5. Use **ifconfig** to assign an IP address, a broadcast address, and a subnetmask to the new interface, or to edit the files `/etc/netmask`, `/etc/networks`, and `/etc/inet/hosts`, and then reboot the system for the changes to be recognized.

In addition, the Solaris system administrator can use the **sys-unconfig** command and reconfigure the Solaris box.

Following is a list of files that the Solaris administrator is likely to modify to make network configuration changes:

- ▶ `/etc/hostname.interface`
Contains the IP address or the host name for each network interface you have to use
- ▶ `/etc/netmasks`
Contains subnetting information
- ▶ `/etc/nodename`
Contains the host name of the system

- ▶ `/etc/defaultdomain`
Contains the fully qualified domain name of the system
- ▶ `/etc/defaultrouter`
Contains an entry for each router that the server will use
- ▶ `/etc/inet/hosts`
A database containing the local IP address to name mappings. The `/etc/hosts` is a symlink to this file.
- ▶ `/etc/nsswitch.conf`
Contains configuration of network name services
- ▶ `/etc/resolv.conf`
Contains the Domain Name System (DNS) client configuration of the system
- ▶ `/etc/bootparams`
Contains information for serving network booting services
- ▶ `/etc/ethers`
Contains information about the MAC-to-IP address mapping used by the `rarpd` daemon

(There are other files that are used by networking on Solaris (`/etc/inet/services` or `/etc/inet/protocols`), but their default values are fine for most applications and usually do not require any modification.)

7.1.2 Instructions for AIX 5L

Most of the configuration files defined earlier do not exist on AIX 5L. Therefore, the AIX 5L administrator, to accomplish the task of configuring a new network interface, is most likely to open the System Management Interface Tool (SMIT) or the Web-based System Manager tool (`smitty` or `wsm`), possibly specifying a fast path of `inet`. Using these tools, all the tasks described in 7.1.1, “Instructions for Solaris” on page 184 can be accomplished with the appropriate changes to the AIX 5L configuration files, the interface will be available for use immediately, and will still be working after a reboot. Best of all, no configuration file or item is overlooked or forgotten, and no syntax errors are inadvertently introduced.

The figures displayed in this section demonstrates the use of smit for configuring a virtual IP address interface:

```
# smit inet
```

Figure 7-1 shows the smit inet example screen.

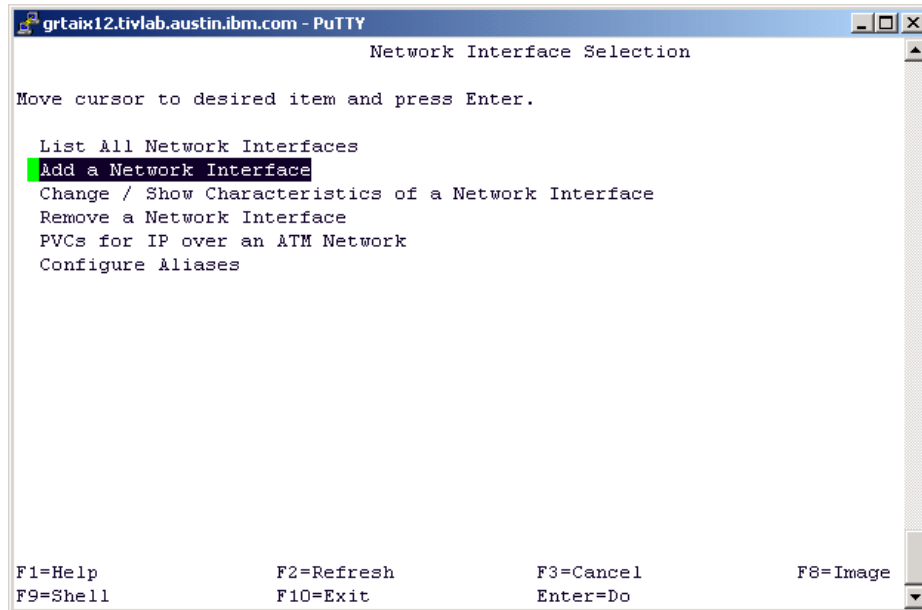


Figure 7-1 *smit inet example*

Figure 7-2 shows the continuation of the smit inet example screen.

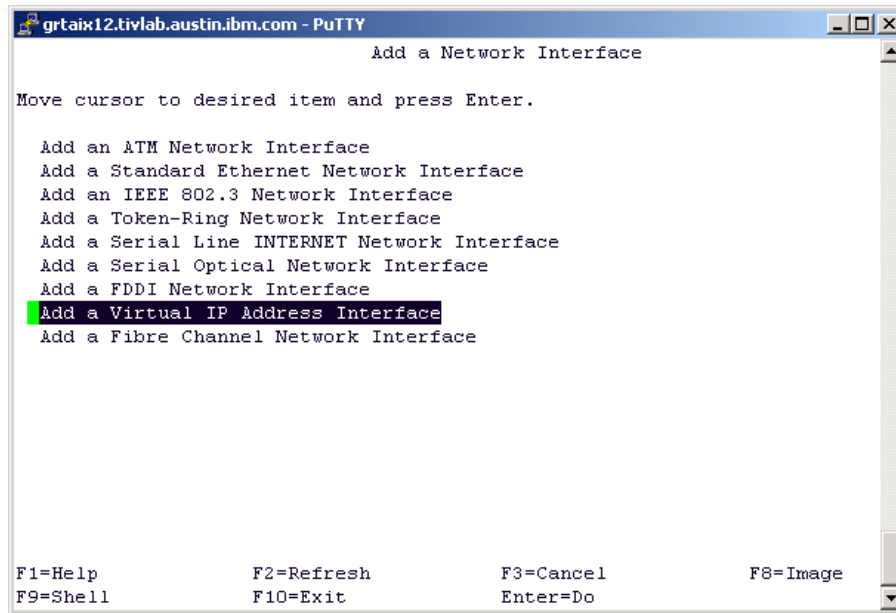


Figure 7-2 smit inet example (continued)

Figure 7-3 shows the continuation of the smit inet example screen.

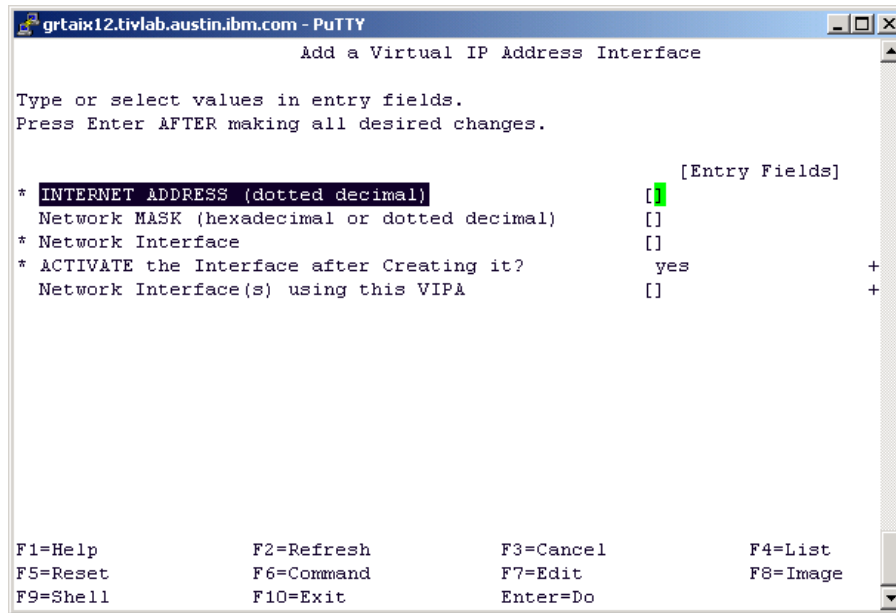


Figure 7-3 smit inet example (continued)

7.1.3 Common network configuration files in Solaris and AIX 5L

Following are the network configuration files that are common to both Solaris and AIX 5L:

- ▶ /etc/hosts
Specifies IP addresses to name mappings
- ▶ /etc/resolv.conf
Contains the DNS client configuration of the system
- ▶ /etc/services
Contains Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port numbers to service name mappings
- ▶ /etc/protocols
Contains IP protocol numbers to protocol name mappings

7.1.4 Other networking differences

Table 7-1 shows the network commands and configuration files in Solaris, and their equivalent in AIX 5L.

Table 7-1 Network commands and configuration files

Task	Solaris	AIX 5L
Configure TCP/IP interface	Edit the following files: <ul style="list-style-type: none"> ▶ /etc/hostname* ▶ /etc/inet/* ▶ /etc/defaultrouter ▶ /etc/defaultdomain ▶ /etc/nodename ▶ /etc/netmasks 	[smit,wsm] tcpip
Display interface settings	ifconfig	ifconfig
Display interface status and statistics	<ul style="list-style-type: none"> ▶ netstat -i ▶ ifconfig 	<ul style="list-style-type: none"> ▶ netstat -i ▶ ifconfig
Configure interface	ifconfig	ifconfig
Check various network statistics	netstat	netstat
Change name server or domains	vi /etc/resolv.conf	<ul style="list-style-type: none"> ▶ namerslv ▶ vi /etc/resolv.conf ▶ smitty namerslv
Specify name services search order	vi /etc/nsswitch.conf	vi /etc/netsvc.conf
Display kernel network parameters	<ul style="list-style-type: none"> ▶ ndd /dev/ip \? ▶ ndd /dev/tcp \? 	no -a
Configure kernel network parameters	ndd -set driver parameter	<ul style="list-style-type: none"> ▶ smit performance or ▶ no -o Tunable=NewValue
Check for network link	<ul style="list-style-type: none"> ▶ ndd or ▶ kstat 	<ul style="list-style-type: none"> ▶ smit performance or ▶ netstat -v interface grep -i link
Set up Dynamic Host Configuration Protocol (DHCP)	<ul style="list-style-type: none"> ▶ dhcpcnfig ▶ dhcprmgr ▶ dhcpcinfo ▶ dhtadm ▶ pntadm 	<ul style="list-style-type: none"> ▶ dhcpsconf ▶ dhcpaction ▶ dhcprd ▶ bootptodhcp ▶ dadmin
Check routing table	<ul style="list-style-type: none"> ▶ netstat -r ▶ route 	<ul style="list-style-type: none"> ▶ netstat -r ▶ route ▶ smitty route

Task	Solaris	AIX 5L
Modify routing table	<code>route</code>	<ul style="list-style-type: none"> ▶ <code>smitty route</code> ▶ <code>route</code>
Test for connectivity	<code>ping</code>	<code>ping</code>
Check IP path	<code>tracert</code>	<code>tracert</code>
Capture network packets	<code>snoop</code>	<ul style="list-style-type: none"> ▶ <code>tcpdump</code> ▶ <code>iptrace/ipreport</code>

Example 7-1 shows the sample Solaris ifconfig output.

Example 7-1 Sample Solaris ifconfig output

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ffffffff
ce0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index
2
    inet 9.3.5.38 netmask fffffff0 broadcast 9.3.5.255
    ether 0:3:ba:53:10:71
lo0: flags=2000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
    inet6 ::1/128
ce0: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
    ether 0:3:ba:53:10:71
    inet6 fe80::203:baff:fe53:1071/10
```

Note: Note that this Solaris machine has only one physical interface, but is configured for both inet (IPv4) and inet6 (IPv6).

Example 7-2 shows the sample AIX 5L ifconfig output.

Example 7-2 Sample AIX 5L ifconfig output

```
ifconfig -a
en0:
flags=4e080863,80<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,MULTICAST,GRO
UPRT,64BIT,PSEG,CHAIN>
    inet 9.48.205.115 netmask 0xfffffe00 broadcast 9.48.205.255
lo0:
flags=e08084b<UP,BROADCAST,LOOPBACK,RUNNING,SIMPLEX,MULTICAST,GROUPRT,6
4BIT>
```

```
inet 127.0.0.1 netmask 0xff000000 broadcast 127.255.255.255
inet6 ::1/0
tcp_sendspace 65536 tcp_recvspace 65536
```

7.2 Differences between Internet Protocol V4 and Internet Protocol V6

Internet Protocol version 4 (IPv4) is the default networking stack for all the recent OS, and is no exception for Solaris and AIX 5L. However, there are a number of minor differences between the two OS and between IPv4 and IPv6. This section highlights these differences.

IPv4 is known as the *dotted-decimal* notation for an IP address that consists of four decimal parts, for example, 192.168.1.100.

IPv6 is known as the *colon-hex* notation for an IP address that consists of eight hexadecimal parts, for example, 0:56:78ab:22:33:44:55:66.

IPv6 was developed to provide an almost unlimited number of IP addresses to a network.

The installation programs of both Solaris and AIX 5L ask if you want to configure IPv6 on a given server and set the right networking parameters for you, so that after installation, the system is ready to operate in an IPv6 network.

IPv6 in Solaris

To configure IPv6 on a Solaris system, you must *touch*, that is, create an empty file, the `/etc/hostname6.interface` file for each IPv6 interface, and reboot the system. Optionally, you can add IP to name mappings in the `/etc/inet/ipnodes` file. You can use most of the tools from IPv4, with special switches for IPv6.

IPv6 in AIX 5L

To configure IPv6 on an AIX 5L system, use `smit tcpip` and select **IPV6 Configuration**. However, the setting will be lost after a reboot. On AIX 5L, it is also necessary to edit the `/etc/rc.tcpip` file that is invoked at boot time, and uncomment the following line:

```
# start /usr/sbin/autoconf6 ""
```

7.3 Mixed IPv4 and IPv6 networks

Because IPv6 is not a widely deployed protocol yet, IPv6 islands might be separated by IPv4 routers, or, when the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic. *Tunneling* provides a way in which to use an existing IPv4 routing infrastructure to carry IPv6 traffic. In order to link the IPv6 islands, use tunnels. Both Solaris and AIX 5L support IPv6 tunneling in IPv4.

7.3.1 Tunneling

There are two types of tunnels in IPv6, automatic tunnels and configured tunnels.

- ▶ Automatic tunnels

Automatic tunnels are configured by using the IPv4 address information embedded in an IPv6 address. The IPv6 address of the destination host includes information about which IPv4 address the packet should be tunneled to.

Automatic tunnels are useful during a transition from IPv4 to IPv6, or when an IPv6 network must continue to pass through IPv4 network clouds.

- ▶ Configured tunnels

Configured tunnels must be configured manually. These tunnels are used when using IPv6 addresses that do not have any embedded IPv4 information. The IPv6 and IPv4 addresses of the endpoints of the tunnel must be specified.

Setting up Solaris tunneling with IPv6 and IPv4

In Solaris, you can add tunnel interfaces using the `ifconfig` command or by adding options to the `/etc/hostname6.interface` file.

To configure IPv6 over IPv4 tunnels, perform the following tasks:

1. As root, create the file `/etc/hostname6.ip.tunn` where `n` is a numeric value, for example, 0, 1, 2, and so on.
2. Add entries to the file as follows:
 - a. Add the tunnel source and destination addresses:

```
tsrc IPv4-source-addr tdst IPv4-destination-addr up
```

- b. (Optional) Add a logical interface for the source and destination IPv6 addresses:

```
addif IPv60source-address IPv6-destination-address up
```

Note: This is for the configured tunnels.

3. Reboot.

For more information about configuring the automatic and configured tunnels, refer to “Set up tunneling in IPv6” in the Solaris 9 System Administration Guide: IP Services.

Notes: `tsrc`, `tdst`, and `addif` are options to the `ifconfig` command. For more information about these options, refer to the Solaris `ifconfig` man page.

Perform the same steps at the other end of the tunnel for bidirectional communication to occur.

If your system is to be configured as a router, you must also configure your router to advertise over tunneling interfaces before rebooting. Refer to “How to Configure Your Router to Advertise Over Tunneling Interfaces” on page 317 of the *Solaris 9 System Administration Guide: IP Services*.

Setting up AIX 5L tunneling for IPv6 with IPv4

As mentioned earlier, there are two types of tunnels in IPv6, automatic tunnels and configured tunnels.

Automatic tunnel

To enable IPv6 and a single automatic tunnel, use the following:

```
autoconf6
```

To enable an automatic tunnel through interface `en0`, use the following:

```
autoconf6 -s -i en0
```

Automatic tunnels are removed when the system is rebooted. Therefore, in order to have the automatic tunnel created at boot time, edit `/etc/rc.tcpip` and uncomment the following line (if it is not already uncommented):

```
#start /usr/sbin/autoconf6 ""
```

Start SMIT by using the following command, and include the options shown in Figure 7-4 and Figure 7-5:

```
“smit ctinet6 --”
```

Figure 7-4 shows the AIX 5L tunneling screen.

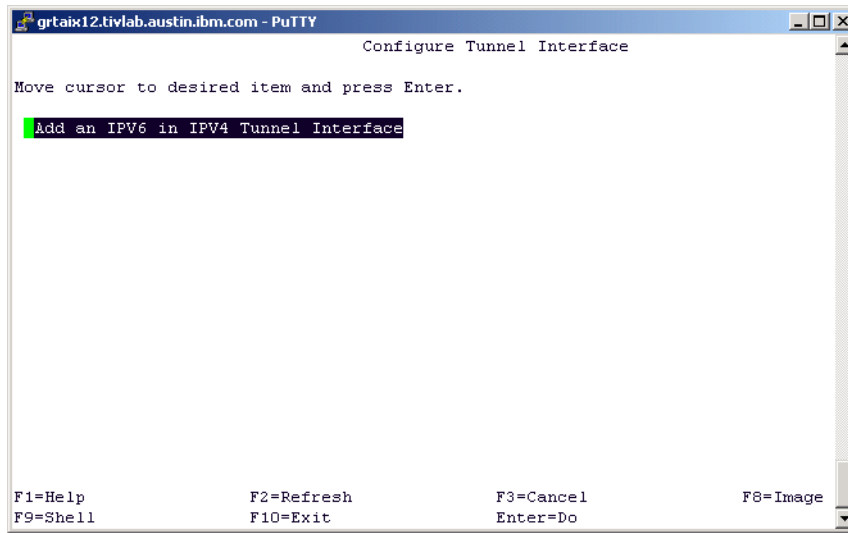


Figure 7-4 AIX 5L tunneling

Figure 7-5 shows the continuation of AIX 5L tunneling screen.

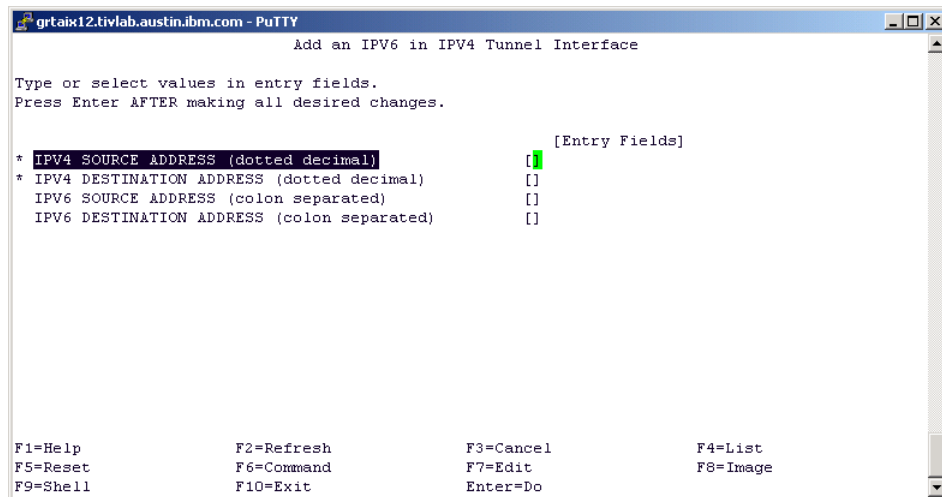


Figure 7-5 AIX 5L tunneling (continued)

7.4 Network load balancing and failover solutions

Different products are available for network load balancing and failover solutions on both the platforms. This section describes the features of these products.

7.4.1 Solaris

Following are the products that are available for network load balancing and failover solutions on Solaris:

SUN Trunking

The network trunking feature in Solaris provides the ability to aggregate multiple Ethernet and Fast Ethernet links into a single link to get a scalable *fat pipe* to carry higher data rates than a single Ethernet link can carry.

Note: The *Sun Trunking*TM product is an add-on, but is not part of the base Solaris OS.

Sun IP Multipath

In Solaris, there is a built-in feature called IP Network Multipath that enables you to create one or more groups of physical interfaces and use them as one virtual interface. The IP Multipath does not provide inbound load balancing, and requires many IP addresses to implement. It provides for:

- ▶ Failure detection
- ▶ Repair detection
- ▶ Outbound load spreading

7.4.2 AIX 5L

Following are the products that are available for network load balancing and failover solutions on AIX 5L.

Etherchannel

The basic concept of Etherchannel on AIX 5L is to provide load balancing and failover resources to network links. Etherchannel is included in the base AIX 5L OS.

Etherchannel is different from Sun Trunking, in that, Etherchannel has a new and important feature called interface backup adapter. This feature is useful if you intend to implement a failover solution across different network switches. A good example of the use of this feature is a scenario where you have two network adapters, and each one is on a different switch.

The Etherchannel can be administrated by a command line or SMIT tool. The smit fast path is **smit etherchannel**, as shown in Figure 7-6.

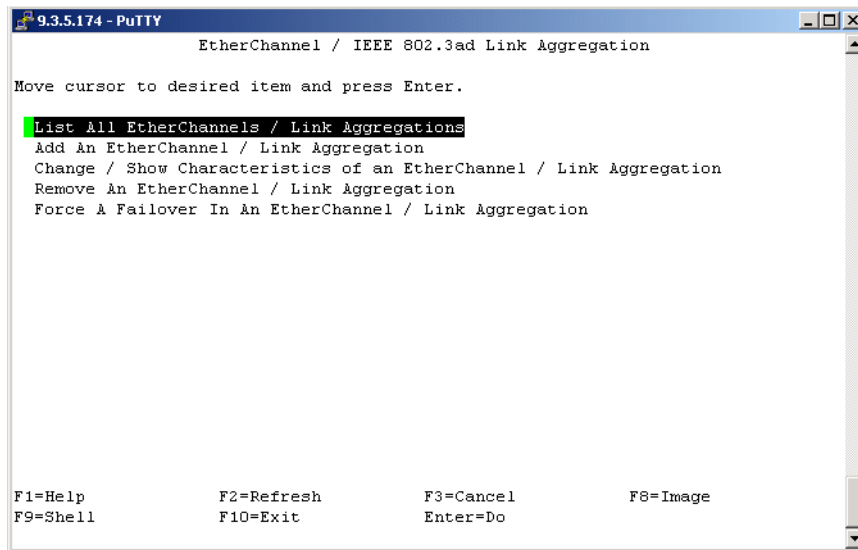


Figure 7-6 *smit etherchannel: Main screen*

For the migration scenario, refer to Table 7-2.

Table 7-2 *Sun Trunking versus Etherchannel*

Feature	Sun Trunking	AIX 5L Etherchannel
Included on BOS	no	yes
Backup Ethernet adapter	no	yes
Failover and repair detection	yes	yes
Inbound and outbound load balance	yes	yes
IEEE 802.3ad compatibility	yes	yes
Load balance by MAC	yes	yes
Load balance by round robin	yes	yes

Feature	Sun Trunking	AIX 5L Etherchannel
Load balance by IP address	yes	yes

For more information about how Etherchannel works on AIX 5L, refer to the online System p AIX 5L Collaboration Center:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?>

Virtual IP address

Virtual IP address (VIPA) on AIX 5L can be used in situations where network communications might have to continue even in the event of a network interface going down.

VIPA is configured, just as any IP network interface is configured, in SMIT. In addition, you can specify a group of interfaces when configuring VIPA. When configured this way, for all the outgoing connections initiated by the VIPA host through these interfaces that are designated to use a VIPA, the virtual address becomes the source address placed in the TCP/IP packet header of the outgoing packets.

To start VIPA configuration from SMIT, the fast path is `smit mkinetvi` (Figure 7-7).

```

Add a Virtual IP Address Interface

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                     [Entry Fields]
* INTERNET ADDRESS (dotted decimal)      []
  Network MASK (hexadecimal or dotted decimal) []
* Network Interface                       []
* ACTIVATE the Interface after Creating it?  yes      +
  Network Interface(s) using this VIPA     []      +

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit       Enter=Do

```

Figure 7-7 VIPA on SMIT

7.5 Static and dynamic routing

Static routing is most useful when a single network is communicating with a small number of other networks. However, when your network begins to communicate with more networks, the number of gateways increases, and so does the amount of time and effort required to maintain a routing table manually.

With dynamic routing, daemons update the routing table continuously as and when they receive information broadcasts by other routing daemons.

Routing in Solaris

To configure a Solaris box to act as a router, you require at least two network interfaces on that box. After ensuring this, perform the following tasks:

1. Create an `/etc/hostname.interface` file for each network interface installed, specifying the host name or the IP address of that interface.
2. Enter these host names and IP addresses in the `/etc/inet/hosts` file for IPv4 and `/etc/inet/ipnodes` for IPv6.
3. If this Solaris router is a part of any subnetted network, add the subnets in the `/etc/inet/netmasks` file. The startup scripts then determine if they have to start a routing daemon for learning and advertising routes (daemons such as Routing Information Protocol (RIP) or Network Router Discovery (RDISC)), or if they have to use static routing.

- Static routing in Solaris

On a user's Solaris box, specify the use of a static default route by editing the `/etc/defaultrouter` file. If the file contains a resolvable host name or IP address, the system uses that default gateway and does not launch a dynamic routing protocol such as RIP or RDISC.

- Dynamic routing in Solaris

If the `/etc/defaultrouter` file is *empty*, the system tries to use a dynamic gateway first, using `/usr/sbin/in.rdisc` if it exists. If this method fails, it starts the RIP in a passive, nonadvertising mode.

A machine with only one network interface can be forced to be a router by creating an empty `/etc/gateways` file. A machine with more than one network interface can be forced to be a multihomed host instead of a router by creating an empty `/etc/notrouter` file.

Before inet services are stopped when a Solaris system is shut down, the existence of either an *in.routed* or an *in.rdisc* process is queried by the */etc/inetinit* script. If either process is running, that indicates that dynamic routing was used, and inetinit creates a file called */etc/.dynamic_routing* to preserve the dynamic routes that were identified earlier.

For IPv6 routing, use the *ndpd* and *ripngd* daemons for static and dynamic routing, respectively.

Routing in AIX 5L

In AIX 5L too, there is static routing and dynamic routing.

Static routing in AIX 5L

Maintain static routing on AIX 5L using either the **route** command or by using SMIT:

```
route add/flush/delete/change/monitor/get .....
```

or

```
smit route
```

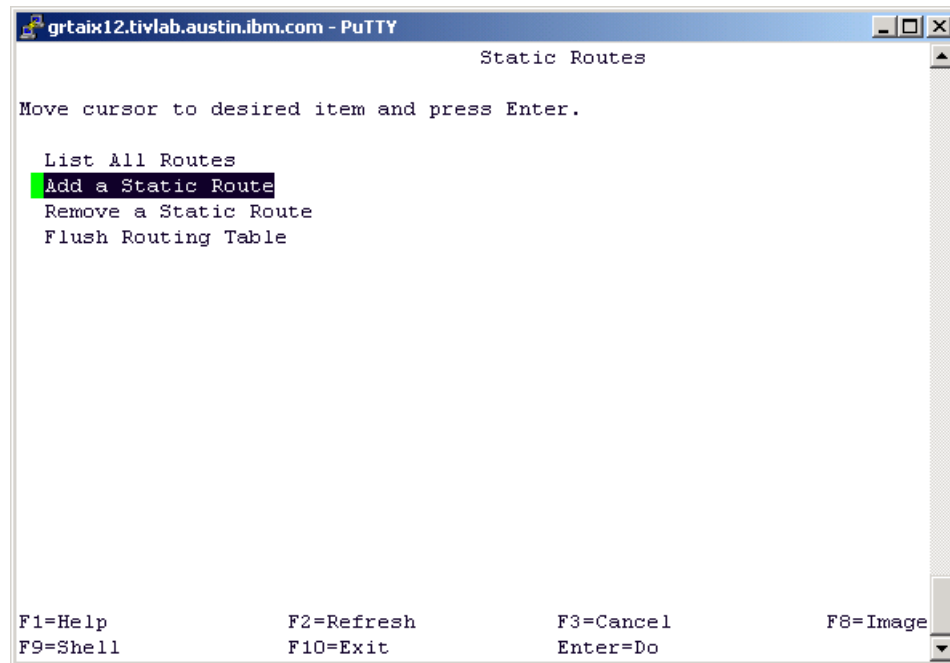


Figure 7-8 Smit route

Figure 7-9 shows the Add a Static Route screen.

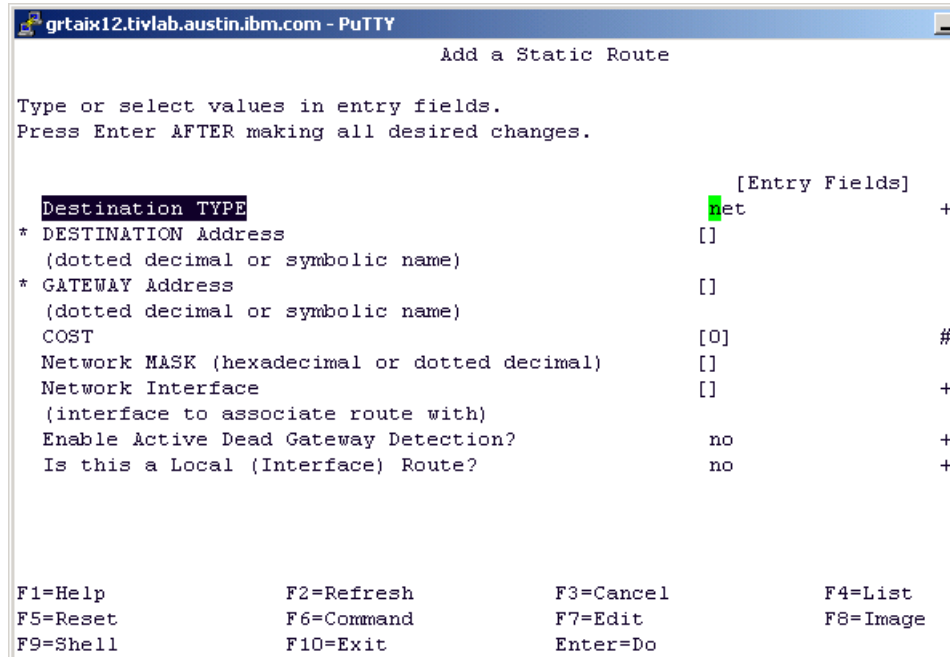


Figure 7-9 Smit route: Add a Static Route screen

Dynamic routing in AIX 5L

The routed daemon supports only the RIP protocol. The gated daemon supports the RIP protocol, Routing Information Protocol Next Generation (RIPng), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), and BGP4+, Defense Communications Network Local-Network Protocol (HELLO), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Internet Control Message Protocol (ICMP and ICMPv6)/Router Discovery routing protocols simultaneously. In addition, the gated daemon supports the Simple Network Management Protocol (SNMP).

To specify dynamic routing in AIX 5L, edit /etc/rc.tcpip to uncomment the starting of either routed or of gated. Table 7-3 shows dynamic routing in Solaris and AIX 5L.

Table 7-3 Dynamic routing

Task	Solaris	AIX 5L
Check routing table	<ul style="list-style-type: none"> ▶ netstat -r ▶ route 	<ul style="list-style-type: none"> ▶ netstat -r ▶ [smit,wsm] route ▶ route

Task	Solaris	AIX 5L
Modify routing table	route	smit route
Specify static routing - IPv4	<ul style="list-style-type: none"> ▶ route add [default] ipaddr ▶ vi /etc/default/r w/ipaddr 	<ul style="list-style-type: none"> ▶ route add default or ▶ [smit,wsm] route
Specify static routing - IPv6	<ul style="list-style-type: none"> ▶ route add [default] ipaddr ▶ ndpd - daemon 	route add -inet6 default IPv6 router address
Specify dynamic routing - IPv4	If /etc/default/router file is empty, in.rdisc and in.routed daemons are started at reboot	<ul style="list-style-type: none"> ▶ vi /etc/rc.tcp and ▶ Uncomment gated or routed^a
Dynamic routing - IPv6 daemon	ripngd	ndpd-router

a. The gated and routed daemons are started at reboot

7.6 IP network services

This section contains information about a set of commonly used network services.

7.6.1 inetd-based

This section describes the differences between inetd for Solaris and AIX 5L.

Solaris inetd server

In Solaris, standard network services such as Telnet, File Transfer Protocol (FTP), remote login (Rlogin), Trivial File Transfer Protocol (TFTP), and others are started on demand by the inetd network daemon through the /etc/inetd.conf configuration file. The /etc/services configuration file contains the port name to port number mappings for network applications, which can be used with the inetd daemon. Activate usage logging and TCP wrappers by specifying the following parameters in the /etc/default/inetd configuration file:

```
ENABLE_CONNECTION_LOGGING=YES
ENABLE_TCPWRAPPERS=YES
```

All the services that are to be run by the inetd daemon are defined in the /etc/inetd.conf configuration file.

AIX 5L inetd server

Refer to *AIX 5L Version 5.3 System Management Guide: Operating System and Devices*, SC23-4910-02 for more information about the System Resource Controller.

Table 7-4 shows the inetd commands for Solaris and AIX 5L.

Note: The inetd is a subsystem of TCP/IP and is a daemon. Subsystems (daemons) have “subservers” that are also daemons. The inetd subsystem daemon controls the subserver daemons of comsat, fingerd, tftpd, rexecd, rlogind, rshd, talkd, syslogd, telnetd, tftpd, and uucpd.

Table 7-4 *inetd* commands

Task	Solaris	AIX 5L
Configuring the inetd subservers (ftp, telnet, rlogin, ssh, and so on)	<ul style="list-style-type: none">▶ vi/etc/services▶ vi/etc/default/inetd▶ vi/etc/init.d/inetsvc▶ vi/etc/inetd.conf	smit inetdconf
Starting the inetd subsystem	/usr/sbin/inetd -s	smit inetd
Stopping the inetd subsystem	/etc/init.d/inetsvc stop	smit inetd
Starting the inetd subservers (ftp, telnet, rlogin, and so on)	/usr/sbin/in.daemon	startsrc -t subservername
Stopping the inetd subservers (ftp, telnet, rlogin, and so on)	kill in.daemon-pid	stopsrc -t subservername
Changing inetd configuration	vi/etc/inetd.conf	smit inetdconf
Refreshing inetd after configuration change	kill -HUP inetd process	If smit inetdconf is used, no refresh is required
Querying inetd subservers	ps -ef grep 'in\.'	lssrc -t subservername

7.6.2 Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) servers from Solaris and AIX 5L have comparable features:

- ▶ Support for earlier Bootstrap Protocol (BOOTP) clients
- ▶ Support for local and remote clients by using DHCP relay services

- ▶ Large network support
- ▶ Network booting information for DHCP clients
- ▶ Dynamic Domain Name System (DDNS) updates

However, the server itself is different in terms of management scripts and configuration files.

The Solaris Dynamic Host Configuration Protocol server

Solaris has several utilities for controlling the `in.dhcpd` server daemons such as `dhcpconfig`, `dhtadm`, `pntadm`, and the GUI `dhcprmgr`.

The configuration is stored in the `/etc/inet/dhcpsvc.conf` file and some other tables, such as `dhcptab`, `macros`, and so on.

The AIX 5L Dynamic Host Configuration Protocol server

On AIX 5L, the DHCP server is based on the `dhcpsd` daemon. The DHCP server maintains a database of addresses it has given out and details about who has them. These databases are kept in the `/etc/dhcpsd.ar` and `/etc/dhcpsd.cr` files. On startup, a server reads the configuration file and sets up its initial database of available addresses. The server accepts the **refresh** command or a `SIGHUP` signal to reread the configuration file.

The DHCP server reads the `/etc/services` file to determine which port it should use for receiving requests. The default service is `dhcps`. Because this is the same port that the `bootpd` daemon uses, you can only have one (either `dhcpsd` or `bootpd`) daemon running. If you choose the `dhcpsd` daemon, you must comment `bootp` from the `/etc/inetd.conf` file, and then enter the following in the command line:

```
refresh -s inetd
```

The **dhcpsconf** command brings up an X Windows GUI that lets the network administrator read, save, and modify the configuration files. It also allows starting, stopping, and retrieving statistics from a running server.

Table 7-5 shows the DHCP commands of Solaris and AIX 5L.

Table 7-5 DHCP commands

Task	Solaris	AIX 5L
Configuring DHCP	<ul style="list-style-type: none"> ▶ DHCP Manager (GUI) ▶ dhcprmgr (GUI) ▶ dhcpconfig ▶ dhtadm ▶ pntadm 	<ul style="list-style-type: none"> ▶ dhcpsconf (GUI) ▶ dhcpaction ▶ dhcprd ▶ bootptodhcp ▶ dadmin

Task	Solaris	AIX 5L
Daemon name	in.dhcpd	dhcpsd
Query information of the DHCP server	dhcpinfo	lssrc -ls dhcpsd
Stopping and starting the DHCP server	<ul style="list-style-type: none"> ▶ DHCP Manager (X Windows) ▶ dhcpmgr (Java GUI) or ▶ /etc/init.d/dhcp stop or start 	<ul style="list-style-type: none"> ▶ [smit, wsm] tcpip or ▶ [startsrc, stopsrc] -s dhcpsd

For information about the AIX 5L DHCP Server for IPv6, refer to *AIX 5L Version 5.3 System Management Guide: Communications and Networks*, SC23-4909.

7.6.3 Domain Name System

For the Domain Name System (DNS) server, both Solaris and AIX 5L OS are based on the BIND solution, and the main configuration file is `/etc/named.conf`.

AIX 5L V5.3 supports BIND Version 8 and Version 9 to simplify migration. By default, named links for BIND Version 8 are described in Example 7-3.

Example 7-3 Listing the actual named version

```
# ls -l /usr/sbin/named* |grep ^l
lrwxrwxrwx 1 root system 16 Sep 20 1970 named ->
/usr/sbin/named8
lrwxrwxrwx 1 root system 21 Sep 20 1970 named-xfer ->
/usr/sbin/named8-xfer
```

To use a different version of named, relink the symbolic links accordingly for the named and the named-xfer daemons.

Use named9 as follows:

```
ln -fs /usr/sbin/named9 /usr/sbin/named
```

In this, you do not have to relink the named8-xfer file because BIND Version 9 does not use this file anymore.

AIX 5L also provides samples for DNS configuration:

- ▶ `/usr/samples/tcpip/named.boot`

This contains the sample named.boot file with directions for its use.

- ▶ /usr/samples/tcpip/named.data
This contains the sample DOMAIN data file with directions for its use.
- ▶ /usr/samples/tcpip/hosts.awk
This contains the sample awk script for converting an /etc/hosts file to an /etc/named.data file. This file also contains directions for its use.
- ▶ /usr/samples/tcpip/addr.awk
This contains the sample awk script for converting an /etc/hosts file to an /etc/named.rev file. This file also contains directions for its use.

The subsystem name is named. Check the named status as shown in Example 7-4.

Example 7-4 Checking the named status

```
# lsrc -s named
```

Subsystem	Group	PID	Status
named	tcpip		inoperative

Start a named service as shown in Example 7-5.

Example 7-5 Starting a named service

```
# startsrc -s named
0513-059 The named Subsystem has been started. Subsystem PID is 319498.
```

Stop a named service as follows:

```
# stopsrc -s named#
```

7.6.4 Network Time Protocol

Both Solaris and AIX 5L provide Network Time Protocol (NTP) services.

Solaris Network Time Protocol

- ▶ ntp_adjtime adjusts the local clock parameters.
- ▶ ntp_gettime gets the local clock values.
- ▶ ntpdate sets the date and time by way of NTP.
- ▶ ntpq is the standard NTP query program.
- ▶ ntptrace traces a chain of NTP hosts back to their master time source.
- ▶ xntpd is the NTP daemon.
- ▶ xntpdc is a special NTP query program.

AIX 5L Network Time Protocol

- ▶ ntpdate sets the date and time of using the NTP.
- ▶ ntpq starts the standard NTP query program.
- ▶ ntptrace traces a chain of NTP hosts back to their master time source.
- ▶ xntpd starts the NTP daemon.
- ▶ xntpd starts the query/control program for the NTP daemon, xntpd.

7.6.5 Lightweight Directory Access Protocol

Both Solaris and AIX 5L support Lightweight Directory Access Protocol (LDAP) as both client and server.

For more information about this topic, refer to *Integrating AIX into Heterogenous LDAP Environments*, SG24-7165, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg247165.html?Open>

7.6.6 Network Information Service and Network Information Service+

Both Solaris and AIX 5L support Network Information Service (NIS) and NIS+ protocols.

For more information about this topic, refer to the AIX 5L Version 5.3 Network Information Services (NIS and NIS+) Guide, available in the online System p AIX 5L Collaboration Center

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?>

7.6.7 Network File System

Network File System (NFS) is used in both Solaris and AIX 5L for sharing file systems across a network. Both the OS can act as servers and as clients, even at the same time.

In Solaris, the server daemon that controls NFS activities is called rpcbind.

In AIX 5L, the server daemon is called portmap.

Network File System server setup in Solaris

The NFS server daemons, nfsd, nfslogd, and mountd, are started and stopped with:

```
/etc/init.d/nfs.server start/stop
```

This file runs automatically at boot time, but can be run manually anytime.

To share an NFS resource, you can either perform the task manually with the **share** command or automatically at boot time by placing an entry in the `/etc/dfs/dfstab` file.

If you already have an NFS server running and you update the content of the `dfstab` file, run the **shareall** command to update the NFS shares without restarting the service.

Example 7-6 shows an `/etc/dfs/dfstab` file.

Example 7-6 Example of an `/etc/dfs/dfstab` file

```
#      Place share(1M) commands here for automatic execution
#      on entering init state 3.
#
#      Issue the command '/etc/init.d/nfs.server start' to run the NFS
#      daemon processes and the share commands, after adding the very
#      first entry to this file.
#
#      share [-F fstype] [ -o options] [-d "<text>"] <pathname>
#      [resource]
#      .e.g,
#      share -F nfs -o rw=engineering -d "home dirs" /export/home2
share -F nfs -d "Patches"/export/local/support/patches
share -F nfs -d "PMRs"export/local/support/pmrs
```

Network File System client setup in Solaris

The NFS client daemons, `statd`, and `lockd`, are started and stopped with:

```
/etc/init.d/nfs.client start/stop
```

This file runs automatically at boot time, but can be run manually anytime.

To mount a shared NFS resource, either perform the task manually with the **mount** command or automatically at boot time by placing an entry in the `/etc/vfstab` file.

To see what file systems are being shared by another system (and are available for you to mount), enter:

```
showmount -e hostname
```

Example 7-7 shows a sample Solaris `/etc/vfstab`.

Example 7-7 Sample Solaris `/etc/vfstab`

#device	device	mount	FS	fsck	mount
mount					
#to mount	to fsck	point	type	pass	at boot
options					
#					
#/dev/dsk/c1d0s2	/dev/rdisk/c1d0s2	/usr	ufs	1	yes
-					
fd	-	/dev/fd	fd	-	no
/proc	-	/proc	proc	-	no
/dev/dsk/c0t10d0s1	-	-	swap	-	no
/dev/md/dsk/d0	/dev/md/rdisk/d0	/	ufs	1	no
/dev/md/dsk/d3	/dev/md/rdisk/d3	/usr	ufs	1	no
/dev/md/dsk/d1	/dev/md/rdisk/d1	/var	ufs	1	no
/dev/md/dsk/d2	/dev/md/rdisk/d2	/opt	ufs	2	yes
/dev/md/dsk/d4	/dev/md/rdisk/d4	/tmp	ufs	2	yes
/dev/md/dsk/d5	/dev/md/rdisk/d5	/data	ufs	2	yes
/dev/dsk/c1t5d0s6	/dev/rdisk/c1t5d0s6	/export/local	ufs		
2	yes	-			
/dev/dsk/c1t5d1s0	/dev/rdisk/c1t5d1s0	/home_dirs	ufs		
2	yes	-			

Network File System server setup on AIX 5L

The NFS server daemons (`rpc.mountd`, `nfsd`, `rpc.statd`, and `rpc.lockd`) can be started or stopped individually with the `startsrc -s daemon`. Alternatively, all the NFS daemons can be started with `startsrc -g nfs`.

To share an NFS resource, either perform the task manually with the `exportfs` command or automatically at boot time by placing an entry in the `/etc/exports` file.

If you make changes to the `/etc/exports` file, execute the `exportfs -a` command to update the NFS shares without restarting the service.

To see which directories are being exported, enter:

```
exportfs
```

Example 7-8 shows an AIX 5L `/etc/exports` file.

Example 7-8 Example of an AIX 5L `/etc/exports` file

```
/cdrom -ro,root=comaix13:comaix14,access=comaix13:comaix14
/data2 -root=comaix13:comaix14,access=comaix13:comaix14
/data1
-root=comaix13:comaix14:comaix06:comaix11:comaix10,access=comaix13:comaix14:comaix06:comaix10:comaix11
```

Network File System client setup in AIX 5L

The NFS server daemons, `biod`, `rpc.statd`, and `rpc.lockd`, can be started or stopped individually with `startsrc -s daemon`. Alternatively, all the NFS daemons can be started with `startsrc -g nfs`.

To mount a shared NFS resource, either perform the task manually with the `mount` command or automatically at boot time by placing an entry in the `/etc/filesystems` file.

To see which file systems are being shared by another system, enter:

```
showmount -e hostname
```

Example 7-9 shows an entry in `/etc/filesystems`.

Example 7-9 An example of an entry in `/etc/filesystems`

```
/data2:
    dev           = /dev/fs1v00
    vfs           = jfs2
    log           = /dev/log1v01
    mount         = true
    options       = rw
    account       = false
```

For more information about NFS, refer to Chapter 4, “Disks and file systems” on page 91.

7.6.8 Mail services

Solaris and AIX 5L both use `sendmail` as the mail transfer agent. For information about configuring `sendmail` on AIX 5L, refer to the description provided in System p AIX 5L Collaboration Center Commands Reference.

7.7 Simple Network Management Protocol

Another commonly used remote system management service is the Simple Network Management Protocol (SNMP). There are many tools available on cross platforms, managed by the SNMP protocol. SNMP is an Internet Engineering Task Force (IETF) standard and is perhaps the most widely implemented standard for system management. The data model used by an SNMP service is called a Management Information Base (MIB). Different sections of MIB are supported by different devices and servers depending on the services available on the system. For more information about the SNMP service, refer to the Internet Engineering Task Force (IETF) Web site at:

<http://www.ietf.org>

There are some differences between SNMP settings on Solaris 9 and AIX 5L V5.3.

Any parameters that you configured in the Solaris Server `/etc/snmp/conf/snmp.conf` file must be manually migrated to the SNMP configuration files in AIX 5L.

In AIX 5L, since V5.3, the default SNMP agent running at system boot time is SNMP V3, which uses the `/etc/snmpdv3.conf` file as its configuration file. The `/usr/sbin/snmpd` on AIX 5L is a symbolic link to SNMP V3. If you want to use the old SNMP configuration file, use the commands shown in Table 7-6.

Table 7-6 *Modifying SNMP configuration*

Command and option	Task
<code>/usr/sbin/snmp3_ssw -e</code>	Switch to the encrypted version of snmpdv3 agent
<code>/usr/sbin/snmp3_ssw -l</code>	Switch to the nonencrypted version of snmpdv3 agent
<code>/usr/sbin/snmp3_ssw -1</code>	Switch to the snmpdv1 agent

For information about how to migrate the configuration file between different snmpd versions, refer to the documentation available online at:

http://inetsd01.boulder.ibm.com/pseries/ca_ES/aixbman/commadm/HT_commandn_snmp_v1v3.htm

Another file that is available on AIX 5L V5.3 is `/etc/clsnpmp.conf`, and its contents are used by the `c1snmp` command. `c1snmp` provides SNMP manager functions from the AIX 5L shell for querying SNMP agents about network management information.

Table 7-7 describes how to stop and start SNMP on the Solaris and AIX 5L servers.

Table 7-7 Starting and stopping SNMP

Task	Solaris	AIX 5L
Stop	<code>/etc/init.d/init.snmpdx stop</code>	<code>stopsrc -s snmpd</code>
Start	<code>/etc/init.d/init.snmpdx start</code>	<code>startsrc -s snmpd</code>

Modify the `/var/tmp/snmpd.log` that records events from the `snmpd` daemon. If the file is removed, it will be recreated by the `snmpd` daemon. The size of the `/var/tmp/snmpd.log` file can be limited so that it does not grow indefinitely. Edit the `/etc/snmpd.conf` file to change the number (in bytes) in the appropriate section for size.

Simply refreshing the SNMP V3 agent will not work as it did in SNMP V1. If you make changes to the `/etc/snmpdv3.conf` file, stop and start the daemon as instructed earlier. The dynamic configuration function supported in SNMP V3 does not allow you to refresh.



Boot and system initialization

This chapter describes the differences in system booting and initialization between Solaris and AIX.

This chapter contains the following topics:

- ▶ 8.1, “Booting a system” on page 214
- ▶ 8.2, “Useful commands” on page 223
- ▶ 8.3, “The /etc/inittab file” on page 225
- ▶ 8.4, “System shutdown” on page 233
- ▶ 8.5, “Network booting” on page 237

8.1 Booting a system

This section provides information about specific ways in which to boot a system, different booting sources, and an overview of the booting process.

8.1.1 Booting types

A server can be booted in several ways depending on the tasks the system administrator has to perform.

Where the Scalable Processor ARChitecture (SPARC) platform has the OpenPROM firmware to control and initiate the system booting, AIX 5L uses the Read Only Storage Initial Program Load (ROS IPL). This phase includes a power-on self test (POST), the locating the boot device, and loading the boot kernel into memory.

Table 8-1 shows the equivalence between the Solaris and AIX 5L boot process and locations of items that are involved in booting and shutting down a system in AIX 5L and Solaris.

Table 8-1 Boot process comparison

Tasks	Solaris	AIX 5L
Boot process	Phases: <ul style="list-style-type: none"> ▶ Boot PROM: Display system information, run POST, load bootblk, locate ufsboot ▶ Boot programs: bootblk loads and executes the ufsboot ▶ Kernel initialization: ufsboot loads and executes the core kernel, initializes core kernel data structures, loads other kernel modules based on the /etc/system file, starts /sbin/init program ▶ init: Starts other processes based on the /etc/inittab file 	Phases: <ul style="list-style-type: none"> ▶ ROS: Check the system board, perform POST, locate the boot image, load the boot image into memory, begin system initialization and execute phase 1 of the /etc/rc.boot script ▶ Base device configuration: Start Configuration Manager to configure base devices ▶ System boot: Start init process phase 2, switch to hard disk root file system, start other processes defined by records in the /etc/inittab file and execute phase 3 of the /etc/rc.boot script
Kernel modules directory	Kernel modules are stored in three directories: <ul style="list-style-type: none"> ▶ /platform/sparc/kernel or /platform/i86pc/kernel ▶ /kernel ▶ /usr/kernel 	Kernel and kernel extension modules are stored in two directories: <ul style="list-style-type: none"> ▶ /usr/lib/boot ▶ /usr/lib/drivers

Tasks	Solaris	AIX 5L
System-run levels	Eight run levels: <ul style="list-style-type: none"> ▶ 0: Power-down state ▶ s or S: Single-user state ▶ 1: Administrative state ▶ 2: Multiuser state ▶ 3: Multiuser state with NFS resources shared (default run level) ▶ 4: Alternative multiuser (nit in use) ▶ 5: Power-down state ▶ 6: Reboot to run level 3 state 	Defined run levels: <ul style="list-style-type: none"> ▶ 0-1: Reserved for future use ▶ 2: Multiuser mode with NFS resources shared (default run level) ▶ 3-9: Defined according to user's preferences ▶ m, M, s, S: Single-user mode (maintenance level) ▶ a, b, c: Starts processes assigned to the new run levels while leaving the existing processes at the current level running ▶ Q, q: init command to reexamine the /etc/inittab file^a
Determine a system's run level	who -r	who -r
Change a system's run level	Choose one of the following: <ul style="list-style-type: none"> ▶ halt ▶ init ▶ poweroff ▶ reboot ▶ shutdown ▶ telinit ▶ uadmin 	<ul style="list-style-type: none"> ▶ init or ▶ telinit level number
Startup script	/sbin/rc <i>run-level number</i>	/etc/rc
Use new kernel	N/A	bosboot -k
Shutdown and reboot	<ul style="list-style-type: none"> ▶ reboot or ▶ shutdown -i 6 	<ul style="list-style-type: none"> ▶ reboot (single-user mode) or ▶ Shutdown -Fr
Shutdown	<ul style="list-style-type: none"> ▶ init 5 ▶ shutdown ▶ halt or ▶ poweroff (ok prompt only) 	<ul style="list-style-type: none"> ▶ shutdown or ▶ halt

a. When a level from 1 - 9 is specified, the **init** command kills processes at the current level and restarts any processes associated with the new run level based on the /etc/inittab file.

8.1.2 Overview of Solaris for SPARC booting process

In Solaris for SPARC, booting a kernel is the task of the PROM chip with the monitor program. This controls the operation of the system before the kernel is available. It then begins the boot process:

1. POST is run.
2. The proper device for booting is identified and initialized.
3. PROM loads the primary boot program, bootblk, whose purpose is to load the secondary boot program that is located in the UNIX file system (UFS), from the default boot device.
4. The bootblk program finds and executes the secondary boot program, ufsboot, and loads it into the memory.
5. After the ufsboot program is loaded, the ufsboot program loads the kernel.
6. The kernel initializes itself and begins loading modules by using ufsboot to read the files. When the kernel has loaded enough modules to mount the root (/) file system, the kernel unmaps the ufsboot program and continues, using its own resources.
7. Other kernel modules based on the /etc/system file are loaded.
8. The kernel creates a user process and the /sbin/init program is started, which brings up the system based on the information in the /etc/inittab file.
9. The /sbin/init process starts the run control (rc) scripts that execute a series of other scripts. These scripts (/sbin/rc*) check and mount the file systems, start various processes, and perform system maintenance tasks.

8.1.3 Overview of the AIX 5L boot process

As an AIX 5L system administrator, you must have a general understanding of the boot process. This knowledge is useful for solving problems that prevent a system from booting properly. These problems can be related to both software and hardware. It is also important to be familiar with the hardware configuration of your system.

Booting involves the following steps:

1. As with Solaris, the initial step in booting a system is POST. Its purpose is to verify that the basic hardware is in a functional state. The memory, keyboard, communication, and audio devices are also initialized. You can see an image or text for each of these devices displayed on the screen. It is at this point that you can use the function key to choose a different boot list. The light-emitting diode (LED) values displayed during this phase are model-specific.

2. System Read Only Storage (ROS) is specific to each system type. It is necessary for AIX 5L V5.3 to boot, but it does not build the data structures required for booting. It locates and loads the bootstrap code. System ROS contains generic boot information and is operating system-independent.
3. Software ROS (also called bootstrap) forms an initial program load (IPL) control block that is compatible with AIX 5L V5.3. This takes control and builds AIX 5L-specific boot information. A special file system located in memory, which is called RAMFS, is created. Software ROS then locates, loads, and turns over control to the AIX 5L boot logical volume (BLV). The Software ROS is responsible for completing machine preparation in order to enable it to start the AIX 5L kernel.
4. A complete list of the files that are a part of the BLV can be obtained from the `/usr/lib/boot` directory. The most important components are:
 - The AIX 5L kernel
 - Boot commands called during the boot process, such as **bootinfo** and **cfgmgr**
 - A reduced version of the Object Data Manager (ODM). Many devices must be configured before `hd4` is made available. Therefore, their corresponding methods have to be stored in the BLV. These devices are marked as base in `PdDv`. (Refer to Appendix C, “AIX 5L Object Data Manager” on page 503.)
 - The `rc.boot` script
5. The AIX 5L kernel is loaded and takes control. The system displays 0299 on the LED panel. All the previous codes are hardware-related. The kernel completes the boot process by configuring the devices and starting the init process. LED codes displayed during this stage are generic AIX 5L codes.
6. So far, the system has tested the hardware, found a BLV, created the RAMFS, and started the init process from the BLV. The `rootvg` has not yet been activated. From here on, the `rc.boot` script is called three times, and is passed a different parameter each time.

During *boot phase 1*, the following actions take place:

- a. The init process started from RAMFS executes the boot script `rc.boot 1`. If the init process fails for some reason, code `c06` is shown on the LED display.
- b. At this stage, the **restbase** command is called to copy a partial image of the ODM from the BLV into the RAMFS. If this operation is successful, the LED display shows `510`; otherwise, LED code `548` is shown.
- c. After this, the **cfgmgr -f** command reads the `Config_Rules` class from the reduced ODM. In this class, devices with the attribute `phase=1` are considered to be base devices. Base devices are devices that are

necessary to access rootvg. If, for example, the rootvg is located on a hard disk, all the devices starting from the system board up to the disk must be initialized. The corresponding methods are called so that rootvg can be activated in boot phase 2.

- d. At the end of boot phase 1, the **bootinfo -b** command is called to determine the last boot device. At this stage, the LED shows 511.

In *boot phase 2*, the rc.boot script is passed to the parameter 2. During this phase the following steps take place:

- a. The rootvg volume group is varied on with the special version of the **varyonvg** command, the **ipl_varyon** command. If this command is successful, the system displays 517. Otherwise, one of the LED codes, 552, 554, or 556, is displayed, and the boot process is halted.
- b. Root file system hd4 is checked using the **fsck -f** command. This verifies whether the file system is unmounted cleanly before the last shutdown. If this command fails, the system displays code 555.
- c. The root file system (/dev/hd4) is mounted on a temporary mount point (/mnt) in RAMFS. If this fails, 557 is displayed in the LED display.
- d. The /usr file system is verified using the **fsck -f** command and then mounted. If this operation fails, the LED 518 is displayed.
- e. The /var file system is verified using the **fsck -f** command and then mounted. The **copycore** command checks if a dump occurred. If it did, it is copied from the default dump devices, /dev/hd6, to the default copy directory, /var/adm/ras. Afterwards, /var is unmounted.
- f. The primary paging space from rootvg /dev/hd6 is activated.
- g. The mergedev process is called and all the /dev files from the random access memory (RAM) file system are copied on to the disk.
- h. All the customized ODM files from the RAM file system are copied to disk. Both the ODM versions from hd4 and hd5 are now synchronized.
- i. Finally, the root file system from rootvg (disk) is mounted over the root file system from the RAMFS. The mount points for the rootvg file systems become available. Now, the /var and /usr file systems from rootvg are mounted again on their ordinary mount points.
- j. No console is available at this stage. Therefore, all the boot messages are copied to **alog**. The **alog** command maintains and manages logs.

After phase 2 is completed, rootvg is activated and the following steps take place:

- a. The /etc/init process is started. It reads the /etc/inittab file and calls rc.boot with argument 3.

- b. The /tmp file system is mounted.
- c. The rootvg is synchronized by calling the **syncvg** command and launching it as a background process. As a result, all the stale partitions from rootvg are updated. At this stage, LED code 553 is shown.
- d. At this stage, the **cfgmgr** command is called. If the system is booted in normal mode, the **cfgmgr** command is called with option -p2. If the system is booted into service mode, the **cfgmgr** command is called with option -p3. The **cfgmgr** command reads the Config_rules file from ODM and calls all the methods corresponding to either phase=2 or phase=3. All the other devices that are *not* base devices are configured at this time.
- e. The console is then configured by calling the **cfgcon** command. After the configuration of the console, boot messages are sent to the console if no STDOUT redirection is made. However, all the missed messages can be found in /var/adm/ras/conslog. The LED codes that might be displayed at this time are:
 - c31: Console is not yet configured. Provides instructions to select console.
 - c32: Console is an LFT
 - c33: Console is a TTY
 - c34: Console is a file on the disk
- f. Finally, the synchronization of the ODM in the BLV with the ODM from the /(root) file system is performed by the **savebase** command.
- g. The syncd daemon and errdemon are started.
- h. The LED display is turned off.
- i. If the file /etc/nologin exists, it is removed.
- j. If there are devices marked as missing in CuDv, a message is displayed on the console.
- k. The message system initialization that is completed is sent to the console. The execution of the rc.boot is completed. Process init continues processing the next command from /etc/inittab.

8.1.4 Boot modes

In AIX 5L, there are five different startup modes:

- ▶ Normal
- ▶ System Management Service (SMS)
- ▶ Diagnostic with default bootlist (DIAG_DEFAULT)
- ▶ Diagnostic with stored bootlist (DIAG_STORED)
- ▶ Open Firmware OK prompt (OPEN_FIRMWARE)

This section describes the five startup modes.

Normal mode

By default, the machine uses the “normal” boot list, which usually contains one or more hard drives. When the machine performs a normal boot, it completes the full AIX 5L boot sequence and start processes, enables terminals, and generates a login prompt to make it available for multiuser access.

System Management Services

Another boot option for the IBM eServer pSeries and IBM RS/6000 is to boot a machine-specific code called the System Management Service (SMS) programs. These programs are not a part of AIX 5L. This code is shipped with the hardware and is built into the firmware. It can be used to examine the system configuration and set boot lists without the aid of an AIX 5L operating system. It is invoked during the initial stages of the boot sequence using the F1 key or the 1 key.

Tip: To start System Management Service, reboot the system. Press the F1 key or the 1 key when the monitor light turns green. You have approximately 15 seconds to press F1 or 1. When all the device icons (or words) display in the monitor, it is too late to interrupt the boot sequence, and the system boots from the default boot list, for example, hdisk0.

The System Management Service menu varies depending on the model, generally, there are four main services. These are shown in Table 8-2.

Table 8-2 System Management Service menu

System Management Service menu	Explanation
Language	Select from English, French, German, Italian, Spanish, and the default language
Set up Remote IPL	View or change the boot list
Utilities	Set power on and supervisory passwords, update firmware, select console, and so on.
Exit	Return to previous screen

Maintenance mode

A machine is started from a hard disk, network, tape, or CD-ROM with the boot mode set to maintenance, through the Hardware Management Console (HMC) or with the key in the service position on an older system. This condition is also called maintenance mode. In maintenance mode, a system administrator can perform tasks such as installing new or updated software and running diagnostic checks.

Diagnostic with default bootlist (DIAG_DEFAULT)

The logical partition boots using the default boot list that is stored in the system firmware. This mode is normally used to boot customer diagnostics from the CD-ROM drive. Use this boot mode to run stand-alone diagnostics.

Diagnostic with stored bootlist (DIAG_STORED)

The logical partition performs a service mode boot using the service mode boot list saved in nonvolatile random access memory (NVRAM). Use this boot mode to run online diagnostics.

OPEN_FIRMWARE

The logical partition boots to the open firmware prompt. This option is used by service personnel to obtain additional debug information.

Note: Any change you make to the boot mode from the HMC takes effect only after you shut down the logical partition and reactivate that partition profile.

All the machines have a normal boot list and one or more service boot lists. The normal boot list is the default boot list.

To view the normal boot list, type the following in an AIX 5L command prompt:

```
# bootlist -m normal -o
```

Change the boot list using the same command:

```
# bootlist -m normal hdiskX "2nd device"
```

Systems use sounds and graphics to show the different phases of the boot process, for example, as soon as you power on the system, an audio beep is produced when the processor is found to be active, the PowerPC logo is shown (or the text presented) when the system memory checking is completed, and the device logos are shown for all the devices that have a valid address. At the end of the device logo display, if the system ROS is not damaged, an audio beep is produced again.

Several systems have LED displays to show what phase of the boot process the system is going through. If something goes wrong, you can interpret the LED codes and take the appropriate action to rectify the problem.

8.1.5 Using the Hardware Management Console to perform a slow boot

In some cases, you must perform a slow mode boot in order to perform extended diagnostic testing.

Note: A slow mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in the subsequent steps.

Perform the following tasks:

1. Record any reference codes appearing in the control panel or the HMC.
2. Shut down all the logical partitions and the server.
3. In the navigation area, select **Server and Partitions** → **Server Management**.
4. Select the server you want to perform a slow boot on.
5. Select **Selected** → **Properties**.
6. Click the **Power-On Parameters** tab.
7. In the Advanced Options section of the window, click the **Show details** button.
8. Record the current boot setting in the power-on speed override box and select **Slow** in the power-on speed override list.

Note: These settings apply to all future boots. After you complete the service action, change the settings back to what you recorded in step 8.

9. Click **OK**.
10. After completing the tasks, return to the step in the procedure that caused you to perform a slow boot. This ends the procedure.

8.2 Useful commands

The commands that are used to manage system startup, shutdown, and related tasks are discussed in the following sections.

Using the `alog` command

There might be instances when you must trace the boot process and obtain it if something went wrong with the system during the boot process. AIX 5L provides you with an excellent tool to monitor these problems with the `alog` command.

The `alog` command maintains and manages logs. It reads standard input, writes to standard output, and copies the output into a fixed-size file. This file is treated as a circular log. If the file is full, new entries are written over the oldest existing entries.

The `alog` command works with the log files that are specified in the command line or with logs that are defined in the `alog` configuration database.

The most common flags used with the `alog` command and their descriptions are provided in Table 8-3.

Table 8-3 Command flags for the `alog` command

Flag	Description
<code>-f LogFile</code>	Specifies the name of a log file. If the specified log file does not exist, one is created. If the <code>alog</code> command is unable to write to the log file, it writes to <code>/dev/null</code> .
<code>-L</code>	Lists the log types currently defined in the <code>alog</code> configuration database. If you use the <code>-L</code> flag with the <code>-t LogType</code> flag, the attributes for a specified LogType are listed.
<code>-o</code>	Lists the contents of the log file. Writes the contents of the log file to standard output in sequential order.
<code>-q</code>	Copies standard input to the log file, but does not write to standard output.
<code>-t</code>	Identifies a log defined in the <code>alog</code> configuration database. The <code>alog</code> command gets the log's file name and size from the <code>alog</code> configuration database.

Following are some examples of the `alog` command:

- ▶ To view the boot log, run the following command:

```
# alog -o -t boot
```

- ▶ To record the current date and time in a log file named `/tmp/mylog`, run the following command:

```
# date | alog -f /tmp/mylog
```

- ▶ To view the list of logs defined in the `alog` database, run:

```
# alog -L
```

Using the `bootlist` command

The `bootlist` command allows you to display and alter the list of boot devices from which the system can be booted. When the system is booted, it scans the devices in the list and attempts to boot from the first device it finds containing a boot image. This command supports the updation of the following boot lists:

- ▶ Normal boot list

The normal list designates possible boot devices for when the system is booted in normal mode.

- ▶ Service boot list

The service list designates possible boot devices for when the system is booted in service mode.

- ▶ Previous boot device

This entry designates the last device from which the system booted. Some hardware platforms might attempt to boot from the previous boot device before looking for a boot device in one of the other lists.

Support of these boot lists varies from platform to platform. Some platforms do not have boot lists. When searching for a boot device, the system selects the first device in the list and determines if it is bootable. If no boot file system is detected on the first device, the system moves on to the next device in the list. Because of this, the ordering of devices in the device list is extremely important.

The general syntax of the command is as follows:

```
# bootlist [ { {-m Mode } [ -r ] [ --o ] [ [ --i ] | [ [ --f File ] ] ] } [ Device [Attr=Value ...] ... ] ]
```

The most common flags used with the `bootlist` command are provided in Table 8-4.

Table 8-4 Command flags for the `bootlist` command

Flag	Description
<code>-m mode</code>	Specifies which boot list to display or alter. Possible values for the mode variable are normal, service, both, or prevboot.

Flag	Description
-f <i>File</i>	Indicates that the device information is to be read from the specified file name
-i	Indicates that the device list specified by the -m flag should be invalidated
-o	Displays bootlist with the -m flag. Applies only to AIX 5L V4.2 or later.
-r	Indicates whether to display the specified bootlist after any specified alteration is performed.

Some examples of the **bootlist** command are:

- ▶ To display a boot list (AIX 5L V4.2 or later), use the following command:

```
# bootlist -m normal -o
fd0
cd0
hdisk0
```

- ▶ To make changes to your normal boot list, use the following command:

```
# bootlist -m normal hdisk0 cd0
```

8.3 The /etc/inittab file

The /etc/inittab file has the same purpose in both the operating systems, that is, when the kernel loads the /sbin/init program, it reads this file to see what the default run level is and what scripts must be run. After initialization, the information in this file is used whenever the administrator changes the run level of the system.

If you modify the /etc/inittab file and want to instruct init to reload it, do so with the **init q** or the **init Q** commands.

The syntax of this file is almost the same in both Solaris and AIX. For more information about this file, refer to the man page for **inittab**.

8.3.1 Startup process in Solaris

The `/etc/inittab` file is configured in Solaris to reach run level 3, by first running the scripts for run level 2 and then the scripts for run level 3. But in AIX, there is only one set of scripts for each run level, meaning that for run level 2, the `init` program runs only the scripts for run level 2 if they have been assigned the value 2 in the `inittab` file. It does not run the lower run level scripts to get to its intended run level. Pay extra attention to where you are manually placing an `rc` script.

8.3.2 Startup process in AIX 5L

The `/etc/inittab` file (Figure 8-1 on page 229) lists the processes that `init` starts. It also specifies when to start them. If this file gets corrupted, the system does not boot properly. It is useful to keep a backup of this file. The default run level on AIX 5L is run level 2.

The fields are:

► identifier

Up to 14 characters that identify the process. Terminals use their logical device name as an identifier.

► runlevel

Defines what run levels the process is valid for. AIX 5L uses run levels of 0 - 9. If the `telinit` command is used to change the run level, a `SIGTERM` signal is sent to all the processes that are not defined for the new run level. If, after 20 seconds, a process has not terminated, a `SIGKILL` signal is sent. The default run level for the system is 2, which is AIX 5L multiuser mode.

► action

How to treat the process. The valid actions are:

– respawn

If the process does not exist, start the process. Do not wait for its termination. Continue scanning the `/etc/inittab` file. Restart the process when it dies. If the process exists, do nothing and continue scanning the `/etc/inittab` file.

– ondemand

Functionally identical to `respawn`, except that this action applies to the `a`, `b`, or `c` values, not to run levels.

- wait

When the **init** command enters the run level that matches the entry's run level, start the process and wait for its termination. All the subsequent reads of the `/etc/inittab` file when the **init** command is in the same run level causes the **init** command to ignore this entry.

- once

When the **init** command enters a run level that matches the entry's run level, start the process, and do not wait for its termination. When it dies, do not restart the process. When the system enters a new run level, and the process is still running from a previous run level change, the program will not be restarted. All the subsequent reads of the `/etc/inittab` file when the **init** command is in the same run level causes the **init** command to ignore this entry.

- sysinit

Entries of this type are executed before the **init** command tries to access the console before login. It is expected that this entry will only be used to initialize the devices on which the **init** command might try to ask the run level question. These entries are executed and waited for before continuing.

- off

If the process associated with this entry is currently running, send the warning signal (SIGTERM), and wait 20 seconds before terminating the process with the kill signal (SIGKILL). If the process is not running, ignore this entry.

- command

The AIX 5L command to run to start the process.

- boot

Process the entry only during system boot, which is when the **init** command reads the `/etc/inittab` file during system startup. Start the process, do not wait for its termination, and when it dies, do not restart the process. For the instruction to be meaningful, the run level must either be the default or it must match the **init** command's run level at boot time. This action is useful for an initialization function following a hardware reboot of the system.

- powerfail

Execute the process associated with this entry only when the **init** command receives a power fail signal (SIGPWR).

- powerwait

Execute the process associated with this entry only when the **init** command receives a power fail signal (SIGPWR), and wait until it terminates before continuing to process the /etc/inittab file.

- bootwait

Process the entry the first time the **init** command goes from the single user state to the multiuser state after the system is booted. Start the process, wait for its termination, and when it dies, do not restart the process. If the initdefault is 2, run the process immediately after the boot.

- initdefault

An entry with this action is only scanned when the **init** command is initially invoked. The **init** command uses this entry, if it exists, to determine which run level to enter initially. It does this by taking the highest run level specified in the run level field, and uses that as its initial state. If the run level field is empty, this is interpreted as 0123456789. Therefore, the **init** command enters run level 9. Additionally, if the **init** command does not find an initdefault entry in the /etc/inittab file, it requests an initial run level from the user at boot time.

Figure 8-1 shows an sample AIX 5L /etc/inittab file.

```
: Note - initdefault and sysinit should be the first and second entry.
:
init:2:initdefault:
brc::sysinit:/sbin/rc.boot 3 >/dev/console 2>&1 # Phase 3 of system boot
powerfail::powerfail:/etc/rc.powerfail 2>&1 | alog -tboot > /dev/console # Power
Failure Detection
mkatmpvc:2:once:/usr/sbin/mkatmpvc >/dev/console 2>&1
atmsvcd:2:once:/usr/sbin/atmsvcd >/dev/console 2>&1
load64bit:2:wait:/etc/methods/cfg64 >/dev/console 2>&1 # Enable 64-bit execs
tunables:23456789:wait:/usr/sbin/tunrestore -R > /dev/console 2>&1 # Set tunable
s
rc:23456789:wait:/etc/rc 2>&1 | alog -tboot > /dev/console # Multi-User checks
fbcheck:23456789:wait:/usr/sbin/fbcheck 2>&1 | alog -tboot > /dev/console # run
/etc/firstboot
srcmstr:23456789:respawn:/usr/sbin/srcmstr # System Resource Controller
rctcpip:23456789:wait:/etc/rc.tcpip > /dev/console 2>&1 # Start TCP/IP daemons
sniinst:2:wait:/var/adm/sni/sniprei > /dev/console 2>&1
rcnfs:23456789:wait:/etc/rc.nfs > /dev/console 2>&1 # Start NFS Daemons
cron:23456789:respawn:/usr/sbin/cron
pio:2:wait:/usr/lib/lpd/pio/etc/pioint >/dev/null 2>&1 # pb cleanup
cons:0123456789:respawn:/usr/sbin/getty /dev/console
sqdaemon:23456789:wait:/usr/bin/startsrc -sqdaemon
writesrv:23456789:wait:/usr/bin/startsrc -swritesrv
uprintfd:23456789:respawn:/usr/sbin/uprintfd
shdaemon:2:off:/usr/sbin/shdaemon >/dev/console 2>&1 # High availability daemon
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
l7:7:wait:/etc/rc.d/rc 7
l8:8:wait:/etc/rc.d/rc 8
l9:9:wait:/etc/rc.d/rc 9
naudio::boot:/usr/sbin/naudio > /dev/null
ntbl_reset:2:once:/usr/bin/ntbl_reset_datafiles
rcml:2:once:/usr/sni/aix53/rc.ml > /dev/console 2>&1
logsymp:2:once:/usr/lib/ras/logsymptom # for system dumps
perfstat:2:once:/usr/lib/perf/libperfstat_updt_dictionary >/dev/console 2>&1
diagd:2:once:/usr/lpp/diagnostics/bin/diagd >/dev/console 2>&1
ctrmc:2:once:/usr/bin/startsrc -s ctrmc > /dev/console 2>&1
ha_star:h2:once:/etc/rc.ha_star >/dev/console 2>&1
webserverstart:2:once: >/dev/null 2>&1
```

Figure 8-1 Sample AIX 5L /etc/inittab file

The format of the /etc/inittab is:

id:runlevel:action:command

The inittab file is reread by the init daemon every 60 seconds. The **telinit q** command is required only if you cannot wait for the next 60-second check.

To list all the entries that are currently in the `/etc/inittab` file, use the following command:

```
# lsitab -a
```

To add records into the `inittab` file, use the `mkinitab` command, for example, to add an entry for `tty4`, enter the following command:

```
# mkinitab "tty4:2:respawn:/usr/sbin/getty /dev/tty4"
```

Use the `-i` option to add records after a particular entry.

To change the currently existing entries from this file, use the `chinitab` command, for example, to change `tty4`'s run level, enter the following command:

```
# chinitab "tty4:23:respawn:/usr/sbin/getty /dev/tty4"
```

To remove the currently existing entries from this file, use the `rmitab` command, for example, to remove the `tty` entry shown previously, enter the following command:

```
# rmitab tty4
```

8.3.3 AIX 5L run levels

AIX 5L uses a default run level of 2. This is the normal multiuser mode. AIX 5L does not follow the System V R4 run level specification with special meanings for run levels 0, 3, 5, and 6. In AIX 5L, run levels of 0 - 1 are reserved, 2 is the default, and 3 - 9 can be defined according to the system administrator's preference.

There are three other values that appear in the run level field, even though they are not true run levels: `a`, `b`, and `c`. Entries that have these characters in the run level field are processed only when the `telinit` command requests them to be run (regardless of the current run level of the system). They differ from run levels, in that, the `init` command can never enter run level `a`, `b`, or `c`. Also, a request for the execution of any of these processes does not change the current run level. Furthermore, a process started by an `a`, `b`, or `c` command is not killed when the `init` command changes levels. They are only killed if their line in the `/etc/inittab` file is marked off in the action field, their line is deleted entirely from `/etc/inittab`, or the `init` command goes into single-user mode.

The `telinit` command can be used to change the run level of the system. This can also be accomplished by using the `smitty telinit` fast path. When the `telinit` command is used to change the run level, the system begins to respond by telling you which processes are terminating or starting as a result of the change in the run level.

Use the **shutdown -m** command to enter maintenance mode. When the system enters maintenance mode from another run level, only the system console is used as the terminal.

Each run level has a set of scripts associated with it called run control (rc) files.

In Solaris, each run level has a master script, `/sbin/rcX`, where X is the run level, and an associated directory in `/etc/rcX.d/`, where X is again the run level.

When entering a run level, the init program starts the corresponding `/sbin/rcX` script, which in turn executes the associated scripts from `/etc/rcX.d/`.

For AIX, run-level scripts allow users to start and stop selected applications when changing the run level. Scripts beginning with “K” are stop scripts and scripts beginning with “S” are start scripts.

These scripts reside on the subdirectory that is specific to the run level they belong to. Each subdirectory has the form `rcn.d`, where n is the run level:

- ▶ `/etc/rc.d/rc2.d`
- ▶ `/etc/rc.d/rc3.d`
- ▶ `/etc/rc.d/rc4.d`
- ▶ `/etc/rc.d/rc5.d`
- ▶ `/etc/rc.d/rc6.d`
- ▶ `/etc/rc.d/rc7.d`
- ▶ `/etc/rc.d/rc8.d`
- ▶ `/etc/rc.d/rc9.d`

The `/etc/rc.d/rc` script runs the start script it finds in the specified directory and executes it when the run level changes. The script first runs the stop application scripts, and then runs the start application scripts.

System Resource Controller

Many lines in the `/etc/inittab` file contain one or several System Resource Controller (SRC) statements. The SRC provides a set of commands to make it easier for the administrator to control the subsystems.

A subsystem group is a group of any specified subsystems. The grouping systems together allow the control of several subsystems at one time, for example, TCP/IP, Systems Network Architecture (SNA), Network Information Service (NIS), and Network File System (NFS).

A subserver is a program or process that belongs to a subsystem. A subsystem can have multiple subservers and is responsible for starting, stopping, and providing the status of subservers.

Subservers are started when their parent subsystems are started. If you try to start a subservier and its parent subsystem is not active, the `startsrc` command starts the subsystem also. The relationship between the group and the subsystem can easily be seen from the output of `lssrc -a`.

Following are some examples of this command:

- ▶ To list the SRC status, run the command shown in Example 8-1.

Example 8-1 SRC status

```
# lssrc -g nfs
Subsystem      Group          PID           Status
biod           nfs            11354         active
rpc.lockd      nfs            11108         active
nfsd           nfs                        inoperative
rpc.statd      nfs                        inoperative
rpc.mountd     nfs                        inoperative
```

- ▶ To list the long status of a subsystem, run the command as shown in Example 8-2.

Example 8-2 Long-format SRC status

```
# lssrc -ls inetd
Subsystem      Group          PID           Status
inetd         tcpip          10322         active

Debug          Not active

Signal         Purpose
SIGALRM       Establishes socket connections for failed services.
SIGHUP        Rereads the configuration database and reconfigures
services.

SIGCHLD       Restarts the service in case the service ends abnormally.

Service       Command          Description          Status
cmsd          /usr/dt/bin/rpc.cmsd  cmsd 100068 2-5      active
ttdbserver   /usr/dt/bin/rpc.ttdbserver  rpc.ttdbserver 100083 1
active

dpc1SD       /etc/dpc1SD      dpc1SD /etc/dpc1d      active
pmdv4       /etc/pmdv4       pmdv4                active
dtspc       /usr/dt/bin/dtspcd  /usr/dt/bin/dtspcd  active
time        internal          active
daytime     internal          active
time        internal          active
```

daytime	internal		active
ntalk	/usr/sbin/talkd	talkd	active
exec	/usr/sbin/rexecd	rexecd	active
login	/usr/sbin/rlogind	rlogind	active
shell	/usr/sbin/rshd	rshd	active
telnet	/usr/sbin/telnetd	telnetd -a	active
ftp	/usr/sbin/ftpd	ftpd	active

- ▶ To start a subsystem, run:

```
# startsrc -s lpd
0513-059 The lpd Subsystem has been started. Subsystem PID is 24224.
```

- ▶ To stop a subsystem, run:

```
# stopsrc -s lpd
0513-044 The lpd Subsystem was requested to stop.
```

For more information about the AIX 5L boot and startup process, refer to the following publications:

- ▶ Systems Management Guide: Operating Systems and Devices" section of the System p AIX Collaboration Center Commands Reference
- ▶ *IBM eServer Certification Study Guide - pSeries AIX System Administration*, SG24-6191
<http://www.redbooks.ibm.com/abstracts/sg246191.html>
- ▶ *IBM eServer Certification Study Guide - AIX 5L Installation and System Recovery*, SG24-6183
<http://www.redbooks.ibm.com/abstracts/sg246183.html?Open>

8.4 System shutdown

Mission critical UNIX servers are made to be left powered on continuously. However, you have to halt or shut down the system and sometimes remove the power when performing some maintenance tasks. These tasks could include the following:

- ▶ Turning off a system's power due to an anticipated power outage
- ▶ Adding or removing system hardware that is not hot-pluggable or hot-swappable
- ▶ Moving a system from one location to another

In Solaris you can use **shutdown**, **init**, **telinit**, and the **halt** commands to bring the system down. In AIX, **shutdown** and **halt** are the main commands. For **init** and **telinit**, there is no predefined level for bringing the system down. However, an init level can be customized to do this.

Solaris

In Solaris, one of the most commonly used methods for shutting down is the **init** command. The command format is **init** [0123456s].

- ▶ To shut down the system and reach the programmable read-only memory (PROM) monitor level, run the following:

```
# init 0
```

- ▶ To perform a simple reboot, run the following:

```
# init 6
```

Note: When using the **init** command, no shutdown message is sent to the users. The **init** command performs a clean shutdown.

Solaris also has the **shutdown** command. The command format is:

```
shutdown [ -y ] [ -g seconds ] [ -i init state ] [ message ]
```

- ▶ The **-y** flag continues to shut down the machine without further intervention. If it is not specified, users are asked whether they want to continue or not after 60 seconds.
- ▶ The **-g** flag indicates the time in seconds before the system is shut down. The default is 60 seconds.
- ▶ The **-i** flag brings the system to an init state that is different from the default of S. The choices are 0, 1, 2, 5, and 6.

AIX

For AIX, the **shutdown** command is the most useful command because it has more options available.

The **shutdown** command halts the OS. Only a user with root user authority can run this command. During the default shutdown, users are notified (by a **wall** command) of the impending system shutdown with a message. However, shutdown is not complete until the user receives a shutdown completion message.

Important: Do not attempt to restart the system or turn off the system before the shutdown completion message is displayed. Otherwise, file system damage might occur.

When the shutdown time approaches, warning messages are displayed on the terminals of all the users on the system.

Note: The “Hal t Completed” message is not displayed in the tty from which the shutdown is invoked if it is connected to the system through a multiport adapter.

After the specified number of seconds (60 by default), the system stops the accounting and error logging processes and writes an entry to the error log. The **shutdown** command then runs the **killall** command to end any remaining processes and the **sync** command to flush all the memory resident disk blocks. Finally, it unmounts the file systems and calls the **halt** command.

Note: Users who have files open on the node that is running the **shutdown** command, but are not logged into that node, are *not* notified about the shutdown.

If you request a complete halt to the OS, the **shutdown** command stops all the processes, unmounts all the file systems, and calls the **halt** command.

The system administrator can place local customized shutdown procedures in a shell script named `/etc/rc.shutdown`. If it exists, this script runs at the beginning of the shutdown. If the script runs, but fails with a non-zero return code, the shutdown stops. Table 8-5 shows the shutdown options.

Attention: If you are bringing the system down to maintenance mode, run the **shutdown** command from the `/(root)` directory to ensure that it can cleanly unmount the file systems.

Table 8-5 Shutdown options

Flag	Explanation
-d	Brings the system down from a distributed mode to a multiuser mode
-F	Performs a quick shutdown, bypassing the messages to other users and bringing the system down as quickly as possible
-h	Halts the OS completely
-i	Specifies interactive mode. Displays the interactive messages to guide the user through the shutdown.

Flag	Explanation
-k	Allows the administrator to broadcast the shutdown warning messages without causing the system to shut down. When the -k flag is used, no other shutdown activity, except sending messages occurs, for example, no processes are killed, no activity is logged in /etc/shutdown.log if the -l flag is specified, and if an /etc/rc.shutdown script exists, it does not run.
-m	Brings the system down to maintenance (single-user) mode.
-r	Restarts the system after being shut down with the reboot command.
-l	Creates or appends the /etc/shutdown.log file that contains information about the file systems, daemons, user login, licensing services, and the network interfaces being brought down. The file might be used for diagnostic and debugging purposes in the event of shutdown failures.
-t	Restart the system on the date specified by using the following: mmddHHMM [yy] Here, mm specifies the month.

To turn off the machine, use the **shutdown** command. This shuts down the system, waiting for a minute before stopping the user processes and the init process.

To give users more time to finish what they are doing and bring the system to maintenance mode, use the following command:

```
shutdown -m +2
```

This brings the system down from multiuser mode to maintenance mode after waiting for two minutes.

To restart the machine as quickly as possible, use the following command:

```
shutdown -Fr now
```

The file /usr/sbin/shutdown contains the **shutdown** command.

Using the halt command

The **halt** command writes data to the disk and then stops the processor. The machine does *not* restart.

Following are a few considerations that you must keep in mind when using the **halt** command:

- ▶ Only a root user should run this command.
- ▶ Do not use this command if other users are logged into the system. If no other users are logged in, the **halt** command can be used.

- ▶ Use the **halt** command if you are not going to restart the machine immediately or if the **shutdown** command hangs or fails for some reason.
- ▶ When the message “halt completed” is displayed, turn the power off.

For more information refer to the system manual page for halt:

```
# man halt
```

8.5 Network booting

Sometimes, it is useful to boot from the network. Both Solaris and AIX 5L support network booting. This section describes how to set up a machine to act as a network boot server and how to boot an AIX 5L system from the network as a client.

Solaris network boot server setup

In Solaris, configure the services as shown in Table 8-6.

Table 8-6 Solaris network boot services

Service	Description
rarp	For serving IP address information
bootparams	For boot information
dhcp	Can be used instead of rarp and bootparams for network boot configuration
tftp	For serving the proper kernel from /tftpboot
nfs	For sharing file systems

This task can be performed manually (editing the configuration files), or automatically (using the `add_install_client` script from the installation CD or DVD).

AIX 5L network boot server setup

When a node boots over the network, it issues a bootp request on that network, specifying its network device hardware address. The boot/install server has a list of nodes it boots and their associated hardware Ethernet addresses. Therefore, it replies to only those bootp requests for which it has an entry.

The following entries are required in `/etc/inetd.conf` of your boot server to allow the network boot of remote systems:

- ▶ `bootps dgram udp wait root /usr/sbin/bootpd bootpd /etc/bootptab`
- ▶ `tftp dgram udp6 SRC nobody /usr/sbin/tftpd tftpd`

The best solution for setting up a boot server is to use Network Installation Management (NIM). For more information about setting up NIM master and NIM clients, refer to 3.9.2, “Network Installation Management setup” on page 69.



Managing system resources

This chapter describes the differences in managing the system resources of Solaris and AIX 5L. It provides details about the differences in the system resources, along with the concepts, tasks, and commands used to control them.

This chapter discusses the following topics:

- ▶ 9.1, “Displaying system information” on page 240
- ▶ 9.2, “Resource management” on page 243
- ▶ 9.3, “Starting and stopping the system services” on page 250
- ▶ 9.4, “Scheduling services” on page 254
- ▶ 9.5, “Quotas” on page 256
- ▶ 9.6, “Process accounting” on page 259
- ▶ 9.7, “Management tools” on page 260

9.1 Displaying system information

Table 9-1 shows the basic information pertaining to the differences in the Solaris and the AIX 5L operating systems (OS).

Table 9-1 Basic information

System information task	Solaris	AIX 5L
System information	uname	uname
Processor information	prtdiag or psrinfo	lsdev or lsattr
Memory size	prtdiag or prtconf	lsattr -El mem0
Mounted file system information	df	df
File usage	du	du
Host name information	host name or uname -n	host name or uname -n
Serial number	N/A	lsattr -El sys0 grep system
List process	prstat top ps	nmon topas ps
Adapter location	prtdiag, cfgadm or cat /etc/path_to_inst	lsdev lscfg or lsslot
Network IP	ifconfig	ifconfig
Network route	route	route
Network connection feature	ndd or kstat	netstat -v

Examples on AIX 5L

Example 9-1 shows the command for obtaining processor information.

Example 9-1 Processor information

```
# /usr/sbin/lsdev -Cc processor
proc0 Available 00-00 Processor
# /usr/sbin/lsattr -El proc0
```

frequency	1656408000	Processor Speed	False
smt_enabled	true	Processor SMT enabled	False
smt_threads	2	Processor SMT threads	False
state	enable	Processor state	False
type	PowerPC_POWER5	Processor type	False

Example 9-2 shows the command to obtain information pertaining to the memory.

Example 9-2 Memory information

```
# /usr/sbin/lsdev -Cc memory
L2cache0 Available L2 Cache
mem0 Available Memory
# /usr/sbin/lsattr -El mem0
goodsize 1024 Amount of usable physical memory in Mbytes False
size 1024 Total amount of physical memory in Mbytes False
```

Example 9-3 shows the command to obtain model and serial number.

Example 9-3 Model and serial number

```
# /usr/sbin/lsattr -El sys0 | egrep "modelName|systemid"
modelName IBM,9113-550 Machine name
False
systemid IBM,02104790E Hardware system identifier
False
```

Example 9-4 shows the command to obtain network information.

Example 9-4 Network information

```
# /usr/bin/netstat -v
-----
ETHERNET STATISTICS (ent0) :
Device Type: Virtual I/O Ethernet Adapter (1-lan)
Hardware Address: ba:8e:30:00:40:02
Elapsed Time: 0 days 20 hours 41 minutes 45 seconds

Transmit Statistics:                                Receive Statistics:
-----
Packets: 17751                                       Packets: 208111
Bytes: 2087592                                       Bytes: 16661193
Interrupts: 0                                         Interrupts: 187222
Transmit Errors: 0                                    Receive Errors: 0
Packets Dropped: 0                                   Packets Dropped: 0
```

```

Max Packets on S/W Transmit Queue: 0
S/W Transmit Queue Overflow: 0
Current S/W+H/W Transmit Queue Length: 0

Elapsed Time: 0 days 20 hours 41 minutes 44 seconds
Broadcast Packets: 56
Multicast Packets: 2
No Carrier Sense: 0
DMA Underrun: 0
Lost CTS Errors: 0
Max Collision Errors: 0
Late Collision Errors: 0
0
Deferred: 0
0
SQE Test: 0
Timeout Errors: 0
Adapter: 0
Single Collision Count: 0
Multiple Collision Count: 0
Current HW Transmit Queue Length: 0

Bad Packets: 0
Broadcast Packets: 188705
Multicast Packets: 6
CRC Errors: 0
DMA Overrun: 0
Alignment Errors: 0
No Resource Errors: 0
Receive Collision Errors:
Packet Too Short Errors:
Packet Too Long Errors: 0
Packets Discarded by
Receiver Start Count: 0

```

General Statistics:

```

-----
No mbuf Errors: 0
Adapter Reset Count: 0
Adapter Data Rate: 20000
Driver Flags: Up Broadcast Running
                Simplex 64BitSupport DataRateSet

```

Virtual I/O Ethernet Adapter (1-lan) Specific Statistics:

```

-----
RQ Length: 4481
No Copy Buffers: 0
Trunk Adapter: False
Filter MCast Mode: False
Filters: 255
    Enabled: 1 Queued: 0 Overflow: 0
LAN State: Operational

```

```

Hypervisor Send Failures: 0
    Receiver Failures: 0
    Send Errors: 0

```

Hypervisor Receive Failures: 0

ILLAN Attributes: 0000000000000000 [0000000000000000]

Buffers	Reg	Alloc	Min	Max	MaxA	LowReg
tiny	512	512	512	2048	512	510
small	512	512	512	2048	512	510
medium	128	128	128	256	128	128
large	24	24	24	64	24	24
huge	24	24	24	64	24	24

9.2 Resource management

On Solaris 9 and AIX 5L V5.3 OS, there are two basic ways in which to work with resource management.

The first relates to hardware compatibility and is called *domains* in Solaris and *logical partitions* (LPAR) in AIX 5L. In this method, you have separate OS running in each domain or LPAR. Domains or LPARs provide absolute OS separation. Thus, a task within one domain cannot affect other domains.

The name used to describe changing resources dynamically in a domain is *dynamic reconfiguration* in Solaris and *dynamic logical partitioning* (DLPAR) in AIX 5L.

The other way of working with resource management involves using a tool for managing resources in the same OS. On Solaris servers, it is called Solaris Resource Manager. On AIX 5L, a similar tool is called AIX 5L Work Load Manager.

Another option is available in AIX 5L called Reliable Scalable Cluster Technology (RSCT). This is a set of software components that together provide a comprehensive clustering environment.

9.2.1 Solaris domains and dynamic reconfiguration

It is important to understand the concepts of domains and dynamic reconfiguration in Solaris in order to make a comparison with the new features available in AIX 5L.

In summary, to understand how domains run on Sun servers, refer to the hardware manual and specifications. In general, for high-end servers, one domain comprises a number of system boards and input/output (I/O) boards. The

CPU and memory reside on the system boards, and the adapters reside on the I/O boards. On IBM servers, you work directly with a number of processors, memory, and adapters. This is a more flexible solution for administrators.

Therefore, for dynamic reconfiguration on Sun high-end servers, if you do not have processors or memory on the system boards attached to a domain, you have to add another system board.

9.2.2 Solaris Resource Manager

Solaris Resource Manager (SRM) software can be used for more advanced resource management and control.

SRM consists of two rather disparate functions, resource limitations and fair-share scheduling. Think of resource limitations as an extension of the standard “limits” that can be set within Solaris. Fair-share scheduling is a new scheduler that manages CPU scheduling based on the allocated shares, instead of the usual “use-the-most-CPU-cycles” kind of scheduling.

SRM is *not* a replacement for domain or other “pure” resource use limiters, that is, an OS crash takes down all the processes on that system (or within that domain), including all the SRM jobs. SRM can therefore, help optimize the use of a system and allow programs that might usually be mutually exclusive, to live in harmony on a system.

Dynamic reconfiguration allows resources to move between domains, but testing and planning must occur, and issues such as memory allocation must be resolved (because an application suddenly has more memory available). SRM is more flexible, but does not provide a wall between applications. It must be used when fine-grained resource control is required, when resource-use changes might be frequent, and on systems that do not have domain available. Of course, it can be used in conjunction with domains for the most complete set of solutions.

9.2.3 AIX 5L logical partitioning, dynamic LPAR, and virtualization

In AIX 5L, LPAR management is simple and efficient. It is different from Solaris, in that, all the dynamic reconfigurations or dynamic LPARs (DLPARs) work directly on resource, without preoccupation with system boards or I/O boards.

This technology provides fine-tuning capability and resource allocation capability of system resources, enabling better utilization of the system resources.

With shared processor LPARs on IBM p5 servers, multiple AIX 5L partitions can simultaneously use individual processors, memory modules, and I/O adapters. Furthermore, each partition can draw on resources from multiple CPUs to meet

the requirements of a particular workload. Administrators can configure up to 10 instances of OS per CPU, whereby a partition can utilize the resources of a single CPU in increments of 1/100. The superior granularity allows workloads to be assigned to AIX 5L resources with great precision. By contrast, Sun's dynamic domains must be configured along the boundaries of four CPU processor boards.

AIX 5L V5.3 running on POWER 5 and later based systems supports the sharing of I/O across partitions. Using this capability, Ethernet adapters and fibre channel adapters can be shared among multiple partitions. Small Computer System Interface (SCSI) disks can also be virtualized and then shared across multiple partitions, allowing partitions to boot from the internal SCSI disks. Administrators can, for example, take a 200 GB SCSI disk, segment it into 10 GB chunks, and assign these 10 GB chunks to 20 partitions, in which each chunk becomes a virtual disk.

For more information about partition implementations on p5, refer to *Partitioning Implementations for IBM eServer p5 Servers*, SG24-7039, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg247039.pdf>

9.2.4 AIX 5L Partition Load Manager

The Partition Load Manager (PLM) for AIX 5L is designed to automate the administration of memory and CPU resources across LPARs within a single central electronics complex (CEC). To improve resource usage, PLM automates the migration of these resources between partitions, based on partition loads and priorities. Partitions with a high demand receive resources donated by or taken from partitions with a low demand. A user-defined policy governs how resources are moved. PLM does not contradict the partition definitions in the Hardware Management Console (HMC). On the contrary, it adds additional flexibility on top of the micropartitioning capability provided by the IBM POWER Hypervisor™.

LPARs are the major tools in server consolidation. But how can you manage them? PLM is the solution for this.

PLM is a part of the Advanced POWER Virtualization feature. It is supported on both the dedicated and the shared processor partitions of IBM System p5 servers running AIX 5L V5.3 or AIX 5L V5.2 (ML4) or later. It can be started in either of the following modes:

- ▶ In *monitoring mode*, PLM reports provide a number of statistics on resource usage in the managed partitions.

- ▶ In *management mode*, PLM initiates dynamic reconfiguration operations in order to match system resources with partition workload in accordance with the defined policy.

For complete information about how to work with PLM, refer to Chapter 7 of *Advanced POWER Virtualization on IBM System p5*, SG24-7940, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg247940.pdf>

9.2.5 AIX 5L Work Load Manager

AIX 5L Workload Manager (WLM) and Solaris Resource Manager allows the system administrator to divide resources between jobs. AIX 5L WLM, as part of the Base Operating System (BOS), provides isolation between user communities with different system behaviors. This prevents effective starvation of workloads with certain characteristics (interactive or low CPU usage jobs) and by workloads with other characteristics (batch or high memory usage jobs). CPU time, memory, and I/O bandwidth are managed separately. Therefore, different styles of applications can be managed.

AIX 5L WLM can ensure that at least a section of a process is stored in the memory by providing a minimum memory allocation to the process, ensuring that the entire process is never paged out. By contrast, the Solaris 9 Workload Manager software does *not* support minimum physical memory allocations. Also, AIX 5L WLM allows administrators to allocate disk I/O bandwidth in addition to processor resources and physical memory.

AIX 5L V5.3 WLM provides system administrators with more control over how the scheduler, Virtual Memory Manager (VMM), and the device drivers call and allocate CPU, physical memory, and I/O bandwidth to the class-based user, group, application path, process type, or application tags. It allows a hierarchy of classes to be specified, processes to be automatically assigned to classes by their characteristics, and manual assignment of processes to classes. Classes can be superclasses or subclasses. AIX 5L WLM self-adjusts when there are no jobs in a class or when a class does not use all the resources that are allocated to it. The resources are automatically distributed to other classes to match the policies of the system administrator.

Attention: Efficient use of AIX 5L WLM requires extensive knowledge of existing system processes and performance. If the system administrator configures AIX 5L WLM with extreme or inaccurate values, performance is significantly degraded.

Figure 9-1 shows an example of AIX 5L WLM implementation.

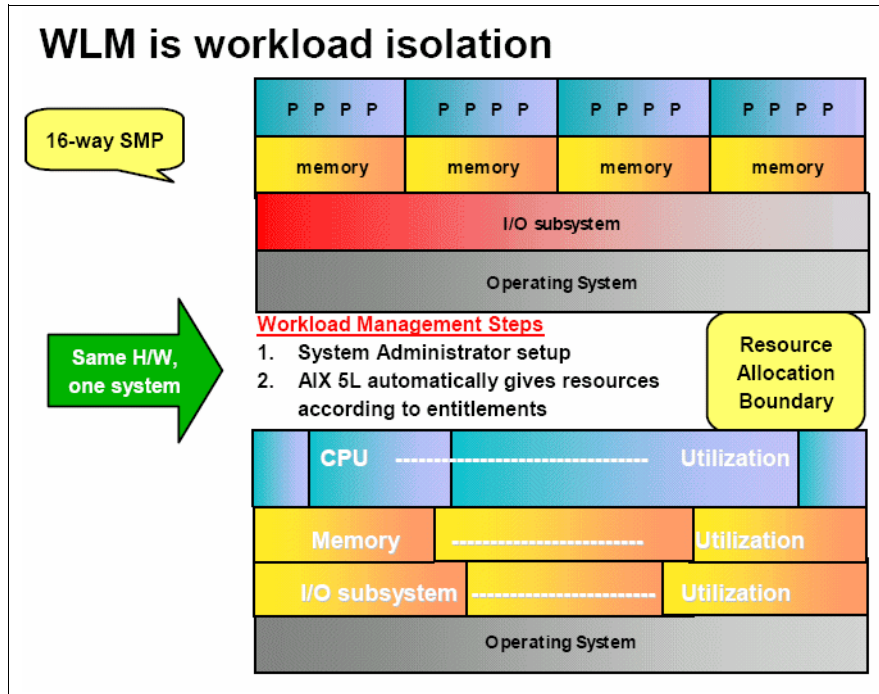


Figure 9-1 Example of WLM implementation

There is a useful menu administration for AIX 5L WLM that is shown in Figure 9-2. To start the smit menu, type `smit wlm`.

```
Workload Manager

Move cursor to desired item and press Enter.

Manage time-based configuration sets

Work on alternate configurations
Work on a set of Subclasses
Show current focus (Configuration, Class Set)

List all classes
Add a class
Change / Show Characteristics of a class
Remove a class
Class assignment rules

Start/Stop/Update WLM
Assign/Unassign processes to a class/subclass

F1=Help          F2=Refresh       F3=Cancel        F8=Image
F9=Shell         F10=Exit         Enter=Do
```

Figure 9-2 Workload Manager

For complete information about WLM, refer to *AIX 5L Workload Manager (WLM)*, SG24-5977, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg245977.html?open>

9.2.6 Reliable Scalable Cluster Technology

Reliable Scalable Cluster Technology (RSCT) is a set of software components that together provide a comprehensive clustering environment for AIX 5L and Linux. RSCT is the infrastructure used by a variety of IBM products to provide clusters with improved system availability, scalability, and ease-of-use. RSCT can also be used on stand-alone systems.

The basic RSCT components are:

- ▶ The Resource Monitoring and Control (RMC) subsystem

This is the scalable, reliable backbone of RSCT. It runs on a single machine or on each node (OS image) of a cluster and provides a common abstraction for the resources of the individual system or a cluster of nodes. You can use RMC for single-system monitoring or for monitoring nodes in a cluster. In a

cluster, however, RMC provides global access to subsystems and resources throughout the cluster, thus providing a single monitoring and management infrastructure for clusters.

- ▶ The RSCT core resource managers

A resource manager is a software layer between a resource (a hardware or software entity that provides services to some other component) and the RMC. A resource manager maps the programmatic abstractions in RMC into the actual calls and commands of a resource.

- ▶ The RSCT cluster security services

These provide the security infrastructure that enables RSCT components to authenticate the identity of other parties.

- ▶ The Topology Services subsystem

This provides, on some cluster configurations, node and network failure detection.

- ▶ The Group Services subsystem

This provides, on some cluster configurations, cross node/process coordination.

The same type of resources are defined into the resource classes. A resource class sets the common characteristics that the instances of the resource class can have, and the resource itself contains the specific characteristic value.

To display the classes available on your machine, issue the `lsrsrc` command, as shown in Example 9-5.

Example 9-5 Using the `lsrsrc` command

```
# lsrsrc
class_name
"IBM.Association"
"IBM.ATMDevice"
"IBM.AuditLog"
"IBM.AuditLogTemplate"
"IBM.Condition"
"IBM.EthernetDevice"
"IBM.EventResponse"
"IBM.FDDIDevice"
"IBM.Host"
"IBM.FileSystem"
"IBM.PagingDevice"
"IBM.PhysicalVolume"
"IBM.Processor"
```

```

"IBM.Program"
"IBM.TokenRingDevice"
"IBM.Sensor"
"IBM.Sfp"
"IBM.ServiceEvent"
"IBM.ManagementServer"
"IBM.NetworkInterface"
"IBM.HostPublic"
"IBM.DRM"
"IBM.WLM"
"IBM.LPAR"
"IBM.LPCommands"
#

```

9.3 Starting and stopping the system services

System services are defined as processes or daemons that usually run in the background. These are not associated with any user login, and have a user interface.

Solaris system services

In Solaris, the `/etc/rc*.d/` directory contains all the Solaris system startup and shutdown scripts, some of which are soft links to the actual file that resides in `/etc/init.d/`. Startup script names start with an “S” and shutdown scripts start with a “K”. To disable a service from running at startup time, a script is simply renamed so that it does not begin with a capital “S”. To manually start or stop a service, use the `/etc/init.d/service` (**start**, **stop**) commands.

AIX 5L system services

The OS service management in AIX 5L uses completely different concepts than the Solaris environment.

In AIX 5L, the services are divided into groups, subsystems and subservers.

Table 9-2 shows a summary of how to manage system services on AIX 5L.

Table 9-2 Managing system services on AIX 5L

Task	Command
List all subsystems	<code>lssrc -a</code>
List all subsystems of a specific group	<code>lssrc -g group_name</code>

Task	Command
List one subsystem	<code>lssrc -s subsystem_name</code>
Start all subsystems of a group	<code>startsrc -g group_name</code>
Start one subsystem	<code>startsrc -s subsystem_name</code>
Stop all subsystems of a group	<code>stopsrc -g group_name</code>
Stop one subsystem	<code>stopsrc -s subsystem_name</code>
Restart all subsystems of a specific group	<code>refresh -g group_name</code>
Restart one subsystem	<code>refresh -g subsystem_name</code>

Examples of subsystems and group management

This section provides examples of subsystems and group management.

Example 9-6 lists all the subsystems and their status.

Example 9-6 Listing all the subsystems and their status

```
# lssrc -a
Subsystem      Group          PID           Status
syslogd        ras            98398         active
sendmail       mail           102518        active
portmap        portmap        139382        active
inetd          tcpip         151650        active
snmpd          tcpip         196716        active
hostmibd       tcpip         110748        active
snmpmibd       tcpip         168074        active
aixmibd        tcpip         69810         active
muxatmd        tcpip         278666        active
qdaemon        spooler        237758        active
writesrv       spooler        209010        active
ctrmc          rsct           241804        active
IBM.ERRM       rsct_rm        254104        active
IBM.HostRM     rsct_rm        258182        active
IBM.CSMAgentRM rsct_rm        262306        active
IBM.ServiceRM  rsct_rm        274624        active
IBM.DRM        rsct_rm        221330        active
IBM.AuditRM    rsct_rm        127066        active
IBM.LPRM       rsct_rm        225420        active
lpd            spooler        0             inoperative
LUMlmd         lumls          0             inoperative
LUMgdb         lumls          0             inoperative
```

rwhod	tcpip	inoperative
xntpd	tcpip	inoperative
dpid2	tcpip	inoperative
dhcpcd	tcpip	inoperative
dhcpcd6	tcpip	inoperative
ndpd-host	tcpip	inoperative
ndpd-router	tcpip	inoperative
tftpd	tcpip	inoperative
gated	tcpip	inoperative
named	tcpip	inoperative
routed	tcpip	inoperative
iptrace	tcpip	inoperative
timed	tcpip	inoperative
dhcpsd	tcpip	inoperative
dhcpsdv6	tcpip	inoperative
dhcprd	tcpip	inoperative
mrouted	tcpip	inoperative
rsvpd	qos	inoperative
policyd	qos	inoperative
pxed	tcpip	inoperative
binld	tcpip	inoperative
dfpd	tcpip	inoperative
ypserv	yp	inoperative
ypupdated	yp	inoperative
yppasswdd	yp	inoperative
keyserv	keyserv	inoperative
ypbind	yp	inoperative
biod	nfs	inoperative
nfsd	nfs	inoperative
rpc.mountd	nfs	inoperative
automountd	autofs	inoperative
nfsrgyd	nfs	inoperative
gssd	nfs	inoperative
llbd	iforncs	inoperative
glbd	iforncs	inoperative
cpsd	ike	inoperative
tmd	ike	inoperative
isakmpd	ike	inoperative
cdromd		inoperative
i4lmd	iforls	inoperative
i4glbcd	iforncs	inoperative
i4gdb	iforls	inoperative
i4llmd	iforls	inoperative
nimsh	nimclient	inoperative
ctcas	rsct	inoperative


```

vert_serv      nrd          inoperative
rpc.lockd      nfs         inoperative
rpc.statd      nfs         inoperative
#

```

Example 9-7 lists all the subsystems of a group.

Example 9-7 Listing all the subsystems of a group

```

# /usr/bin/lssrc -g yp
Subsystem      Group        PID          Status
ypserv        yp           221300       inoperative
ypupdated      yp           221300       inoperative
yppasswdd     yp           221300       inoperative
ypbind        yp           221300       inoperative

```

Example 9-8 shows how to stop a subsystem.

Example 9-8 Stopping a subsystem

```

# /usr/bin/lssrc -s biod
Subsystem      Group        PID          Status
biod          nfs         221300       active
# stopsrc -s biod
0513-044 The biod Subsystem was requested to stop.
# lssrc -s biod
Subsystem      Group        PID          Status
biod          nfs         221300       inoperative
#

```

Example 9-9 shows how to start a subsystem.

Example 9-9 Starting a subsystem

```

# lssrc -s xntpd
Subsystem      Group        PID          Status
xntpd         tcpip       102562       inoperative
# startsrc -s xntpd
0513-059 The xntpd Subsystem has been started. Subsystem PID is 102562.
# lssrc -s xntpd
Subsystem      Group        PID          Status
xntpd         tcpip       102562       active

```

Example 9-10 shows how to restart a subsystem.

Example 9-10 Restarting a subsystem

```
# /usr/bin/lssrc -s inetd
Subsystem      Group          PID           Status
inetd         tcpip         82044        active
# refresh -s inetd
0513-095 The request for subsystem refresh was completed successfully.
```

Network services and inetd

Both Solaris and AIX 5L configure the network service ports through the `/etc/services` file, and both use the `/etc/inetd.conf` file to configure the `inetd` processes.

The `inetd` daemon provides Internet service management for a network. This daemon reduces the system load by invoking other daemons only when they are required and by providing several simple Internet services internally without invoking other daemons.

On Solaris servers, when restarting the `inetd` daemon, it is necessary to identify the process number and send a hang-up signal with the command `kill -HUP`. On AIX 5L, you can just use the command `refresh -s inetd`, as shown in Example 9-10.

9.4 Scheduling services

This section describes how to administrate scheduled tasks in Solaris and AIX 5L.

Using crontab

The concepts about `crontab` in Solaris and AIX 5L are the same. However, there are a few differences (Table 9-3).

Table 9-3 Crontab command options

Crontab option	Description on Solaris	Description on AIX 5L
-e	edit crontab	edit crontab
-r	remove crontab	remove crontab
-l	list crontab	list crontab
-v	N/A	crontab status

Table 9-4 shows how to start and stop crontab.

Table 9-4 Starting and stopping crontab

Crontab task	Solaris	AIX 5L
Start	/etc/init.d/cron start	Automatically by /etc/inittab
Stop	/etc/init.d/cron stop	<ul style="list-style-type: none"> ▶ 1- remove from inittab with "rmitab cron" ▶ 2- kill crontab process identification number (PID)
Restart	<ul style="list-style-type: none"> ▶ kill -HUP PID, or ▶ /etc/init.d/cron stop, and /etc/init.d/cron start 	Kill contab PID (be sure that cron is enabled on /etc/inittab)

Table 9-5 shows the crontab control files.

Table 9-5 Crontab control files

Task	Solaris	AIX 5L
Users allowed to use crontab	/etc/cron.d/cron.allow	/var/adm/cron/cron.allow
Users denied access to crontab	/etc/cron.d/cron.deny	/var/adm/cron/cron.deny
Spool area	/var/spool/cron/crontabs	/var/spool/cron/crontabs

Using at

You can use **at** for scheduling jobs to run at a later time. The job is executed in a separate invocation of the shell, running in a separate process group with no controlling terminal, except that the environment variables, the current working directory, the file creation mask, and the system resource limits are retained and used when the **at** job is executed.

The main difference with **at** options is that in Solaris it is possible to specify under which project the **at** or batch job will be run. When used with the **-l** option, it limits the search to that particular project. Values for the project are interpreted first as a project name, and then as a possible project ID, if entirely numeric. By default, the user's current project is used.

Table 9-6 describes the control files' differences for **at** in Solaris and AIX 5L.

Table 9-6 The "at" files

Description	File on Solaris	File on AIX 5L
Users allowed to use "at"	/usr/lib/cron/at.allow	/var/adm/cron/at.allow
Users not allowed to use "at"	/usr/lib/cron/at.deny	/var/adm/cron/at.deny
Spool area	/var/spool/cron/atjobs	/var/spool/cron/atjobs

9.5 Quotas

The disk quota system, which is based on the Berkeley Disk Quota System, provides an effective way to control the use of disk space. The quota system can be defined for individual users or groups, and is maintained for each file system.

The quota's concepts and commands are the same in Solaris and AIX 5L for journaled file systems (JFS), but there is a plus for AIX 5L V5.3 with JFS2, with a new implementation about disk usage quotas to control the use of persistent storage.

Disk quotas can be set for individual users or groups on a per file system basis.

AIX 5L V5.3 also introduces the concept of limit classes for JFS2. It allows the configuration of per file system limits, provides a method to remove old or stale quota records, and offers comprehensive support through dedicated SMIT panels. It also provides a method to define a set of hard and soft disk block and file allocation limits, and the grace periods before the soft limit becomes enforced as the hard limit.

The quota support for JFS2 and JFS can be used on the same system.

The disk quota system establishes the limits based on the following parameters, which can be changed with the **edquota** command:

- ▶ User or group soft limits
The soft limit defines the number of 1 KB disk blocks or files under which the user must remain.
- ▶ User or group hard limits
The hard limit defines the maximum amount of disk blocks or files the user can accumulate under the established disk quotas.

► Quota grace period

The quota grace period allows the user to exceed the soft limit for a short period of time (the default value is one week). If the user fails to reduce usage below the soft limit during the specified time, the system interprets the soft limit as the maximum allocation allowed, and no further storage is allocated to the user. The user can reset this condition by removing enough files to reduce the usage below the soft limit. The disk quota system tracks user and group quotas in the `quota.user` and `quota.group` files located in the root directories of the file systems enabled with quotas. These files are created with the **quotacheck** and **edquota** commands and are readable with the **quota** commands.

The basic commands for quota administration described in Table 9-7 are the same in Solaris and AIX 5L. Refer to the man pages for checking the differences between the command options.

Table 9-7 shows the **quota** commands in Solaris and AIX 5L.

Table 9-7 Quota commands

Task	Solaris	AIX 5L
Displays disk usage and quotas	quota	quota
Edits user and group quotas	edquota	edquota
Checks file system quota consistency	quotacheck	quotacheck
Turns on file system quota	quotaon	quotaon
Turns off file system quota	quotaoff	quotaoff
Manages quota limit classes for JFS2	N/A	j2edlimit (available only for JFS2)

For JFS2 limit classes management, you have two options:

- ▶ The first is to use the command **j2elimit**. Refer to the man pages for details.
- ▶ The second option for limit classes management on JFS2 is to use **smit**. The fast path is **smit j2fsquotas**. Figure 9-3 shows the **smit** screen for quotas on JFS2.

```

                                Manage Quotas for an Enhanced Journaled File System

Move cursor to desired item and press Enter.

Enable / Disable Quota Management
Stop / Restart Quota Limits Enforcement
List Quota Usage
Recalculate Current Disk Block and File Usage Statistics
Add a Limits Class
Change / Show Characteristics of a Limits Class
Make a Limits Class the Default Limits for a File System
Assign a User or Group to a Limits Class
List Limits Classes for a File System
Remove a Limits Class

F1=Help          F2=Refresh      F3=Cancel      F8=Image
F9=Shell        F10=Exit       Enter=Do

```

Figure 9-3 Class limits on JFS2

Table 9-8 compares the differences in files for quota administration in Solaris and AIX 5L.

Table 9-8 Quota configuration files

Task	File on Solaris	File on AIX 5L
Parameters for each file system	/etc/vfstab	/etc/filesystems
Specifies user quotas	quota.user	quota.user
Specifies group quotas	quota.group	quota.group

9.6 Process accounting

This section describes the differences in process accounting services. Process accounting is the method of keeping records about what commands are run and the users executing the commands, and the system resources used.

The commands in Solaris are similar to those available in AIX 5L.

The AIX 5L accounting system provides you with information about the use of system resources. This data can be used to:

- ▶ Bill the users for the resources used
- ▶ Control the use of some resources, such as disk space
- ▶ Substantiate the requirement for system expansion
- ▶ Carry out performance monitoring
- ▶ Maintain an audit trail for security purposes

AIX 5L accounting implementation is fully compatible with AT&T System V Release 4. With AIX 5L, you can also use 4.3 Berkeley Software Distribution (BSD) accounting utilities to inspect some of the accounting files. Because of this two-fold interface, you occasionally find two different ways to obtain the same accounting data.

A summary of commands and the files pertaining to AIX 5L accounting is provided in Table 9-9.

Table 9-9 Accounting in Solaris and AIX 5L

Command	Specification
runacct	The runacct command is the main daily accounting shell procedure. Normally initiated by the cron daemon.
acctcom	Displays selected process accounting record summaries. The acctcom command then writes the records you request to standard output. This command is stored in the <code>/usr/sbin/acct</code> directory for access by all users.
dodisk	The dodisk command initiates disk usage accounting by calling the diskusg command and the acctdisk command.
▶ acctdisk ▶ acctusg (On Solaris, only acctdisk)	The acctdisk and acctusg commands are called by the dodisk command to perform disk usage accounting. Usually, this procedure is initiated when the cron daemon runs the dodisk command.
chargefee	Charges users for the computer resources they use. The chargefee command writes a record to the <code>/var/adm/fee</code> file.

Command	Specification
acctmrg	Merges total accounting files into an intermediary file or a daily report
acctcms	Produces command usage summaries from accounting records
<ul style="list-style-type: none"> ▶ acctprc1 ▶ acctprc2 ▶ accton (On Solaris only accton)	These are called by the runacct command to perform process accounting shell procedures.
lastcomm	Displays information about the last commands executed
who	Identifies the users currently logged in

For more information about Accounting Management in AIX 5L, refer to *Auditing and Accounting on AIX*, SG24-6020, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246020.pdf>

9.7 Management tools

Solaris and AIX 5L servers can be managed either from a server console or remotely by using a network connection.

In the case of servers, the administrators usually work on the console for the installation and maintenance tasks. For normal administration tasks, the network is used. By using the network, the administrator can manage the systems from a command-line or an interface tool.

Common and specific interface tools exist for Solaris and AIX 5L. These are discussed in this chapter subsequently.

9.7.1 Common system management tools

This section describes the common system management tools.

Web-Based Enterprise Management and Common Information Model

Web-Based Enterprise Management (WBEM) is a set of management and Internet standard technologies developed to unify the management of distributed computing environments. WBEM provides the industry with the ability to deliver a well-integrated set of standards-based management tools, facilitating the exchange of data across otherwise disparate technologies and platforms.

The Distributed Management Task Force (DMTF) has developed a core set of standards that make up WBEM, including the following:

- ▶ The Common Information Model (CIM) standard
The data model for WBEM, CIM, provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions. For more information, visit the CIM standard Web page.
- ▶ CIM-XML
CIM-XML, which is an example of a WBEM protocol, includes the representation of CIM using Extensible Markup Language (XML) written in document type definition (DTD), and CIM operations over Hypertext Transfer Protocol (HTTP), a transport mechanism for WBEM.
- ▶ WBEM Discovery using Service Location Protocol (SLP) and WBEM Universal Resource Identifier (URI) mapping
Two standards that provide a way for applications to identify and interact with WBEM management systems, capitalizing on the existing standards and protocols to enable rapid development and deployment of management solutions.
- ▶ CIM query language
A query language used to extract data from a CIM-based management infrastructure.

In addition, the DMTF has developed a WBEM Management Profile template, allowing simplified profile development to deliver a complete, stand-alone definition for the management of a particular system, subsystem, service, or other entity.

For more information about WBEM, refer to the following Web site:

<http://www.dmtf.org/standards/wbem/>

On the AIX 5L V5.3 Expansion Pack CD, there is Pegasus CIM Server. It is one of the open source implementations of the CIM Object Manager, which is an object management engine that exists between the managed system and the management application.

Pegasus is written in C++ and adheres to the DMTF, CIM, and WBEM standards. CIM on AIX 5L V5.2 and AIX 5L V5.3 includes the following:

- ▶ An open source implementation of the CIM Object Manager called Pegasus V2.3.
- ▶ A CIM schema, V2.9, that defines an information model for representing system management resources, provided that instrument is a set of AIX 5L resources based on a CIM schema, V2.9.

For additional information about Pegasus and WBEM, refer to the following Web site:

<http://www.openpegasus.org/>

Simple Network Management Protocol

Another commonly used remote system management service is the Simple Network Management Protocol (SNMP). There are many tools available on cross platforms managed by the SNMP protocol. SNMP is an Internet Engineering Task Force (IETF) standard and is perhaps the most widely implemented standard for system management. The data model used by an SNMP service is called a Management Information Base (MIB). Different sections of MIB are supported by different devices and servers depending on the services available in the system. For more information about SNMP differences between Solaris and AIX 5L, refer to Chapter 7, “Network services” on page 183.

9.7.2 Solaris remote system management

Table 9-10 describes some Sun tools for Solaris administration with graphical interfaces.

Table 9-10 Solaris graphic tools

Product	Description
admintool	Managing users, groups, hosts table, printers, serial ports, and software
Patch Manager	Patch management
vea	If you work with Veritas Volume Manager, this is a graphical user interface (GUI) for LVM management.

Product	Description
Solaris Management Console	System status, configuration, jobs scheduling, and storage management

In AIX 5L, the `smit` is a unique tool for all the tasks described in Table 9-10, and much more. For more details, refer to “SMIT” on page 263.

9.7.3 AIX 5L management tools

In AIX 5L, the basic tools available for system management are SMIT and WSM.

SMIT

SMIT is a useful and powerful tool available in AIX 5L. SMIT runs in two modes, American Standard Code for Information Interchange (ASCII) (nongraphical) and X Windows (graphical).

ASCII SMIT can run on both terminals and graphical displays.

The graphical mode, which supports a mouse and point-and-click operations, can be run only on a graphical display and with X Windows support.

The ASCII mode is often the preferred way to run SMIT because it can be run from any display:

- ▶ To start the text mode, type `# smitty` or `smit -C`
- ▶ To start the graphical mode, type `# smit` or `smit -m`

SMIT is an interactive menu-driven interface application designed to simplify system management tasks. It provides a complete administrator's toolbox that can be used to perform system management activities such as installing software, configuring devices, administering user accounts, performing system backups, scheduling jobs, and diagnosing problems.

Note: The function keys used in the ASCII version of SMIT do not correspond to the actions in the graphical SMIT. The details are described in Table 9-11 on page 265.

smit fast path

The `smit` or `smitty` command takes you to the top level of the menu hierarchy if you do not use the fast path parameter. All the commands run by SMIT can be used as fast path. If you want to, for example, go directly to the `lvm` screen, type `smit lvm`. To take a fast path of a screen, press F8 or Esc+8.

smit logs

The SMIT log is smit.log in the home directory of the user.

SMIT selector screen

A selector screen is a special version of a dialog screen in which there is only one value to change. This value of the object is used to determine which subsequent dialog is to be displayed. Figure 9-4 shows the SMIT selector screen.

```
+-----+
|-----+
|                                     Available Network Interfaces
|
| Move cursor to desired item and press Enter.
|
| en0  10-80  Standard Ethernet Network Interface
| et0  10-80  IEEE 802.3 Ethernet Network Interface
| tr0  10-88  Token Ring Network Interface
|
| F1=Help          F2=Refresh          F3=Cancel
| F8=Image         F10=Exit            Enter=Do
| /=Find           n=Find Next
|-----+
+-----+
```

Figure 9-4 SMIT selector screen

Smit dialog screen

A dialog screen allows you to enter input values for the selected operation. Some fields are already filled with default values in the system. Usually, you can change these values.

To enter data, move the highlighted bar to the value you want to change and either enter a value or select one from a pop-up list. Fields that you can type into are indicated by square brackets ([]). Fields that have data that is larger than the space available to display it are indicated by angle brackets (<>) to indicate that there is further data to the left or right (or both) of the display area.

Figure 9-5 shows the SMIT dialog screen.

```

                                Add a Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]                                [Entry
* Group NAME                            [ ]
  ADMINISTRATIVE group?                  false +
  Group ID                               [ ] #
  USER list                              [ ] +
  ADMINISTRATOR list                     [ ] +

F1=Help          F2=Refresh          F3=Cancel
F4=List          F5=Reset             F6=Command
F8=Image        F9=Shell              F10=Exit
Enter=Do

```

Figure 9-5 SMIT dialog screen

Table 9-11 shows the different SMIT symbols. Special symbols on the screen are used to indicate how data is to be entered.

Table 9-11 SMIT symbols

Symbols in SMIT dialog screen	Explanation
*	A required field.
#	A numeric value is required for this field.
/	A path name is required for this field.
X	A hexadecimal value is required for this field.
?	The value entered will not be displayed.

Symbols in SMIT dialog screen	Explanation
+	A pop-up list or ring is available.

An asterisk (*) symbol in the left-most column of a line indicates that the field is required. A value must be entered here before you commit the dialog and execute the command.

In the ASCII version, a plus (+) sign is used to indicate that a pop-up list or ring is available. To access a pop-up list, use the F4 key. A ring is a special type of list. If a fixed number of options are available, the Tab key can be used to cycle through the options.

In the Motif version, a List button is displayed. Either click the button or press Ctrl+L to access a pop-up window from which to select from.

Table 9-12 shows the keys that can be used in the menus and the dialog screens. Some keys are valid only for particular screens. Those that are valid only for the ASCII interface are marked (A) and those that are valid only for the Motif interface are marked (M). Table 9-12 provides an overview of all the function keys.

Table 9-12 SMIT function keys

Function key	Explanation
F1 (or Esc+1)	Help: Show contextual help information
F2 (or Esc+2)	Refresh: Redraw the display (A)
F3 (or Esc+3)	Cancel: Return to the previous screen (A)
F4 (or Esc+4)	List: Display a pop-up list of possible values (A)
F5 (or Esc+5)	Reset: Restore the original value of an entry field
F6 (or Esc+6)	Command: Show the AIX 5L command that will be executed
F7 (or Esc+7)	Edit: A field in a pop-up box or select from a multiselection pop-up list
F8 (or Esc+8)	Image: Save the current screen to a file (A) and show the current fast path
F9 (or Esc+9)	Shell: Start a subshell (A)
F9	Reset all fields (M)
F10 (or Esc+0)	Exit: Exit SMIT immediately (A)
F10	Go to command bar (M)

Function key	Explanation
F12	Exit: Exit SMIT immediately (M)
Ctrl-L	List: Give a pop-up list of possible values (M)
PgDn (or Ctrl+V)	Scroll down one page
PgUp (or Esc+V)	Scroll up one page
Home (or Esc+<)	Go to the top of the scrolling region
End (or Esc+>)	Go to the bottom of the scrolling region
Enter	Perform the current command or select from a single-selection pop-up list
/text	Find the text in the output
n	Find the next occurrence of the text

SMIT output screen

The Command field can have the following values: OK, RUNNING, and FAILED.

Note: In the Motif version, there is a running man icon in the top right-hand corner of the screen that is used to indicate this value.

stdout is the standard output, that is, an output is produced as a result of running the command. The output is displayed in the body of this screen. If there is an error, the message shown is “stderr”. (Figure 9-6 does not show an error message.) The body of the screen shows the output and error messages if any that are generated by the command.

Figure 9-6 shows the SMIT output screen.

```
COMMAND STATUS
Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

system 0      true   root   files
staff  1      false  invscout,snapp,daemon  files
bin    2      true   root,bin   files
sys    3      true   root,bin,sys  files
adm    4      true   bin,adm files
uucp   5      true   nuucp,uucp   files
mail   6      true   files
security 7      true   root   files
cron   8      true   root   files
printq 9      true   lp     files
audit  10     true   root   files
ecs    28     true   files
nobody -2      false  nobody,lpd   files
usr    100    false  guest  files
perf   20     false  files
shutdown 21     true   files
lp     11     true   root,lp,printq  files
imnadm 188    false  imnadm files

F1=Help          F2=Refresh          F3=Cancel
F6=Command       F9=Shell           F10=Exit
F8=Image         /=Find
n=Find Next
```

Figure 9-6 SMIT output screen

For more indepth information about SMIT, refer to the following Web site:

<http://www.ibm.com/servers/aix/products/aixos/whitepapers/smit.html>

9.7.4 Web-based System Manager

Web-based System Manager is a GUI administration tool for AIX 5L. This is a Java-based comprehensive suite of system management tools for AIX 5L.

Because of the mouse-driven, point-and-click, drag-and-drop Web-based desktop environment, the Web-based System Manager is intuitive to use. It is more colorful than SMIT, and is an easy-to-use tool. It is a Web-based console that enables administrators to efficiently conduct a full range of systems management processes.

The Web-based System Manager utilizes a management console capable of administering multiple AIX 5L hosts from AIX 5L, PC, or Linux remote clients.

AIX 5L V5.3 contains new functions for the System Manager, including enhanced resource set and job scheduling capabilities. The Web-based System Manager is a highly scalable, provides a multiple host view of the administration environment, and secure host management with optional Secure Sockets Layer (SSL) security.

Web-based System Manager features

The Web-based System Manager provides the following features to assist you in easily managing your system:

- ▶ **Comprehensiveness**

With the extensive and consistent administrative environment, you can manage your system without having to manually edit configuration files or use UNIX commands.

- ▶ **Multiple host views**

There are only a few environments where there is a single system that has to be managed. The Web-based System Manager provides a view of the multiple host management environments. Adding hosts to the management console can be accomplished by reading a text file containing host names, or by manually adding hosts to the console.

- ▶ **Client independence**

The Web-based System Manager offers you the choice of client OS and platforms. You can use various client platforms to manage AIX 5L systems. Supported platforms for remote clients in Linux are Red Hat Enterprise V3, SUSE Linux Enterprise Server 8 (SLES 8), SLES 9, SUSE Linux 8.0, SUSE Linux 8.1, SUSE Linux 8.2, and SUSE Linux 9.0 using K Desktop Environment (KDE) and GNU Object Model Environment (GNOME) only.

- ▶ Location independence
You can use a locally attached graphical terminal or remote client with equal ease. The same GUI is available irrespective of whether the client is a personal computer or an IBM workstation.
- ▶ Ease-of-use
The Web-based System Manager can reduce training costs and costs caused by human error. It also enhances productivity and work satisfaction. The Web-based System Manager makes extensive use of “wizards” and “overviews” in order to provide the user with a “one-stop-shop” for basic management and status information, links to online help, and “one-click” task initiation.
- ▶ Enhanced ease of management
The AIX 5L release of the Web-based System Manager further simplifies administrative tasks through improvements in task design, new user interface features, and enhanced user assistance technology. In addition, use of Java 1.4 Java foundation class (JFC) technology makes it more accessible to users with disabilities. At present, it uses Java 1.4.2 (AIX 5L V5.3) instead of 1.4.1 (AIX 5L V5.2 ML3).
- ▶ Dynamic monitoring, notification, and control
The Resource Monitoring and Control (RMC) subsystem is a powerful and flexible monitoring system that provides dynamic status updates, e-mail notification, and unattended responses to system events.
- ▶ Support for Java™

Web-based System Manager server installation

The first step you must perform prior to using the Web-based System Manager is to check if the necessary packages are already installed on the environment. Refer to the examples provided here.

Example 9-11 shows the command to check the Web-based System Manager packages that are not installed.

Example 9-11 Web-based System Manager packages not installed

```
# ls1pp -h sysmgt.websm.framework  
ls1pp: 0504-132 Fileset sysmgt.websm.framework not installed.
```

Example 9-12 shows the command to check the Web-based System Manager packages that are already installed.

Example 9-12 Web-based System Manager packages already installed

```
# ls1pp -h sysmgt.websm.framework
  Fileset          Level   Action      Status      Date      Time
-----
-----
Path: /usr/lib/objrepos
  sysmgt.websm.framework
                5.3.0.40  COMMIT      COMPLETE    04/28/06
10:41:17

Path: /etc/objrepos
  sysmgt.websm.framework
                5.3.0.40  COMMIT      COMPLETE    04/28/06
10:44:51
```

To install the Web-based System Manager packages, use the command shown in Example 9-13.

Example 9-13 Web-based System Manager installation

```
# /usr/lib/instl/sm_inst installp_cmd -a \
> -d /dev/cd0 -f sysmgt.websm.framework -c -N -g -X
```

When installation finish, you will see the follow message:

Installation Summary

Name	Level	Part	Event
sysmgt.websm.icons	5.3.0.40	USR	APPLY
SUCCESS			
sysmgt.websm.framework	5.3.0.40	USR	APPLY
SUCCESS			
sysmgt.websm.rte	5.3.0.40	USR	APPLY
SUCCESS			
sysmgt.websm.apps	5.3.0.40	USR	APPLY
SUCCESS			
sysmgt.websm.framework	5.3.0.40	ROOT	APPLY
SUCCESS			

sysmgt.websm.rte	5.3.0.40	ROOT	APPLY
SUCCESS			
sysmgt.websm.apps	5.3.0.40	ROOT	APPLY
SUCCESS			

Operating modes

On AIX 5L you can run the Web-based System Manager in three different modes:

- ▶ Stand-alone managing AIX 5L systems local
- ▶ Remote client mode using any AIX 5L system as the Web-based System Manager client.
- ▶ For remote AIX 5L systems in an applet (browser)

Local mode

No Internet or intranet connection is required to run the Web-based System Manager from the command line or the CDE desktop in the stand-alone mode on a local system. Run the # `wsm` command.

Remote client/server mode

The Web-based System Manager can also be remotely run on any AIX 5L host known to the system. In remote (client/server) mode, the user interface is managed locally, but the operations are performed on the remote host. The Web-based System Manager for AIX 5L V5.2 supports, and has been tested on AIX 5L V5.1C, V5.1D, V5.1F, V5.2B, V5.2F, V5.2H, and V5.3.

The Web-based System Manager can be run remotely using the remote client software for Windows-based and Linux platforms. The Web-based System Manager for AIX 5L V5.2 and V5.3 supports, and has been tested on Windows 2000, Windows XP Professional, and Windows Server® 2003, Red Hat Enterprise V3, SLES 8, SLES 9, SUSE 8.0, SUSE 8.1, SUSE 8.2, and SUSE 9.0 using desktops KDE or GNOME only. The Web-based System Manager no longer provides remote client support on Windows 95, Windows 98 ME, and Windows NT® platforms.

The installable file sets for remote clients can be found and downloaded from any AIX 5L system or from the Hardware Management Console (HMC) of your managed system. On AIX 5L, the file is located on `/usr/websm/pc_client/`.

Note: To acquire the Web-based System Manager client from an AIX 5L server, the file set `sysmgt.websm.webaccess` must be installed. If you use FTP, remember to use binary mode.

If you choose to get a remote client from the HMC, direct your browser to the following URL:

http://HMC_IP/remote_client.html

Figure 9-7 shows the Web-based System Manager.

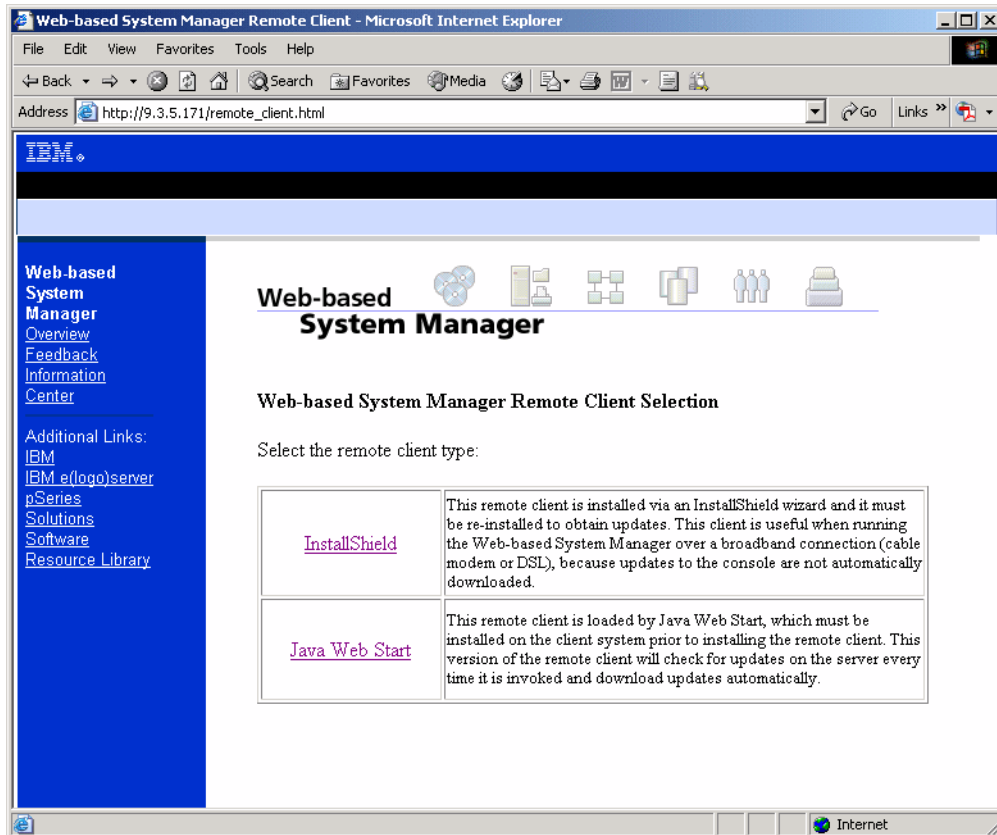


Figure 9-7 Web-based System Manager

In this step, select a remote client. Following are the options:

- ▶ InstallShield

This remote client is installed through a Windows InstallShield wizard. It must be reinstalled manually to obtain updates when the software level of the managed systems changes to some extent. This client is useful when running the Web-based System Manager over a broadband connection (cable modem or Digital Subscriber Line (DSL)) because updates to the console are

not automatically downloaded and the startup of the application itself is reasonably fast after it is installed. However, the download for installation must be performed by using a capable network because the size of the setup.exe file is quite large (100 MB).

► **Java Web Start**

This version of the remote client checks for updates on the server every time it is invoked, and downloads updates automatically. Because this requires some network bandwidth, this client does not perform well on broadband network links. However, the advantage of using this client is that your Web-based System Manager application is always up-to-date and in sync with the OS level of your managed system. This remote client is loaded by the Java Web Start application, which must be installed on the client system prior to installing the remote client. If you do not already have it installed on your workstation (it comes with most of the current Java Runtime Environments), you can also download it from the HMC. Selecting the Java Web Start link takes you to a screen where you can download a Java Runtime Environment that includes the Java Web Start application, as shown in Figure 9-8.

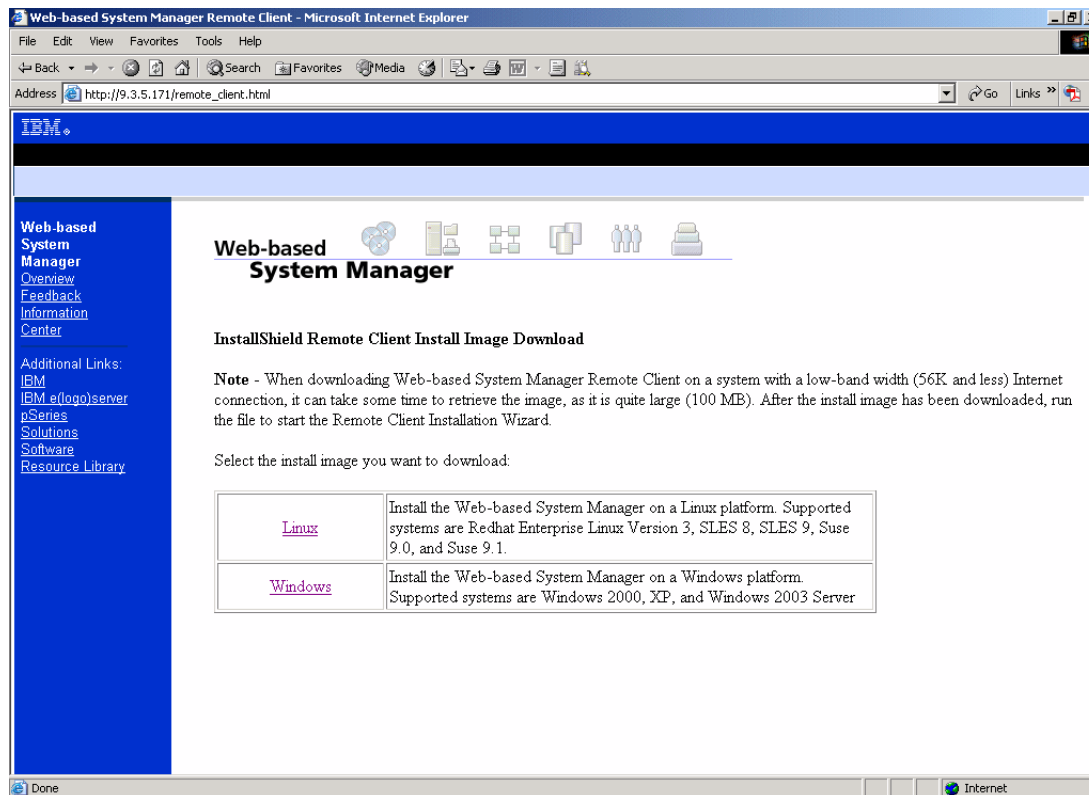


Figure 9-8 Web-based System Manager remote client

After selecting the desired remote client type, the next task is about the OS that will be used by the client. Select either the Windows or the Linux version of the software in order to start the download. A confirmation window to save or open the setup.exe opens. You can start the installation directly over the network in the course of the download or save the file to your hard disk and run it from there to finish the installation of the remote client version.

Applet mode

Finally, with the Web-based System Manager, any OS and platform for which a Java 1.4-enabled (AIX 5L V5.3 Java V1.4.2 and V5.2 ML3 Java V1.4.1) browser is available, can be used to manage an IBM system. The Web-based System Manager has been tested with Mozilla and Microsoft® Internet Explorer®.

There is a significant difference between using an applet mode and a client/server mode. In an applet mode, it is possible to only manage a set of machines that have the same version of the Web-based System Manager installed. The reason for this is that applets in general are restricted, for security reasons, to loading Java classes only from the HTTP server running the applet. The Java classes that are required to operate the Web-based System Manager console come from the managing machine. Another set of Java classes are used to operate tasks on the managed machines. These classes must be loaded from the machine being managed (this is different from the managing machine) for these classes to match the OS being managed. In an applet mode, this situation is *not* possible.

IBM Hardware Management Console

The IBM Hardware Management Console for pSeries provides a standard user interface for configuring and operating partitioned and SMP systems. The HMC supports the system with features that enable a system administrator to manage the configuration and operation of partitions in a system, and to monitor the system for hardware problems. It consists of a 32-bit Intel®-based desktop PC with a DVD-RAM drive.

Following are the main tasks that an HMC performs:

- ▶ Creates and maintains a multiple partitioned environment
- ▶ Displays a virtual OS session terminal for each partition
- ▶ Displays virtual operator panel values for each partition
- ▶ Detects, reports, and stores the changes in hardware conditions

- ▶ Powers managed systems on and off
- ▶ Acts as a service focal point for service representatives to determine an appropriate service strategy and enable the Service Agent Call Home capability
- ▶ Activates additional resources on demand

For more information about HMC, refer to *Effective System Management Using the IBM Hardware Management Console for pSeries*, SG24-7038, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg247038.pdf>

Coexistence of Web-based System Manager and Hardware Management Console

If you work with a remote client installed on a PC for HMC management, you can include the AIX 5L servers in the same HMC screen for Web-based System Manager-based OS administration.

In this scenario, you can consolidate HMC and a lot of administration tasks of different servers into one unique console.

For details about the Web-based System Manager installation, refer to 9.7.4, “Web-based System Manager” on page 269.

To add an AIX 5L server Web-based System Manager based on the same console of an HMC that is already installed, perform the following tasks:

1. Click **Console**.
2. Click **Add**.
3. Click **Hosts**.
4. Type the full name in the Hosts field.

- The server name is now available on the console. When you try to access the server name, you will be asked for the login ID and the password. After you enter this information, the consolidation scenario is complete.

Figure 9-9 shows the coexistence of the HMC and the Web-based System Manager.

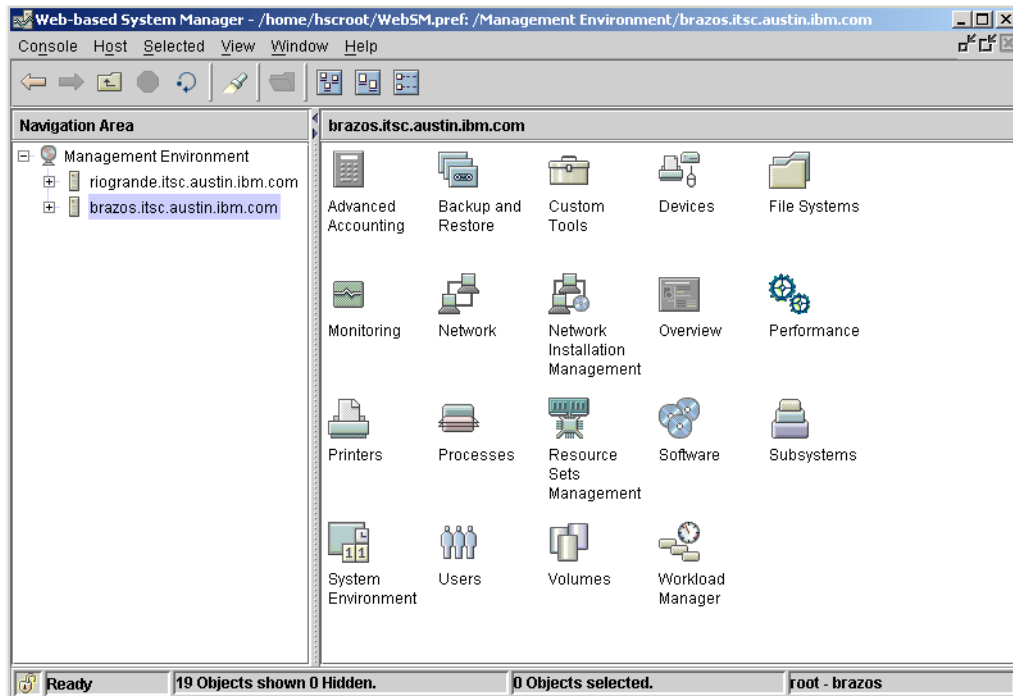


Figure 9-9 Coexistence of the HMC and the Web-based System Manager



Printing services

This chapter discusses the differences between the printing subsystems on Solaris and AIX 5L. This chapter contains the following topics:

- ▶ 10.1, “Overview” on page 280
- ▶ 10.2, “AIX 5L print subsystem versus Solaris lpsched print subsystem” on page 280
- ▶ 10.3, “Print queue administration” on page 283
- ▶ 10.4, “Print job management” on page 294
- ▶ 10.5, “Printer pooling” on page 310
- ▶ 10.6, “Using System V print subsystem on AIX 5L” on page 310
- ▶ 10.8, “Remote printing” on page 313
- ▶ 10.9, “Common UNIX Printing System” on page 317
- ▶ 10.10, “Quick reference” on page 318

10.1 Overview

In AIX 5L, IBM includes both the traditional AIX 5L print subsystem, and the AIX 5L System V print subsystem, which has been a printing standard for many years in the UNIX environment. For more complex printing environments, IBM also offers a print management product called IBM Infoprint® Manager.

10.2 AIX 5L print subsystem versus Solaris lpsched print subsystem

This section introduces printing on Solaris and AIX 5L.

Solaris

Solaris uses the lpsched print subsystem, which is the System V interface, and uses the System V or the Berkeley Software Distribution (BSD) printing protocol. The BSD and System V printing protocol is widely used and provides compatibility between the different types of systems from various manufacturers. Under Solaris 9, the lpsched process does *not* start automatically unless printers are defined.

Table 10-1 shows the commands that are used to create and manage the lpsched subsystem.

Table 10-1 Commands used to create and manage the lpsched subsystem

Command	Task
lp	Submit and queue print jobs
cancel	Cancel jobs
lpstat	Give status of the print queue
accept	Enable queuing
reject	Disable queuing
enable	Start printing to a device
disable	Stop printing to a device
lpsched	Start the LP print service daemon
lpset	Set printing configuration in /etc/printers.conf
lpshut	Stop the LP print service

Command	Task
lpssystem	Register remote systems with print service
lpusers	Set printing queue priorities
lpforms	Administer forms used with the LP service
lpget	Get printing configuration
lpfilter	Administer filters used with the LP service

For more information about Solaris printing, refer to the man pages or Sun documents Web site at:

<http://docs.sun.com/app/docs>

AIX 5L

In AIX 5L, IBM includes both the traditional AIX 5L print subsystem, which is the BSD printing protocol, and the System V print subsystem, which has been a printing standard for many years in the UNIX environment. For more complex printing environments, IBM also offers a print management product called Infoprint Manager.

Following are some of the features of the Infoprint Manager:

- ▶ Secure and scalable enterprise printing support
- ▶ Reliability for mission-critical applications such as SAP/R3
- ▶ Ability to manage, print, store, and reprint to printer, fax machines, and more
- ▶ Multiple printer support (up to 1000 plus pages per minute)
- ▶ Includes printing in your IBM Tivoli system management solution

For more information about Infoprint Manager, refer to the following Web site:

http://www.printers.ibm.com/internet/wwsites.nsf/vwwebpublished/ipmoverview_ww

AIX 5L print subsystem characteristics

Following is a list of AIX 5L print subsystem's characteristics:

- ▶ Flexible printer drivers

AIX 5L printer drivers provide many printing options that can be easily controlled using the **qprt** command. Printer defaults can be easily managed using SMIT or the command line.

- ▶ System management tools

The AIX 5L print subsystem includes mature and powerful system management, using either the Web-based System Manager or SMIT, and the command line. System management tools for the System V print subsystem are less mature in this initial release. Some of the specific system management advantages of using the AIX 5L print subsystem are:

- Limits fields and options validation
- Easy printer customization
- Single-step print device and queue creation
- Support for dial-in administration

- ▶ Customizable spooling subsystem

The AIX 5L print subsystem is specifically designed so that it can be used to serialize other types of jobs beyond just printing.

In the AIX 5L printing environment, the files that are to be printed are sent to the AIX 5L print spooler daemon (qdaemon) using any of the AIX 5L print commands (**enq**, **qprt**, **lp**, or **lpr**). The spooler daemon serializes the jobs. The spooler sends the jobs, one at a time, to back-end programs that might filter the data before sending it to the local printer driver or network printing application.

In summary, the main advantages of AIX 5L printing have to do with flexibility and ease-of-use. AIX 5L printing is tightly integrated into SMIT and the Web-based System Manager. Also, System V is not yet mature on AIX 5L, although system management features will be enhanced in future releases of AIX 5L.

System V print subsystem characteristics

This section describes System V print subsystem's characteristics:

- ▶ Long-term strategy

The long-term printing strategy for AIX 5L is to maintain compatibility with other UNIX systems.

- ▶ Standard PostScript filters

The System V print subsystem includes a number of filters for converting a number of different file formats to PostScript.

- ▶ Support for forms

The System V print subsystem provides a mechanism for mounting forms on printers and allowing or denying user access based on the form that is mounted. To provide this capability under AIX 5L printing, create multiple queues and manage which queues are enabled when a form is mounted.

► Security

System V printing includes built-in capabilities for restricting user access to certain printers. Using the AIX 5L print subsystem, the back-end program must be customized to restrict user access.

In the System V printing environment, the files to be printed are sent to the System V print service daemon (lpsched), using the **lp** or **lpr** commands. The print service daemon serializes the jobs so that they will be printed in the order in which they were submitted. The print service might filter the file to format the data so that it matches the types of data acceptable to the printer. The print service then sends files, one at a time, to the interface program, which might perform additional filtering before sending the file to the local printer driver or network printing application.

10.3 Print queue administration

Local printing to serial and parallel attached printers for both the System V and AIX 5L print subsystems is performed through standard AIX 5L device drivers. Before using either of the print subsystems, you must be aware of how these device drivers work and at some of the commands that you can use to look at the devices.

Print devices can be added from the command line, from SMIT, and from the Web-based System Manager. The device created in all the three methods will be the same, and can be used by either of the base print subsystems. The printer type that you add when creating a device determines the buffer size and some timing parameters for the serial or parallel device driver that is ultimately used. It is not important that the device printer type and the print subsystem printer type match each other exactly, only that they are of similar type. If you are adding a laser printer, you must choose a laser printer that is similar in speed to the actual print model you will be using.

When a print device is added, the device is represented by a special character device file in /dev with a name starting with lp, and the number of the printer that is given in sequential order when the devices are added. A list of all the printers that are currently on a system can be obtained with `lsdev`, as shown in Example 10-1

Example 10-1 Obtaining a list of all the printers currently on a system

```
# lsdev -Cc printer
lp0 Available 00-00-0P-00 Lexmark Optra laser printer
lp1 Available 00-00-S2-00 IBM Network Printer 12
lp2 Available 00-00-S1-00 Hewlett-Packard Color LaserJet 4500
```

This not only provides you with information about the models of all the printers that have been added, but also tells you whether they are available, and the adapter number and port number on which they have been installed.

To list all the available printer types, use the following command:

```
# lsdev -Pc printer
```

To obtain a list of individual device files use the `ls -l` command as follows:

```
# ls -l /dev/lp0
crw-rw-rw- 1 root system 26, 0 Oct 19 13:52 /dev/lp0
```

The device files for the local serial devices and the parallel devices must always have a listing starting with *cr* for character devices that are readable.

10.3.1 Adding a local print queue

Perform the following tasks to add a local print queue using SMIT (in this example, text-based SMIT screens are shown, but the same functionality is available from the graphical user interface-based (GUI-based) SMIT on X Windows displays):

1. Enter the following command:

```
# smitty mkpq
```


On entering this command, the screen shown in Figure 10-1 is displayed. Move the cursor to the desired item and press Enter. (In our example, we selected the local option.) Use the arrow keys to scroll.

```

                                Add a Print Queue

Move cursor to desired item and press Enter. Use arrow keys to
scroll.

# ATTACHMENT TYPE      DESCRIPTION
local                  Printer Attached to Local Host
remote                 Printer Attached to Remote Host
xstation               Printer Attached to Xstation
ascii                  Printer Attached to ASCII Terminal
hpJetDirect            Network Printer (HP JetDirect)
file                   File (in /dev directory)
ibmNetPrinter          IBM Network Printer
ibmNetColor            IBM Network Color Printer
other                  User Defined Backend

F1=Help                F2=Refresh            F3=Cancel
F8=Image               F10=Exit              Enter=Do
/=Find                 n=Find Next
```

Figure 10-1 *Smitty mkpq* screen

2. The screen shown in Figure 10-2 is displayed. The screen shows the available printer drivers. If your printer model is not listed, select **Other**, which is at the bottom of the list. To get to the bottom of the list, use the Down Arrow or the PgDn key.

```
Printer Type

Move cursor to desired item and press Enter.

Bull
Canon
Dataproducts
Hewlett-Packard
IBM
Lexmark
OKI
Printronic
QMS
Texas Instruments
Other (Select this if your printer type is not listed above)

F1=Help          F2=Refresh       F3=Cancel
F8=Image         F10=Exit         Enter=Do
/=Find           n=Find Next
```

Figure 10-2 Printer Type menu

3. If you select a printer model that has its device driver installed (available) on your system, the screen shown in Figure 10-3 is displayed. Select the **parallel** option.

Note: If your printer model is not listed, you can install the printer driver from the AIX 5L CD-ROMs. To do this, issue a **smitty pdp** command and select **Install Additional Printer/Plotter software**.

```
Printer Interface

Move cursor to desired item and press Enter.

parallel
rs232

F1=Help          F2=Refresh       F3=Cancel
F8=Image         F10=Exit         Enter=Do
/=Find           n=Find Next
```

Figure 10-3 Printer interface

4. The Parent Adapter screen (Figure 10-4) is displayed. In our example, there was only one adapter to select. If multiple adapters are present, they will all be listed. Select the parent adapter that corresponds to the communications port you have connected your printer to.

```
Parent Adapter

Move cursor to desired item and press Enter.

ppa0 Available 01-R1 CHR P IEEE1284 (ECP) Parallel Port Adapter

F1=Help          F2=Refresh       F3=Cancel
F8=Image         F10=Exit         Enter=Do
/=Find           n=Find Next
```

Figure 10-4 Parent adapter menu

- In the screen shown in Figure 10-5, you are prompted to choose a name for each queue that is created for each type of mode your printer can emulate. Each name that you enter creates a separate queue and virtual printer. Select names in such a way that it is easy to remember the name of each queue. (In our example, we chose the name PCL-mv200 for the PCL Emulation queue and PS-mv200 for the PostScript queue.) After selecting the queue names, press Enter.

```

                                Add a Print Queue

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry
Fields]
  Description                                IBM 4079 Color
Jetprin>
  Names of NEW print queues to add
    GL Emulation                            [PCL-mv200]
    PostScript                              [PS-mv200]

Printer connection characteristics
*  PORT number                               [p]
+
  Type of PARALLEL INTERFACE                [standard]
+
  Printer TIME OUT period (seconds)        [600] +#
  STATE to be configured at boot time      available
+

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit       Enter=Do

```

Figure 10-5 Add a Print Queue

6. If the screen shown in Figure 10-6 is displayed, it means that you have successfully configured a printer into the print spooling subsystem.

```
COMMAND STATUS

Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

Added printer 'lp0'.

Added print queue 'PCL-mv200'.
Added print queue 'PS-mv200'.

F1=Help          F2=Refresh          F3=Cancel
F6=Command       F9=Shell            F10=Exit          /=Find
F8=Image         n=Find Next
```

Figure 10-6 Output

You can also add a print queue through the command line. However, by using the Web-based System Manager or SMIT to add a print queue, you can avoid dealing with a queue, a queue device, and a virtual printer. If you are going to add a virtual printer queue, the steps to add the printer become quite complicated, and unless you are going to create shell scripts to add your queues, it is recommended that you avoid it.

To add a remote queue that does not use a virtual printer, perform the following tasks (this procedure can also be used to add a queue with a custom backend):

1. Add a queue using the **mkque** command. The following command will, for example, configure a remote queue. It configures only the queue and not the queue device:

```
# mkque -qlp -a "host=puttifar" -a "rq=solar"
```

- The **-q** flag specifies the name of the queue to be added (lp).
- The **-a** flag specifies a line to be added to the queue stanza in the qconfig file (host=puttifar and rq=solar). These flags must be entered last, when entering the **mkque** command on the command line.

2. Add a queue device associated with the queue you have added, using the **mkquedev** command. In our example, for the queue we added (as described earlier), the following command added a device named `lpdev` that has `/usr/lib/lpd/rembak` as its backend:

```
# mkquedev -qlp -dlpdev -a "backend=usr/lib/lpd/rembak"
```

- The `-q` flag specifies the name of the queue (this name must already exist) to which the queue device is added. The **mkquedev** command automatically adds the `device=attribute` to the specified queue stanza.
- The `-a` flag specifies the attribute to be added to the device stanza in the `/etc/qconfig` file (`backend=usr/lib/lpd/rembak`).

10.3.2 Displaying a queue configuration information

After the printers are established, you might want to review their configuration. This section describes how to accomplish this by using SMIT and the command line.

To display the names of all the configured queues, enter the following command:

```
# smitty lsallq
```

This SMIT command lists the names of all the configured queues, as shown in Figure 10-7.

COMMAND STATUS			
Command: OK	stdout: yes	stderr: no	
Before command completion, additional instructions may appear below.			
# PRINT QUEUE	PRINTER	DESCRIPTION	
PCL-mv200	lp0	ibm4079 (GL Emulation)	
PS-mv200	lp0	ibm4079 (PostScript)	
F1=Help	F2=Refresh	F3=Cancel	
F6=Command			
F8=Image	F9=Shell	F10=Exit	/=Find
n=Find Next			

Figure 10-7 Smitty `lsallq` command

To list the installed printer queues, type the following from the command line:

```
# lsallq -c
```

10.3.3 Deleting a queue

You might have to remove a print queue occasionally. To delete a queue or queue device, you must have root authority. You can do this by using one of the interfaces (Web-based System Manager, SMIT, or the command line).

Using the Web-based System Manager or SMIT is a lot easier than using the command line because you only deal with the print queue. If the print queue has any device associated with it, the Web-based System Manager or SMIT automatically removes it for you. If you have many print queues associated with the same device, and you want to remove all the queues, the Web-based System Manager or SMIT removes all the queues for you without removing the queue device, except for the last print queue, when the Web-based System Manager or SMIT removes the queue and its associated device.

To delete a queue, perform the following tasks:

1. Enter the following command in the command prompt:

```
# smitty rmpq
```

The Remove a Print Queue screen is displayed (Figure 10-8). Press F4 to select the queue you want to remove.

Remove a Print Queue

Type or select a value for the entry field.
Press Enter AFTER making all desired changes.

[Entry

Fields]

* PRINT QUEUE name []

+

F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 10-8 Remove a Print Queue

- The screen shown in Figure 10-9 is displayed. Select the queue you want to remove.

```

                                PRINT QUEUE name

Move cursor to desired item and press Enter. Use arrow keys to
scroll.

# PRINT QUEUE                DESCRIPTION
GL-mv200                    ibm4079 (GL Emulation)
PS-mv200                    ibm4079 (PostScript)

F1=Help                      F2=Refresh                F3=Cancel
F8=Image                     F10=Exit                  Enter=Do
F5 /=Find                    n=Find Next
```

Figure 10-9 Print Queue name

- The confirmation screen is displayed. Press Enter to complete the deletion process. If your attempt is successful, a screen showing OK status is displayed.

When removing the queue using the command line, first ensure that no jobs are queued. If there are jobs, cancel them before removing the queues. If there is a virtual printer, remove it using the `rmvirprt` command. After checking to see if the queues still exist, remove the queue device with the `rmquedev` command, and then the queue with the `rmque` command. If there are multiple queue devices in the queue, all the queue devices must be deleted using the `rmquedev` command before using the `rmque` command.

To remove the print queue `lp0`, enter the command shown in Example 10-2.

Example 10-2 Removing the print queue `lp0`

```
# cancel 4312psg
# rmvirprt -d lp0 -q PCL-mv200
# rmquedev -q PCL-mv200 -d lp0
# rmque -q PCL-mv200
```

If you remove the queue device and do not remove the queue, a dummy queue device is created, and the `qdaemon` will have problems processing the queue.

10.3.4 Enabling and disabling a queue

When a printer is not functioning properly, you might want to take that printer offline. The terminology for this varies. Some documents talk about starting and stopping a queue, and others use the terms enabling and disabling the queue. You also have the option of the interface starting or stopping a queue. This section shows you how to enable and disable a print queue using SMIT and the command line.

To disable a queue, enter the following command:

```
# smitty qstop
```

In the screen shown in Figure 10-2, press the F4 key to select a queue to stop.

To start a queue, enter the following command:

```
# smitty qstart
```

You will see the screen shown in Figure 10-2. You can start again by selecting a queue.

The **qadm** command brings printers, queues, and the spooling system up or down (makes printers available or unavailable), and cancels jobs. The **qadm** command can only affect local print jobs. You must also have root user authority, or belong to either the system group or the printq group, to run this command.

Examples

To bring down the PCL-mv200 queue, enter one of the following commands:

- ▶ # qadm -D PCL-mv200
- ▶ # disable PCL-mv200

When you check the queue status by using the **qchk** or the **lpstat** command, the status of this queue will be READY.

The other options of the **qadm** command are **-G** and **-K**. The **-G** option gracefully brings down the queuing system. This flag temporarily interrupts the daemon process after all the currently running jobs on all the queues are finished. Using this flag is the only way to bring the system down without causing problems such as jobs hanging in the queue. The **-K** option brings down the printer you name, ending all the current jobs immediately. Jobs remain in the queue and run again when the printer is brought back up.

10.3.5 Cancelling print jobs

To cancel all your jobs on printer lp0 (or all the jobs on printer lp0 if you have root user authority), enter one of the following commands:

- ▶ # qadm -X 535pc1
- ▶ # cancel 535pc1
- ▶ # qcan -X 535pc1

The -X flag cancels the printing of the user's jobs on the specified queue (PS-mv200). If you have root user privileges, all the jobs on that queue are deleted.

You can also cancel individual jobs by using the job ID. Use the following commands:

- # qcan -x 435
- # cancel 435

You can also use SMIT and the Web-based System Manager to perform this task. The smit fast path is **smitty qcan**.

10.4 Print job management

Now that you have a printer configured, you probably want to use it. This section reviews the methods that are available to request for a job to be printed and then manage the progress of that job through the print spooling subsystem. It is important that a systems administrator has a good understanding of these commands because users will often seek assistance about how to meet their complex printing requirements or to get that special rush job printed. Solaris uses System V printing system. AIX 5L V5.x can also use the System V and BSD printing system. Table 10-2 shows the different printing commands.

Table 10-2 System V, BSD, and AIX 5L print commands

System V	BSD	AIX 5L
lp	lpr	qprt

10.4.1 Submitting printing jobs

There are three sets of commands for submitting, listing, and cancelling print jobs. They come from either System V, BSD, or IBM versions of UNIX, and are all available in AIX 5L. The commands have slightly different options.

To submit a print job to a queue, use either **lp**, **lpr**, or **qprt**. All the jobs will go to the system default queue unless the **PRINTER** or **LPDEST** variables are set. You can also specify, on the command line, which queue to use. Use **-d** with **lp** or use **-P** with **qprt** and **lpr**.

The commands **lp** and **qprt** both queue without spooling, by default. Specify the **-c** option if spooling is required. The command **lpr** spools and queues by default. The **-c** option turns off spooling with **lpr**.

To print multiple copies, use the **qprt -N #** or **lp -n #** command. For **lpr**, use only a dash followed by the number of copies (**- #**).

The **lp**, **lpr**, and **qprt** commands create a queue entry in **/var/spool/lpd/qdir** and, depending on the options specified, copy the file to be printed to the **/var/spool/qdaemon** directory.

All the print commands, **lp**, **lpr**, and **qprt**, actually call the **enq** command, which places the print request in a queue. The **enq** command can be used instead of the other commands to submit jobs, view job status, and so on. To submit a job using **enq**, run:

```
# enq -PqueueName filename
```

The qprt command

The **qprt** command is the IBM AIX 5L printing tool. The first step in the process of printing using **qprt** is to place a print job or a request into the print spooling subsystem. AIX 5L features a number of commands and facilities to perform this task. The prerequisite to initiating a print request is that before you can print a file, you must have read access to it.

Note: SMIT must be used only when the user wants to set specific settings and does not know the **qprt** command.

To start a printing job, perform the following tasks:

1. Enter the following command:

```
# smitty qprt
```
2. To print the desired file, fill in, along with the print queue name, details about where you want to print your file. Alternatively, press **F4** to view a list of available queues. Press **Enter** after selecting the queue. If no printer is specified, the default is used.
3. If you press **F4**, the available print queues are listed, as shown in Figure 10-2 on page 286. Select the queue you will send your print request to. (In our example, we chose the **GL-mv200** queue.) On selecting the queue, the

screen shown in Figure 10-10 is displayed. Select a print file type that you want to start.

```
Print File Type

Move cursor to desired item and press Enter.

a ASCII
p PCL
n troff (ditroff) intermedia outout
p pass-through
s PostScript

F1=Help          F2=Refresh      F3=Cancel
F8=Image        F10=Exit        Enter=Do
F5 /=Find       n=Find Next
```

Figure 10-10 Selecting the type of text file

4. In the screen that appears (Figure 10-11), specify the details pertaining to your job, including:
 - Text print options
 - Job processing options
 - Text formatting options
 - Paper or page options
 - Header or trailer page options
 - Messages or diagnostics

Enter the details in the “Name of FILE to print” field with the name of the file you want to print, perform all the necessary modifications, and press Enter to print your file.

```

Start a Print Job

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                     [Entry Fields]
Print queue name                       test2
* Name of FILE to print                 []

----- Text Print Options -----
Print QUALITY                           quality          +

----- Job Processing Options -----
Number of COPIES                         [1] +#
Place job in 'HELD' state when queued?   no              +
COPY FILE and print from copy?           no              +
REMOVE FILE after print job completes?   no              +
Print job PRIORITY                       [15] +#
Pre-processing FILTER NAME                []              +
INITIALIZE printer?                      yes             +
RESTORE printer?                         yes             +

----- Text Formatting Options -----

----- Paper/Page Options -----

----- Header/Trailer Page Options -----
SEPARATOR PAGES                          none            +
Job TITLE                                 []
'DELIVER TO' TEXT                         []
HOSTNAME for "PRINTED AT:" on HEADER PAGE []

----- Messages/Diagnostics -----
MAIL MESSAGES instead of displaying them? no              +
NOTIFY when job finished?                 no              +
TEXT to display on console before printing job []
FILE to display on console before printing job [] /
DIAGNOSTIC LEVEL                          (normal) - print job; > +

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command          F7=Edit           F8=Image
F9=Shell         F10=Exit            Enter=Do

```

Figure 10-11 Starting a print job

As mentioned earlier, you can also use the **qprt** command to perform the same task from the command line. The **qprt** command creates and queues a print job. It is designed to work with the virtual printer subsystem, and there are **qprt** print flags for most print customizations. The **qprt** command has a large variety of parameters that can be used. Some of the most useful are shown here as examples:

- ▶ Use **qprt -p** to select the printer pitch. Normally, values of 10 and 12 are accepted, but sometimes a value of 17 is also accepted:

```
# qprt -p12 -P queue-name /tmp/testfile
```
- ▶ Use **qprt -z+** to print landscape:

```
# qprt -z+ -P puttifar /tmp/testfile
```
- ▶ Use **qprt -Y+** to print duplex:

```
# qprt -Y+ -P andrea /tmp/testfile
```
- ▶ To indent a page on the left margin, use the **qprt -i** command:

```
# qprt -i 5 -P veronica /tmp/testfile
```
- ▶ To print formatted files in passthrough mode, use the **qprt -dp** command. Note that in the command provided here, you can also specify landscape orientation:

```
# qprt -dp -z+ -P fischer /tmp/testfile
```
- ▶ To print text files to a PostScript queue, use the **qprt -da** flag (this can be combined with the **-p** flag to designate the character size that the virtual printer uses (enscript) to convert the text to PostScript):

```
# qprt -da -p 14 -P ps /tmp/testfile
```
- ▶ Note that the flags can be combined. To print landscape, 17 characters per inch with a line printer font, use the following:

```
# qprt -z+ -p17 -slineprinter -P funjet /tmp/testfile
```
- ▶ In addition to **qprt**, the **enq**, **lp**, and **lpr** commands can be used from the command line.
- ▶ To print from the Common Desktop Environment (CDE), use the command **dtprint**.
- ▶ When using **lp** or **enq**, the **qprt** flags can be set with the **-o** options, for example, to set the pitch to 12 with **lp** and **enq**, use the following commands:

```
# lp -o -p12 -d pcl /tmp/testfile  
# enq -o -p17 -P pcl /tmp/testfile
```

- ▶ The **lpr** command does *not* use the **-o** flag, and therefore cannot be used for most virtual printer settings. By default, **lpr** spools all the files and overrides the queue header page setting to always generate a header, unless you use the **-h** flag to turn off the headers as follows:

```
# lpr -h -P pcl /home/toenrtr/adress.doc
```

10.4.2 Checking the status

After a print job is submitted to the queuing system, you might want to see the status of the job on the print spooling subsystem. You can do this through the Web-based System Manager, SMIT, or the command line. This section describes how to use SMIT and a command line to list the queue information.

Irrespective of the method you use, you can review the contents of one or more print queues to check the current status of the queues and the jobs that you have submitted. The contents also show the status of the printers and the queues. In AIX 5L, two commands are available, **qchk** and **qstatus**.

To check only the status of the queues, perform the following tasks:

1. Enter the following command:

```
# smitty qstatus
```

2. The screen shown in Figure 10-12 is displayed. To see the status of the remote server queues, select **yes** and press Enter.

Show Status of Print Queues

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry

Fields]

Include status of print queues remote servers? [yes]

+

F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 10-12 Show Status of Print Queues

The screen shown in Figure 10-13 is the output for the status of the queues.

```
COMMAND STATUS
Command: OK          stdout: yes          stderr: no
Before command completion, additional instructions may appear below.
Queue  Dev  Status
-----
tdipcl lp0  DEV_BUSY
tdipsq lp0  READY
F1=Help          F2=Refresh          F3=Cancel
F6=Command
F8=Image          F9=Shell            F10=Exit            /=Find
n=Find Next
```

Figure 10-13 Command status

To see the status of the print jobs in a specific queue, perform the following tasks:

1. Enter the following command:

```
# smitty qchk
```
2. The screen shown in Figure 10-14 is displayed. In this screen, you can perform the following tasks:
 - Choose to list information about all the print jobs sent to a specific queue by entering the queue name (or * for all the queues)
 - Select a queue after pressing F4 to see the list of the queues.
 - You can specify a print job number or a print job owner name. To list information about a specific job number in the specified queue, fill in the job number in the Print JOB NUMBER field with the correct job number. To list information about a specific print job owner in the specified queue, fill in the Print JOB OWNER field with the print job owner's user ID.

Press Enter to see the results.

```

                                Show the Status of Print Jobs

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]                                [Entry
* PRINT QUEUE name (* for all queues)  [*]
+
  Print JOB NUMBER                       [] +#
  Print JOB OWNER                         []

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command          F7=Edit           F8=Image
F9=Shell        F10=Exit             Enter=Do

```

Figure 10-14 Show the Status of Print Jobs

Figure 10-15 shows the status of the queue and the jobs in the tdipclq queue.

```

                                COMMAND STATUS
Command: OK                      stdout: yes                      stderr: no

Before command completion, additional instructions may appear below.

Queue  Dev  Status  Job Files                      User      PP %
Blks  Cp Rnk
-----
tdipcl  lp0  DEV_WAIT
      QUEUED  7 /etc/motd                      root
      1  1  1
      QUEUED  8 /etc/hosts                      root
      1  1  1
      QUEUED  9 /.profile                      root
      1  1  1
      QUEUED  10 /.cshrc                      root
      1  1  1

F1=Help          F2=Refresh          F3=Cancel
F6=Command       F9=Shell           F10=Exit          /=Find
F8=Image
n=Find Next

```

Figure 10-15 Command status

Table 10-3 shows how to list jobs in a printer queue using the three different commands.

Table 10-3 List jobs in a printer queue

System V	BSD	AIX 5L
lpstat	lpq	qchk

The **qchk** command displays the current status information regarding specified print jobs, print queues, or users. Use the appropriate flag followed by the requested name or number to indicate specific status information.

The **qchk** command with no flags specifies the default print queue. Following is an explanation of the flags used in this example:

- ▶ The **-A** flag specifies all the queues.
- ▶ The **-L** flag specifies the long form mode.
- ▶ The **-w delay** flag specifies that the print status be displayed until all the print jobs are completed. The status is displayed by updating the screen every five seconds (delay seconds).

To display the status for the **tdipsq** queue, we used the **-P** flag, which specifies the queue (**tdipsq**). To display the status for job number 12, enter the following command:

```
# qchk -#12
```

Table 10-4 illustrates the key attributes reported through the queue status commands and what they refer to.

Table 10-4 *qchk* attributes

Attribute	Description
Queue	The queue name used in the qconfig file
Dev	The queue device name used in the qconfig file
Status	The current status of the job
Job	The job number of this print job, which is used by many of the print spooling subsystem control commands, such as qcan
Files	The name of the files being printed
User	The user ID of the user who owns the job
PP	Pages in the requested print job
%	Percentage of the job completed so far
Blks	The number of blocks the print job has been broken into
Cp	The number of copies of the requested print job that will be printed
Rnk	The job's rank in the print queue. The job ranked 1 should be printing.

10.4.3 Print queue status

Table 10-5 shows the different queue status modes.

Table 10-5 Queue status modes

Status	Description
READY	Indicates that the printer is up and ready to accept jobs
DEV_WAIT	Indicates that the printer is not online, out of paper, has a paper jam, or any similar problem that will prevent the job from printing normally. The problem that causes this state also causes a message to be sent to the job owner or the operator.
RUNNING	Indicates that a job is either enrolled to be printed or is printing
HELD	Indicates that the job is held and will not be put on the queue until it is released using the qhld or enq command
DOWN	Indicates that the printer is not online. It has probably been taken offline by the operator for maintenance.
UNKNOWN	Indicates that the status command cannot determine the status of the printer. This state is often an indicator of problems with printers or the print spooling subsystem.
OPR_WAIT	Indicates that the job is suspended, waiting for an operator response to a message

Examples

To display the queue status for a queue every five seconds, use the following command:

```
# enq -P wsmq -A -w 2
```

To get the status of only local queues, so that you do not have to wait for the remote queues to time out on unavailable or slow servers, use the following command:

```
# enq -P remque -isA
```

To display queues with long queue names, use the following command:

```
# lpstat -vnet17a -W
```

10.4.4 Cancelling a printing job

The **qcan** command cancels either a particular job number or all the jobs in a print queue. Normal users can only cancel their own jobs, but a root user or a member of the `printq` group can cancel any job from any queue.

To cancel a job, use the **smitty qcan** fast path, the Web-based System Manager, or the commands in Table 10-6.

Table 10-6 Cancel a print job

System V	BSD	AIX 5L
<code>cancel</code>	<code>lprm</code>	<code>qcan</code>

Examples

To cancel Job Number 127 on whatever queue the job is on, run the following:

```
# qcan -x 127 or # cancel 127
```

To cancel all the jobs queued on printer `lp0`, enter:

```
# qcan -X -Plp0 or # cancel lp0
```

10.4.5 Prioritizing a printing job

The discipline line in the `/etc/qconfig` file determines the order in which the printer serves the requests in the queue. In the queue stanza, the discipline field can either be set to first-come-first-serve (`fcfs`) or shortest-job-next (`sjn`). If there is no discipline in the queue stanza, requests are serviced in the `fcfs` order.

Each print job also has a priority that can be changed through SMIT or with the **qpri** command.

Print jobs with high priority numbers are handled before requests with low priority numbers. Only a user who has root authority or who belongs to the `printq` group can change the priority of a local print request.

Note: You can only set priorities on local print jobs. Remote print jobs are *not* supported.

The **qprt -R** command can also be used to set job priority. Use the **qchk -L** command to show the new job priorities. Following are some of the characteristics of this command:

- ▶ The **qpri** command prioritizes a job in a print queue by specifying the job number and giving it a priority number.
- ▶ The **qpri** command works only on local print jobs. Remote print jobs are not supported.
- ▶ After a job has been sent to a remote host, that host can change the job's priority, but the sender cannot.
- ▶ You must have root user authority or belong to either the system group or the printq group to run this command.

Example 10-3 shows how to change priorities on a print job.

Example 10-3 The qpri command

```
# qchk -A
5132pcl 1p0  DEV_WAIT
           QUEUED    7  /etc/motd  root           1
           1      1
           QUEUED    8  /etc/hosts root           2
           1      2
           QUEUED   17  /.profile  root           2
           1      3
           QUEUED   27  /.puttifar root           2
           1      4
5132psq 1p0  DEV_WAIT
# qpri -#27 -a 20
# qchk -A
5132pcl 1p0  DEV_WAIT
           QUEUED    27 /.puttifar root           2
           1      1
           QUEUED    7  /etc/motd  root           1
           1      2
           QUEUED    8  /etc/hosts root           2
           1      3
           QUEUED   17  /.profile  root           2
           1      4
5132psq 1p0  DEV_WAIT
```

In our example, we changed the priority of job number 27 and then verified whether the priority and the rank has changed.

In **qpri** command shown in Example 10-3:

- ▶ The `-#flag` specifies the Job Number (14) whose priority should be changed.
- ▶ The `-a` flag specifies the Priority Number to be assigned (20).

SMIT and the Web-based System Manager can also be used to change print job priorities. The `smit` fast path is `smitty qpri`.

10.4.6 Holding and releasing a printing job

The `qhld` command is used to put a temporary hold on a job that is waiting in the queue. The `qhld` command is also the command that is used to release a job back into the queue. Following are some of the characteristics of this command:

- ▶ The `qhld` command holds and releases a spooled print job that is not being printed.
- ▶ The `qhld` command works on local queues only (remote queues are not supported).
- ▶ You must have root authority, be a member of the `printq` group, or be the print job owner to use this command.
- ▶ You can hold or release a spooled job through the SMIT (`smitty qhld`), the command line, or the Web-based System Manager.

In the `qhld` command:

- ▶ The `-r` flag specifies the job to be released.
- ▶ The `-#` flag specifies the job number to be released.

In Example 10-4, the `-#` flag specifies the Job Number (27) to be put in HELD state. To release Job Number 27, we used the `-r` flag. Note that releasing Job Number 27 has changed its state from HELD to QUEUED.

Example 10-4 The `qhld` command

```
# qchk -A
Queue   Dev    Status   Job   Files   User   PP   %   Blks   Cp
Rnk
-----
-----
5132pc1 1p0    DEV_WAIT
        QUEUED   7   /etc/motd  root           1
      1    1
        QUEUED   8   /etc/hosts  root           2
      1    2
        QUEUED  17   /.profile  root           2
      1    3
```

```

        QUEUED      27  /.puttifar root          2
    1      4
5132psq lp0      DEV_WAIT
# qhld -#27
# qchk -A
Queue   Dev   Status   Job   Files   User   PP   %   Blks   Cp
Rnk
-----
-----
5132pc1 lp0      DEV_WAIT
        QUEUED      7  /etc/motd root          1
    1      1
        QUEUED      8  /etc/hosts root        2
    1      2
        QUEUED     17  /.profile root         2
    1      3
        HELD       27  /.puttifar root        2
    1      4
5132psq lp0      DEV_WAIT
# qhld -r -#14
# qchk -A
Queue   Dev   Status   Job   Files   User   PP   %   Blks   Cp
Rnk
-----
-----
5132pc1 lp0      DEV_WAIT
        QUEUED      7  /etc/motd root          1
    1      1
        QUEUED      8  /etc/hosts root        2
    1      2
        QUEUED     17  /.profile root         2
    1      3
        QUEUED     27  /.puttifar root        2
    1      4
5132psq lp0      DEV_WAIT

```

10.4.7 Moving a job between queues

Imagine a situation where you have two queues that have the same printing capabilities. The first queue has many print jobs enqueued, and the second is idle, without any print requests. In a situation such as this, it is a good idea to move some print jobs from the first queue to the second one.

The **qmov** command moves jobs between queues by specifying the destination queue, the job number, the queue name containing all the jobs you want to move, and the user whose jobs you want to move.

Example 10-5 shows four jobs in the 5132pclq queue. Because the last one is a PostScript file, move this print job (job ID 27) to the 8213psq queue.

Example 10-5 The qmov command

```
# qchk -A
Queue      Dev    Status   Job   Files   User   PP   %   Blks   Cp
Rnk
-----
-----
5132pcl   1p0    DEV_WAIT
          QUEUED    7   /etc/motd  root           1
      1     1
          QUEUED    8   /etc/hosts  root           2
      1     2
          QUEUED   17   /.profile  root           2
      1     3
          QUEUED   27   /.puttifar  root           2
      1     4
8213psq  1p0    DEV_WAIT
# qmov -m 8213psq -#27
# qchk -A
Queue      Dev    Status   Job   Files   User   PP   %   Blks   Cp
Rnk
-----
-----
5132pclq  1p0    DEV_WAIT
          QUEUED    7   /etc/motd  root           1
      1     1
          QUEUED    8   /etc/hosts  root           2
      1     2
          QUEUED   17   /.profile  root           2
      1     3
8213psq  1p0    DEV_WAIT
          QUEUED   27   /.puttifar  root           2
      1     1
```

In the **qmov** command:

- ▶ The **-m** flag specifies the destination queue.
- ▶ The **-#** flag specifies the Job Number to be moved.

What about moving all the print jobs from the 5132pclq queue to the 8213psq queue? You can use the following command to move all the jobs (except a job in rank position 1 if the status is running) from the 5132pclq queue to the 8213psq queue:

```
# qmov -m 5132psq -P 8213pclq
```

In this command:

- ▶ The `-m` flag specifies the destination queue.
- ▶ The `-P` flag specifies the origin queue of the jobs to be moved.

10.5 Printer pooling

Print queues can be serviced by more than one printer through printer pooling. This means that a user can submit the job to a queue, and the print service will select the first available printer assigned to that queue. Multiple printers are assigned to a single queue through the use of multiple queue devices for the same queue.

The first virtual printer is created in the normal way, as described in 10.3.1, “Adding a local print queue” on page 284. To add additional queue devices, use the SMIT option Add an Additional Printer to an Existing Print Queue through the **smitty spooler** fast path and perform the corresponding steps for adding a local printer. The last screen allows you to enter the name of an existing print queue. Add the queue name that you added in the first step.

When printer pooling is in effect, all the jobs print to the printer defined in the first queue device listed in `/etc/qconfig`, unless that printer is busy. If that printer is busy, the job is printed to the printer defined in the next queue device, assuming it is not busy. This is similar to printer classes in System V printing.

10.6 Using System V print subsystem on AIX 5L

The default print subsystem in AIX 5L is the current AIX 5L print subsystem. The System V print subsystem is an alternate method of printing. At install time, the AIX 5L subsystem is always set as the active one, and System V is always inactive. Both cannot be set to active state at the same time using the normal procedures. However, there is nothing to prevent an administrator from overriding this manually for some print operations.

There are three ways in which you can switch between print subsystems:

- ▶ From Web-based System Manager
- ▶ Using SMIT
- ▶ Using the command line

Figure 10-16 show how this is accomplished by using SMIT and the command line. The option to Change/Show Current Print Subsystem has been added to the top-level Print Spooling menu in SMIT, as shown in Figure 10-16.

```
Print Spooling

Move cursor to desired item and press Enter.

AIX Print Mode Only:

Start a Print Job
Manage Print Jobs
List All Print Queues
Manage Print Queues
Add a Print Queue
Add an Additional Printer to an Existing Print Queue
Change / Show Print Queue Characteristics
Change / Show Printer Connection Characteristics
Remove a Print Queue
Manage Print Server
Programming Tools

AIX and System V Print Mode:

Change / Show Current Print Subsystem

F1=Help      F2=Refresh   F3=Cancel    F8=Image
F9=Shell     F10=Exit    Enter=Do
```

Figure 10-16 Changing the print subsystem

On selecting **Change/Show Current Print Subsystem**, the next screen displays the line to select the print subsystem:

Change / Show Current Print Subsystem [AIX]

The current subsystem is displayed in the box on the right, and the field toggles between the two choices, AIX 5L and System V. Executing the panel runs the `/usr/aix/bin/switch.prt` command, which in turn runs the `/usr/aix/bin/switch.prt.subsystem` script that takes the value displayed as input. Running the command with the current system as input results in an error. Running the command with the alternate subsystem switches the system from the current one to the alternate one. The more the queues that are defined in the subsystem that you are exiting, the longer it takes for the command to switch.

Using the command line

Use the `switch.prt` command to switch between the printer subsystems or to display the currently active printer subsystem. The syntax of the command is:

```
# switch.prt [-s print_subsystem] [-d]
```

The valid values for `print_subsystem` are AIX 5L and System V. Running the command with the `-d` flag displays the current print subsystem, for example:

```
# switch.prt -s SystemV
# switch.prt -s AIX
```

For security reasons, the `switch.prt` command is a front end to the `/usr/aix/bin/switch.prt.subsystem` script, which performs the actual work. This command is also called by the Web-based System Manager and SMIT interfaces.

10.7 System files associated with printing

Following are the characteristics of system files associated with printing:

- ▶ The `/etc/qconfig` file describes the queues and the devices available for use by the printing commands.
- ▶ The `/var/spool` directory contains the files and the directories used by the printing programs and daemons.
- ▶ The `/var/spool/lpd/qdir` directory contains information about files queued to print.
- ▶ The `/var/spool/qdaemon` directory contains copies of the files that are spooled to print.
- ▶ The `/var/spool/lpd/stat` directory is where the information about the status of jobs is stored. It is used by the `qdaemon` and the back-end programs.
- ▶ The `/var/spool/lpd/pio/@local` directory holds the virtual printer definitions. This is where the attributes of the printers are paired with the attributes of the corresponding data stream types.

It is recommended that SMIT be used to update these device-related files. In most cases, updating standard system files is *not* recommended.

10.8 Remote printing

When printing to a remote server, the administrator of that remote server must already have performed several tasks to enable remote printing.

This section shows how to configure remote printers by using SMIT:

1. Use the **smitty mkpq** fast path or work through the SMIT menus by typing # smitty and selecting **Print Spooling** → **Add a Print Queue**.

The screen looks as shown in Figure 10-1 on page 285.

2. In our example, we defined an IBM 3130 attached to a remote RS/6000. Therefore, we selected **Remote** and pressed Enter. The menu shown in Figure 10-17 is displayed. We selected Standard processing.

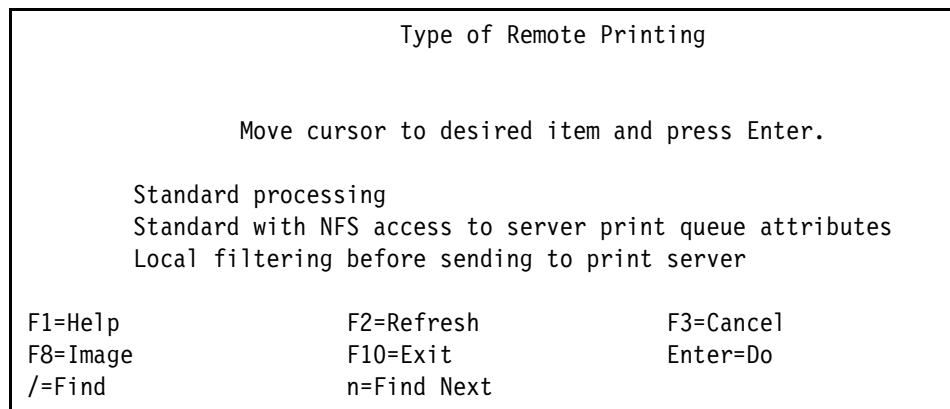


Figure 10-17 Type of Remote Printing

3. The screen shown in Figure 10-18 is displayed. We entered the host name of the remote server (although we could also have entered the dotted decimal address), the name of the print queue that was already defined on that remote server, and the type of spooler used by the remote server. Because the remote server was running AIX 5L, we selected AIX 5L Version 3 or 4.

Other options for this field include BSD, System V, and AIX 5L Version 2 (RT PC). We did not set a timeout value for the back end, and left it at the default value of 90 seconds. We chose not to send the control file before the data file. After entering all these values, we pressed Enter.

```

                                Add a Standard Remote Print Queue

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]                                [Entry
* Name of QUEUE to add                 []
* HOSTNAME of remote server            []
* Name of QUEUE on remote server       []
  Type of print spooler on remote server  AIX Version 3
or 4      +
  Backend TIME OUT period (minutes)     [] #
  Send control file first?               no
+
  To turn on debugging, specify output  []
  file pathname
  DESCRIPTION of printer on remote server []

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit       Enter=Do

```

Figure 10-18 Standard remote queue

Figure 10-19 shows a completed SMIT configuration screen.

```

                                Add a Standard Remote Print Queue

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry
Fields]
* Name of QUEUE to add           [rprinter1]
* HOSTNAME of remote server     [printserver1]
* Name of QUEUE on remote server [printer1]
  Type of print spooler on remote server AIX Version 3
or 4 +
  Backend TIME OUT period (minutes)   []
#
  Send control file first?           no
+
  To turn on debugging, specify output file pathname []
  DESCRIPTION of printer on remote server []

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit       Enter=Do

```

Figure 10-19 Remote print configuration filled out

Figure 10-20 shows the different options for the remote print queue type.

```

Add a Standard Remote Print Queue

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

* Name of QUEUE to add                [Entry Fields]
* HOSTNAME of remote server           [rprinter1]
* Name of QUEUE on remote server      [printserver1]
Type of print spooler on remote server [printer1]
                                         AIX Version 3 or 4
+
+-----+
#
|                                     Type of print spooler on remote server
|
|
| Move cursor to desired item and press Enter.
|
|
| AIX Version 3 or 4
|
| BSD
|
| System V
|
| AIX Version 2 (RT PC)
|
|
| F1=Help           F2=Refresh           F3=Cancel
|
| F1| F8=Image      F10=Exit            Enter=Do
|
| F5| /=Find        n=Find Next
|
| F9+-----+
-+

```

Figure 10-20 Remote spooler options

Select the appropriate remote print spooler type to ensure the correct functioning of the remote queue:

- ▶ AIX 5L Version 3 or 4
This is used when the remote print server is another AIX 5L V3 or later server.
- ▶ BSD
This is used when the remote print server is using the BSD lpd printing service, for example, FreeBSD, NetBSD, Linux.
- ▶ System V
This is used when the remote print server is using the System V Ipsched printing service, for example, Solaris, HP-UX.
- ▶ AIX 5L Version 2 (RT PC)
This is used when the remote print server is an IBM RT PC running AIX 5L V2. (This is unlikely unless you are working in a computer museum.)

10.9 Common UNIX Printing System

Common UNIX Printing System (CUPS) is a publicly available printing subsystem that can be used on a number of different UNIX-based platforms, including AIX 5L and Solaris. It is most commonly used as the default printing subsystem on Linux distributions. For more information about CUPS, refer to the following Web site:

<http://www.cups.org>

To download binaries, refer to the following Web site:

<http://aixpdslib.seas.ucla.edu/packages/cups.html>

10.10 Quick reference

Table 10-7 provides a quick reference for print management in AIX 5L and Solaris.

Table 10-7 Quick reference for print management

Task	AIX 5L	Solaris
Run multiple tasks in a GUI environment	Choose one of the following: <ul style="list-style-type: none"> ▶ The smitty print fast path ▶ smitty ▶ The Web-based System Manager 	<ul style="list-style-type: none"> ▶ smc or ▶ printmgr
Add a printer	mkdev	lpadmin
Start a print queue	<ul style="list-style-type: none"> ▶ qadm (AIX 5L printing subsystem) or ▶ lpc (System V) 	<ul style="list-style-type: none"> ▶ accept and ▶ enable
Stop a print queue	<ul style="list-style-type: none"> ▶ qadm (AIX 5L printing subsystem) or ▶ lpc (System V) 	<ul style="list-style-type: none"> ▶ disable and ▶ reject
Display print queue status	lpstat	lpstat
Cancel a printing job	qcan	cancel
Add a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> – mkque – mkquedev – mkvirprt ▶ System V: <ul style="list-style-type: none"> lpadmin -p 	lpadmin

Task	AIX 5L	Solaris
Change a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> - chque - chquedev - chvirprt ▶ System V: <ul style="list-style-type: none"> lpadmin -p 	lpadmin
Remove a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> - rmque - rmquedev - rmvirprt ▶ System V: <ul style="list-style-type: none"> lpadmin -x 	lpadmin -x
Display settings of a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> - lsque - lsquedev - lsvirprt ▶ System V: <ul style="list-style-type: none"> lpstat 	lpadmin



Users and groups

This chapter provides guidelines and planning information for managing user accounts and groups. It includes information about the files used to store user accounts and group information and information about customizing the user's work environment. This chapter also describes the basic differences between Solaris and AIX 5L and references the important files.

This chapter covers the following topics:

- ▶ 11.1, "Overview" on page 322
- ▶ 11.2, "Adding users" on page 325
- ▶ 11.3, "Removing users" on page 328
- ▶ 11.4, "Displaying users who are currently logged in" on page 329
- ▶ 11.5, "Changing users, passwords, and other attributes" on page 331
- ▶ 11.6, "Customizing a user's work environment" on page 341
- ▶ 11.7, "Password files" on page 344
- ▶ 11.8, "Administering groups" on page 347
- ▶ 11.9, "Checking for inconsistencies in passwords and group definitions" on page 353
- ▶ 11.10, "Defining the system resource limits for users" on page 355
- ▶ 11.11, "Quick reference" on page 357

11.1 Overview

One of the basic system administration tasks is to set up a user account for each user. A typical user account includes the information that a user requires to log in and use a system. User account information consists of five main components:

- ▶ User name
A unique name that a user requires to log in to a system. It is also known as a login name.
- ▶ Password
A secret combination of characters that a user must enter along with the user name to gain access to a system.
- ▶ Home directory
Each user must have a directory designated especially to that user. This is typically the user's current directory at login. The user must have full permission to access that directory and the files it contains.
- ▶ Initialization files
These are typically shell scripts that control how the user's working environment is set up when a user logs in to a system. There are system-wide environment files and a user's own files, usually located in the user's home directory.
- ▶ Group
User groups must be created for people who have to share files on the system, such as people who work in the same department or people who are working on the same project. In general, create as few user groups as possible. Usually, there are some system-defined and system administrator groups, but it is always a good idea to create your own groups for managing user accounts.

User accounts, their passwords, and groups are fundamentals of system security. Therefore, it is important to have them set properly. User management policy is also considered a part of system security policy. User management usually means the following tasks and issues:

- ▶ Adding users
- ▶ Removing users
- ▶ Listing users
- ▶ Changing users' passwords and other attributes
- ▶ User and system-wide environment files
- ▶ Password files

- ▶ Profile template
- ▶ Defining system resource limits for users
- ▶ Configuration information for user authentication
- ▶ Working with groups

This chapter describes all these points, compares Solaris and AIX 5L with regard to these topics, and provides a quick reference.

A variety of tools exist for managing user accounts and groups in both Solaris and AIX 5L operating systems (OS).

In Solaris you can use the following options for user and group management:

- ▶ Admin Tool
- ▶ Solaris Management Console
- ▶ Command-line based management

The following list includes the commands used for user administration in Solaris:

- ▶ **useradd**
Creates a new user login on the system
- ▶ **passwd**
Changes the user login password and attributes
- ▶ **usermod**
Changes the user login attributes
- ▶ **logins**
Displays system and user login data
- ▶ **listusers**
Lists users login details
- ▶ **userdel**
Removes a user login from its home directory
- ▶ **who**
Identifies the users currently logged in
- ▶ **groupadd**
Creates a new group on the system
- ▶ **groupmod**
Modifies a group on the system
- ▶ **groupdel**
Removes a group from the system

In AIX 5L, you have the following tools:

- ▶ Web-based System Manager
- ▶ System Management Interface Tool (SMIT)
- ▶ Command line-based management

Figure 11-1 shows the Web-based System Manager menu that must be used for managing users and groups. With this menu, you can perform most of the tasks relating to user management.

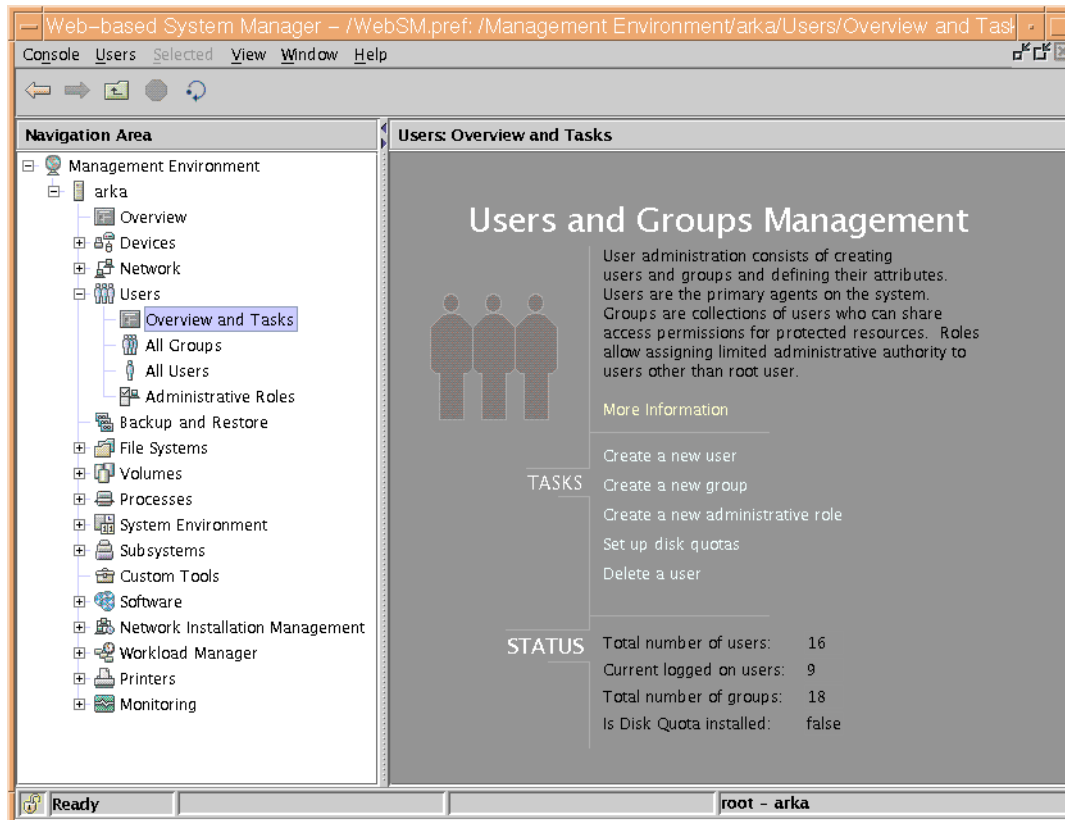


Figure 11-1 Web-based System Manager: Users and Groups Management

The following list includes the most important commands used for user administration in AIX 5L:

- ▶ **mkuser**
Creates a new user account
- ▶ **passwd**
Creates or changes the password of a user

- ▶ **chpasswd**
A noninteractive command for creating or changing passwords of users. Designed to be used in a script.
- ▶ **chuser**
Changes user attributes except password
- ▶ **lsuser**
Lists user attributes
- ▶ **rmuser**
Removes a user and user's attributes
- ▶ **chsec**
Changes security attributes in the configuration files
- ▶ **login**
Initiates a user session
- ▶ **who**
Identifies the users currently logged in
- ▶ **dtconfig**
Enables or disables the desktop autostart feature

The differences are in the tools and commands available in both the OS to perform these tasks. The basic functionality of the commands is similar.

11.2 Adding users

This section describes how to manage users in Solaris and AIX 5L.

In Solaris

In Solaris, the **useradd** and **groupadd** commands are most commonly used to create user logins and groups on the system. Example 11-1 shows how to create a new user login from the command line.

Example 11-1 Creating a new user login from the command line

```
useradd -g resgroup -s /usr/bin/ksh -c "Hess Waltman Tel-241498" -m  
hessw.  
passwd hessw
```

The **useradd** command with only the **-D** option displays the default values that will be used when creating a new user login. The values displayed are group, home directory, shell, skeleton directory, inactive, and expire. These values can be modified with the **useradd** command so that new logins are created with the changed values. Example 11-2 shows the **useradd** defaults.

Example 11-2 The useradd defaults

```
# useradd -D
group=other,1 project=default,3 basedir=/home
skel=/etc/skel shell=/bin/sh inactive=0
expire= auths= profiles= roles=
```

The following command shows the current default values used when creating a new user login if the values are not specified on the command line:

```
# useradd -D -b /prod/home
```

This command changes the default value for the home directory to `/prod/home`. This applies to the new user logins created. The file that is updated and stores the default values is `/usr/sadm/defadduser`.

In AIX 5L

In AIX 5L, the **mkuser** command creates a new user account. By default, the name parameter must be a unique eight byte or less string. However, from AIX 5L V5.3, its length is configurable with the **chdev** command. By default, the **mkuser** command creates a standard user account.

To create an administrative user account, specify the **-a** flag. The **mkuser** command does *not* create password information for a user. Therefore, the new accounts are disabled until the **passwd** command is used to add authentication information to the `/etc/security/passwd` file. The **mkuser** command only initializes the password attribute of the `/etc/passwd` file with an asterisk (*).

Following are some possible options:

- ▶ To create the smith account with smith as an administrator, enter:

```
mkuser -a smith
```

You must be the root user to create Smith as an administrative user.
- ▶ To create the smith user account and set the su attribute to a value of false, enter:

```
mkuser su=false smith
```

- To create a user account, smith, with the default values in the `/usr/lib/security/mkuser.default` file, enter:

```
mkuser smith
```

Tip: In AIX 5L, you can also use the `useradd` command to add a new user account. The syntax of the command is exactly the same as in Solaris.

Alternatively, you can use SMIT:

1. Run `smitty mkuser` to access the menu shown in Figure 11-2.
2. Type `annie` against the User NAME field and press Enter to create the user.

```

                                Add a User

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
* User NAME                            [annie]
  User ID                               []
  ADMINISTRATIVE USER?                 false
+
  Primary GROUP                         []
+
  Group SET                             []
+
  ADMINISTRATIVE GROUPS                 []
+
  ROLES                                 []
+
  Another user can SU TO USER?         true
+
  SU GROUPS                             [ALL]
+
  HOME directory                        []
  Initial PROGRAM                       []
  User INFORMATION                      []
  EXPIRATION date (MMDDhhmmyy)         [0]
[MORE...37]

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit         Enter=Do

```

Figure 11-2 Adding a user

3. When SMIT returns an OK prompt, press F10 to return to the command prompt.

11.3 Removing users

This section discusses how to remove users in Solaris and AIX 5L.

In Solaris

The most common way to remove a user on Solaris is to use the **userdel** command. The **-r** option removes the home directory of the user. An example of using the **userdel** command to delete an existing user account is:

```
userdel -r annie
```

In AIX 5L

In AIX 5L, the **rmuser** command removes the user account identified by the Name parameter. This command removes a user's attributes without removing the user's home directory and files. The user name must already exist as a string of eight bytes or less. If the **-p** flag is specified, the **rmuser** command also removes passwords and other user authentication information from the `/etc/security/passwd` file.

Note: Only the root user can remove administrative users.

The following example shows the use of the **rmuser** command to remove a user account smith and its attributes from the local system:

```
rmuser smith
```

To remove the user account smith and all its attributes, including passwords and other user authentication information in the `/etc/security/passwd` file, use the following command:

```
rmuser -p smith
```

Tip: In AIX 5L, you can also use the **userdel** command to remove the user's account. The syntax is exactly the same as in Solaris.

Alternatively, you can use SMIT:

1. Run `smitty rmuser` to open the menu shown in Figure 11-3.
2. Type `annie` against the User NAME field and press Enter.

```
Remove a User from the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields] [Entry
* User NAME [annie]
+
Remove AUTHENTICATION information? yes
+

F1=Help      F2=Refresh   F3=Cancel    F4=List
F5=Reset     F6=Command   F7=Edit      F8=Image
F9=Shell     F10=Exit     Enter=Do
```

Figure 11-3 Removing a user

3. When SMIT returns an OK prompt, press F10 to return to the command prompt.

11.4 Displaying users who are currently logged in

To achieve this task in Solaris, use the `who` or `w` commands as shown in Example 11-3 and Example 11-4.

Example 11-3 The `who` command

```
# who
root pts/1 May 3 09:07 (dragoon)
root pts/3 May 4 15:26 (caw2kvm.itsc.austin.ibm.com)
```

Example 11-4 `w` command

```
# w
 4:13pm up 29 day(s), 1:51, 3 users, load average: 0.00, 0.01,
0.02
User tty login@ idle JCPU PCPU what
```

root	pts/1	Wed 9am	18	1:21	ksh -o vi
root	pts/4	4:13pm	1		-sh
root	pts/3	3:26pm	1	18	w

From the output of the commands, you can gather information about the following:

- ▶ The user name of the user who is logged in
- ▶ The terminal line of the user who is logged in
- ▶ The date and time the user logged in
- ▶ The host name if a user is logged in from a remote system (optional)

In AIX 5L, the same commands are used. Their functionality is also the same. The **who** command displays information about all the users who are currently on the local system. The following information is displayed:

- ▶ Login name
- ▶ tty
- ▶ The date and time of login

Entering `who am i` or `who am I` displays your login name, tty, and the date and time you logged in. If the user is logged in from a remote machine, the host name of that machine is also displayed. The **who** command also displays the time that has elapsed since the line activity occurred, the process ID of the command interpreter (shell), log ins, log offs, restarts, and changes to the system clock, and other processes generated by the initialization process.

Note: The `/etc/utmp` file contains a record of users logged into the system. The `who -a` command processes the `/etc/utmp` file. If this file is corrupted or missing, no output is generated from the `who` command.

Example 11-5 shows the command used to display information about all the users who are logged in to the system.

Example 11-5 The who command

```
[p650n04] [/]> who
root pts/0 Jun 28 13:06 (tot198.itso.ibm.com)
root pts/1 Jun 29 12:26 (fr114p.itso.ibm.com)
root pts/2 Jun 28 14:18 (tot198.itso.ibm.com)
root pts/3 Jun 28 16:30 (fr114p.itso.ibm.com)
annie pts/4 Jun 29 12:53 (fr114p.itso.ibm.com)
```

The following example shows the command used to display your user name:

```
# who am I
root pts/3 Jun 28 16:30 (fr114p.itso.ibm.com)
```

The following example shows how to display the run level of the local system:

```
# who -r
. run-level 2 Jun 28 13:05 2 0 S
```

11.5 Changing users, passwords, and other attributes

In Solaris, following are some of the tasks pertaining to changing user login attributes:

- ▶ Change a user's password
- ▶ Disable a user's account
- ▶ Change password aging for a user account
- ▶ Change a user's login shell
- ▶ Change a user's primary or secondary group

AIX 5L has a variety of options to choose from when changing a user's attributes, including the ones listed previously. Other than the options listed previously, you can also select the following options:

- ▶ Make a user an administrative user by setting the admin attribute to true
- ▶ Change any attributes of an administrative user
- ▶ Add a user to an administrative group

11.5.1 Changing a user's password

This section describes how to change a user's password in Solaris and AIX 5L.

In Solaris

In Solaris, use the **passwd** command, as shown in Example 11-7.

Example 11-6 Changing a password

```
# passwd phill
New Password:
Re-enter new Password:
passwd: password successfully changed for phill
```

In AIX 5L

In AIX 5L, the **passwd** command creates an encrypted passwd entry in `/etc/security/passwd` and changes the password attribute of `/etc/passwd` from an asterisk (*) to an exclamation (!).

To change your full name in the `/etc/passwd` file, enter the following command:

```
# passwd -f smith
```

The **passwd** command displays the name stored for your user ID, for example, for the login name `annie`, the **passwd** command might display the message shown in Example 11-7.

If you enter a Y for yes, the **passwd** command prompts you for the new name. The **passwd** command records the name you enter in the `/etc/passwd` file.

Example 11-7 Using passwd for full name change

```
# passwd -f annie
annie's current gecoc:
      ""
Change (yes) or (no)? > n
Gecos information not changed.
```

To change your password, enter **passwd**. The **passwd** command prompts you for your old password if it exists and if you are *not* the root user. After you enter the old password, the command prompts you twice for the new password.

You can also use **pwdadm**. The **pwdadm** command administers users' passwords. The root user or a member of the security group can supply or change the password of the user specified by the User parameter. The invoker of the command must provide a password when queried, before being allowed to change the other user's password.

When the **pwdadm** command executes, it sets the ADMCHG attribute. This forces the user to change the password the next time a **login** command or an **su** command is given for the user. Only the root user, a member of the security group, or a user with PasswdAdmin authorization can supply or change the password of the user specified by the User parameter. When this command is executed, the password field for the user in the `/etc/passwd` file is set to an exclamation (!), indicating that an encrypted version of the password is in the `/etc/security/passwd` file. The ADMCHG attribute is set when the root user or a member of the security group changes a user's password with the **pwdadm** command. To set a password for user `harrison`, a member of the security group, use the following command:

```
pwdadm harrison
```


When prompted, the user who invoked the command is prompted for a password before smith's password can be changed.

Alternatively, you can use SMIT:

1. Running **smitty passwd** opens the screen shown in Figure 11-4.
2. Type **harrison** against the User NAME field and press Enter.

Change a User's Password

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry
Fields]

User NAME [harrison]

+

F1=Help	F2=Refresh	F3=Cancel	F4=List
F5=Reset	F6=Command	F7=Edit	F8=Image
F9=Shell	F10=Exit	Enter=Do	

Figure 11-4 Changing a user password

3. You will be prompted to enter the new password (twice), as shown in Example 11-8. Enter the new password and press Enter.

Example 11-8 Entering a user password

Changing password for "harrison"
harrison's New password:
Enter the new password again:

4. When SMIT returns an OK prompt, press F10 to return to the command prompt.

11.5.2 Disabling a user account

This section describes how to disable a user account in Solaris and AIX 5L.

In Solaris

In Solaris, one way of disabling a user account is to achieve by locking the account with the following command:

```
passwd -l user_name
```

The account can be unlocked by resetting the users password or by using the following command:

```
passwd -d user_name
```

In AIX 5L

In AIX 5L, you can lock or unlock a user account by using a simple smitty menu. At the command prompt, type **smitty users**, and then select **Lock/Unlock a User's Account**. Select the user name and set "Is this user ACCOUNT LOCKED?" to true, as shown in Figure 11-5.

```

                                Lock / Unlock a User's Account

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry]

Fields]
* User NAME                                adm
  Is this user ACCOUNT LOCKED?            true
+

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit          Enter=Do
```

Figure 11-5 Disabling a user's account

11.5.3 Modifying a user account

This section describes how to modify a user account in Solaris and AIX 5L.

In Solaris

In Solaris, use the **usermod** command to modify the existing user logins.

The **usermod** command modifies a user's login definition on the system. It changes the definition of the specified login and makes the appropriate login-related system file and file system changes. The syntax of the **usermod** command is as shown in Example 11-9.

Example 11-9 The usermod command syntax

```
usermod [ -u uid [-o]] [-g group] [ -G group [ , group...]]  
      [ -d dir [-m]] [-s shell] [-c comment] [-l new_name] [-  
      f inactive] [-e expire] [-A authorization [, authoriza-  
      tion]] [-P profile [, profile]] [-R role [, role]] login
```

To change the home directory of user *annie* to */export/home/annie_new* and move the contents of the original directory, type:

```
usermod -d /export/home/annie_new -m annie
```

To change user *annie* shell to */bin/ksh*, type:

```
usermod -s /bin/ksh annie
```

You can also list a user's attributes. For listing users and their attributes, you can use two commands, the **logins** and the **listusers** commands, which display user login information. The syntax of the **logins** commands is:

```
logins [-admopstux] [-g groups] [-l logins]
```

Example 11-10 shows the **logins** commands.

Example 11-10 The logins command

```
# logins  
root          0      other      1      Super-User  
daemon        1      other      1  
bin           2      bin        2  
sys           3      sys        3  
adm           4      adm        4      Admin  
uucp          5      uucp       5      uucp Admin  
nuucp         9      nuucp      9      uucp Admin  
smmsp        25     smmsp     25     SendMail Message  
Submission Program
```

listen	37	adm	4	Network Admin
lp	71	lp	8	Line Printer Admin
ausres	100	staff	10	
livio	101	other	1	
phill	102	other	1	
nobody	60001	nobody	60001	Nobody
noaccess	60002	noaccess	60002	No Access User
nobody4	65534	nogroup	65534	SunOS 4.x Nobody

The **logins** command displays useful user and system login details. The command is executed without flags. In Example 11-10, the **login** command executes without any flags, displays the user login, the UID, the group name, group ID, and the user login information. Some of the options for the command are:

- ▶ “a” displays the user expiration information
- ▶ “p” displays logins with no passwords
- ▶ “u” displays only user logins
- ▶ “s” displays only system logins
- ▶ “x” displays extended user login details
- ▶ “d” displays logins with duplicate user IDs

For information about using the other options and more details about the **logins** command, refer to the **logins (1M)** manual page. The syntax of the **listusers** commands is:

```
listusers [ -g groups ] [ -l logins ]
```

Example 11-11 shows the **listusers** command.

Example 11-11 The listusers command

```
# listusers
annieh      annie,,
hessw      Hess Waltman Building C Tel-241498
maryanne    Test Mary,Brazil,1817,2094
mysql
tommy      Tom Da,Pok,897,890
```

When executed without any options (Example 11-11), the **listusers** command lists all the user logins sorted by login.

For a detailed description about the available options, refer to the **listusers** man page.

In AIX 5L

In AIX 5L, there are two separate menus for displaying and changing the user attributes.

The **lsuser** command displays the user account attributes. This is similar to the **logins** command in Solaris. You can use this command to list all the attributes of all the users or all the attributes of specific users, except their passwords. Because there is no default parameter, enter *all* the key words to view the attributes of all the users. By default, the **lsuser** command displays all the user attributes. To view selected attributes, use the **-a** List flag. If one or more attributes cannot be read, the **lsuser** command lists as much information as possible.

Note: If you have a Network Information Service (NIS) database installed on your system, some user information might not appear when you use the **lsuser** command.

By default, the **lsuser** command lists each user's attributes on one line. It displays attribute information as Attribute=Value definitions, each separated by a blank space. To list the user attributes in stanza format, use the **-f** flag. To list the information as colon-separated records, use the **-c** flag.

To display the user ID and group-related information for the root account in stanza form, enter the command as shown in Example 11-12.

Example 11-12 The lsuser output for root account, using the stanza format

```
# lsuser -f -a id pgrp home root
root:
    id=0
    pgrp=system
    home=/
```

To display the user ID, groups, and home directory of user annie in colon format, enter:

```
# lsuser -c -a id home groups annie
```

To display all the attributes of user annie in the default format, enter:

```
# lsuser annie
```

All the attribute information is displayed, with each attribute separated by a blank space.

To display all the attributes of all the users, enter:

```
# lsuser ALL
```

All the attribute information is displayed, with each attribute separated by a blank space.

Alternatively, you can use SMIT:

1. Run **smitty lsuser**, which displays the screen shown in Figure 11-6.

```
COMMAND STATUS

Command: OK          stdout: yes          stderr: no

Before command completion, additional instructions may appear below.

[TOP]
root    0          /
daemon  1          /etc
bin     2          /bin
sys     3          /usr/sys
adm     4          /var/adm
uucp    5          /usr/lib/uucp
guest   100        /home/guest
nobody  -2          /
lpd     9          /
lp      11         /var/spool/lp
invscout 200          /var/adm/invscout
snapp   201        /usr/sbin/snapp
nuucp   6          /var/spool/uucppublic
ipsec   202        /etc/ipsec
sshd    204        /var/empty
rootgwm 0          /home/rootgwm
annie   207        /home/annie
harrison 7          /home/harrison

F1=Help          F2=Refresh          F3=Cancel
F6=Command
F8=Image          F9=Shell            F10=Exit            /=Find
n=Find Next
```

Figure 11-6 Listing user attributes

2. When SMIT returns an OK prompt, press F10 to return to the command prompt.

The **chuser** command changes the attributes for the user identified by the Name parameter. The user name must already exist as an alphanumeric string of eight bytes or less.

Note: Do not use the **chuser** command if you have an NIS database installed on your system.

Only a root user can use the **chuser** command to perform the following tasks:

- ▶ Make a user an administrative user by setting the admin attribute to true
- ▶ Change any attributes of an administrative user
- ▶ Add a user to an administrative group

To allow user smith to access a system remotely, enter:

```
# chuser rlogin=true smith
```

To change the date on which the user annie will expire, to 5 p.m., 31 July, 2005, enter:

```
# chuser expires=0731170005 annie
```

To add annie to the programmers' group, enter:

```
# chuser groups=programmers annie
```

Tip: In AIX 5L, you can also use the **usermod** command to modify a user's account. The syntax of the command is exactly the same as in Solaris.

Alternatively, you can use SMIT:

1. Run **smitty chuser**. This displays the screen shown in Figure 11-7.
2. Type **annie** against the User NAME field, use the arrow keys to highlight the Primary GROUP field, type **programmers** in it, and press Enter.

```
Change / Show Characteristics of a User

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                     [Entry
Fields]
* User NAME                               annie
User ID                                   [207]
#
ADMINISTRATIVE USER?                     false
+
Primary GROUP                             [staff]
+
Group SET                                 [staff]
+
ADMINISTRATIVE GROUPS                    []
+
ROLES                                     []
+
Another user can SU TO USER?             true
+
SU GROUPS                                [ALL]
+
HOME directory                           [/home/annie]
Initial PROGRAM                           [/usr/bin/ksh]
User INFORMATION                          []
EXPIRATION date (MMDDhhmmy)              [0]
[MORE...37]

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit       Enter=Do
```

Figure 11-7 Changing user characteristics

3. When SMIT returns an OK prompt, press F10 to return to the command prompt.

11.6 Customizing a user's work environment

Providing user initialization files for the user's login shell is a part of a user's administration task. A user initialization file is usually a shell script that sets up a work environment for a user after the user logs in to a system. In a user initialization file, you can perform all the tasks that you perform in a shell script. However, a user initialization file's primary job is to define the characteristics of a user's work environment, such as a user's search path, environment variables, and windowing environment. Depending on a login shell, different initialization file (or files) are used when a user logs into a system.

In Solaris

Solaris has the following initialization files for different shells:

- ▶ For the Bourne shell: `$HOME/.profile`
- ▶ For the C shell: `$HOME/.cshrc` and `$HOME/.login`
- ▶ For the Korn shell: `$HOME/.profile` and `$HOME/$ENV`

The Solaris environment also provides default user initialization files for each shell in the `/etc/skel` directory on each system:

- ▶ For the C shell: `/etc/skel/local.login` and `/etc/skel/local.cshrc`
- ▶ For the Bourne and Korn shells: `/etc/skel/.profile`

The user initialization files can be customized by both the administrator and the user. This feature can be accomplished with centrally located and globally distributed environment initialization files called site initialization files. These site initialization files provide you with the ability to introduce a new functionality to the user's work environment whenever you want to do so. However, users can still customize their own initialization file located in the users' home directory.

When you reference a site initialization file in a user initialization file, all the updates to the site initialization file are automatically reflected when the user logs in to the system or when a user starts a new shell.

Any customization that can be performed in a user initialization file can also be performed in a site initialization file. These files typically reside on a server (or set of servers), and appear as the first statement in a user initialization file. Also, each site initialization file must be the same type of shell script as the user initialization file that references it.

Tip: It is always a good practice to reference the site initialization files or the files in a user initialization file.

In AIX 5L

In AIX 5L, the default shell is Korn shell. In AIX 5L, the purpose of providing and using initialization files is exactly the same as in Solaris. The only difference is in the names and the locations of the files. Following is a list of some of the important initialization files in AIX 5L:

- ▶ `/etc/security/environ`
Contains the environment attributes for users
- ▶ `/etc/environment`
- ▶ Specifies the basic environment for all the processes
- ▶ `/etc/profile`
Specifies additional environment settings for all the users
- ▶ `$HOME/.profile`
Specifies environment settings for specific user requirements

/etc/security/environ

The `/etc/security/environ` file is an American Standard Code for Information Interchange (ASCII) file that contains stanzas with the environment attributes for users. Each stanza is identified by a user name and contains attributes in the `Attribute=Value` form, with a comma separating the attributes. Each line is ended by a new-line character, and each stanza is ended by an additional new-line character. If the environment attributes are not defined, the system uses the default values.

The `mkuser` command creates a user stanza in this file. The initialization of the attributes depends on their values in the `/usr/lib/security/mkuser.default` file. The `chuser` command can change these attributes, and the `lsuser` command can display them. The `rmuser` command removes the entire record for a user.

A basic `/etc/security/environ` file is shown in Example 11-13. In this example, no environment attributes are defined. Therefore, the system is using default values.

Example 11-13 Basic /etc/security/environ file contents

```
# pg /etc/security/environ
default:
root:
daemon:
bin:
```

sys:
adm:
uucp:
guest:

/etc/environment

The `/etc/environment` file contains variables specifying the basic environment for all the processes. When a new process begins, the `exec` subroutine makes an array of strings that have the form `Name=Value`, available. This array of strings is called the environment. Each name that is defined by one of the strings is called an environment variable or shell variable. The environment variables are examined when a command starts running.

The `/etc/environment` file is not a shell script. It must only contain data in the `Name=Value` format, and must not contain shell commands. Trying to run commands from this file might cause a failure of the initialization process.

When you log in, the system sets environment variables from the environment file before reading your login profile, `.profile`. Following is a list of some of the variables that make up a part of the basic environment:

▶ HOME

The full path name of the user login or HOME directory. The login program sets this to the directory specified in the `/etc/passwd` file.

▶ LANG

The locale name currently in effect. The LANG variable is set in the `/etc/environment` file at installation time.

▶ NLSPATH

The full path name for message catalogs.

▶ PATH

The sequence of directories that commands such as `sh`, `time`, `nice`, and `nohup` search when looking for a command whose path name is incomplete. The directory names are separated by colons.

▶ TZ

The time zone information. The TZ environment variable is set by the `/etc/environment` file.

Note: Changing the time zone affects only the processes that begin after the change is made. The init process only reads `/etc/environment` at startup. Therefore, init and its child processes are not aware of a change to TZ until the system is rebooted.

/etc/profile and \$HOME/.profile

The `/etc/profile` file contains more environment variables and commands that are applicable to all the users. Use the `/etc/profile` file to control the following variables:

- ▶ Export variables
- ▶ File creation mask (umask)
- ▶ Terminal types
- ▶ Mail messages to indicate when new mail has arrived

The commands to be included in `/etc/profile` must be appropriate for all the users of the system. An example of a command that you might want all the users to run when they log in is the `news` command.

The `$HOME/.profile` file allows you to customize your individual working environment. The `.profile` file also overrides commands and variables set in the `/etc/profile` file. Use the `.profile` file to control personal settings such as the following:

- ▶ Shells to open
- ▶ Default editor
- ▶ Default printer
- ▶ Prompt appearance
- ▶ Keyboard sound

11.7 Password files

In both Solaris and AIX 5L, the purpose and location of the password files is similar. The files are located in the `/etc` directory. In Solaris, the files are `/etc/passwd` and `/etc/shadow`. For AIX 5L, the two basic files are `/etc/passwd` and `/etc/security/passwd`.

In Solaris

Solaris uses a system called shadow passwords. This is where the encrypted passwords are not stored in the `/etc/passwd` file that is world readable. They are stored in the protected shadow file, `/etc/shadow`. This file is accessible only to privileged users.

In AIX 5L

In AIX 5L, the `/etc/passwd` file contains basic user attributes. This is an ASCII file that contains an entry for each user. Each entry defines the basic attributes applied to a user.

When you use the `mkuser` command to add a user to your system, the command updates the `/etc/passwd` file.

An entry in the `/etc/passwd` file has the following form with all the attributes separated by a colon (:):

```
Name:Password:UserID:PrincipleGroup:Gecos:HomeDirectory:Shell
```

Password attributes can contain an asterisk (*), indicating an incorrect password, or an exclamation point (!), indicating that the password is in the `/etc/security/passwd` file. Under normal conditions, the field contains an exclamation point (!). If the field has an asterisk (*), and a password is required for user authentication, the user cannot log in.

The shell attribute specifies the initial program or shell (login shell) that is started after a user invokes the `login` command or `su` command. The Korn shell is the standard OS login shell and is backwardly compatible with the Bourne shell. If a user does not have a defined shell (`/usr/bin/sh`), the system default shell (Bourne shell) is used.

The `mkuser` command adds new entries to the `/etc/passwd` file and fills in the attribute values as defined in the `/usr/lib/security/mkuser.default` file. The Password attribute is always initialized to an asterisk (*), which is an invalid password. You can set the password with the `passwd`, `chpasswd`, or `pwdadm` commands. When the password is changed, an exclamation point (!) is added to the `/etc/passwd` file, indicating that the encrypted password is in the `/etc/security/passwd` file.

Use the `chuser` command to change all the user attributes except the password. The `chfn` command and the `chsh` command change the Gecos attribute and Shell attribute, respectively. To display all the attributes in this file, use the `lsuser` command. To remove a user and all the user's attributes, use the `rmuser` command.

Example 11-14 shows a sample listing of the `/etc/passwd` file.

Example 11-14 Contents of the `/etc/passwd` file

```
# cat /etc/passwd
root!:0:0:/:usr/bin/ksh
daemon!:1:1::/etc:
bin!:2:2::/bin:
sys!:3:3::/usr/sys:
adm!:4:4::/var/adm:
uucp!:5:5::/usr/lib/uucp:
guest!:100:100:~/home/guest:
nobody!:4294967294:4294967294:/:
lpd!:9:4294967294:/:
lp*:11:11:~/var/spool/lp:/bin/false
invscout*:200:1:~/var/adm/invscout:/usr/bin/ksh
snapp*:201:12:snapp login user:/usr/sbin/snapp:/usr/sbin/snappd
nuucp*:6:5:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uucico
ipsec*:202:1:~/etc/ipsec:/usr/bin/ksh
sshd*:204:202:~/var/empty:/usr/bin/ksh
rootgwm!:0:0:Geoffs root:/home/rootgwm:/usr/bin/ksh
annie!:207:1:~/home/annie:/usr/bin/ksh
harrison!:7:7:~/home/harrison:/usr/bin/ksh
```

The `/etc/security/passwd` file is an ASCII file that contains stanzas with password information. Each stanza is identified by a user name followed by a colon (:) and contains attributes in the form `Attribute=Value`. Each attribute is ended with a new line character, and each stanza is ended with an additional new line character.

Although each user name must be in the `/etc/passwd` file, it is not necessary to have each user name listed in the `/etc/security/passwd` file. A typical file contains contents similar to that shown in Example 11-15.

Example 11-15 Contents of the `/etc/security/passwd` file

```
# cat /etc/security/passwd
root:
    password = tnYdhjq5G2h.2
    lastupdate = 1109024627
    flags =

daemon:
    password = *

bin:
```

```
password = *

sys:
password = *

adm:
password = *

uucp:
password = *

guest:
password = *

nobody:
password = *

lpd:
password = *

rootgwm:
password = wPjXpBf37o4ug
lastupdate = 1118773810

annie:
password = umnq7ZK2LqfcQ
lastupdate = 1120069466
flags = ADMCHG

harrison:
password = 2FZQSTgsnTP5g
lastupdate = 1120069844
flags = ADMCHG
```

11.8 Administering groups

A group is a collection of users who can share access permissions for protected resources. A group is usually known as a UNIX group.

Each group must have a name, a group identification (GID) number, and a list of user names that belong to that group. A GID identifies the group internally to the system.

The two types of groups to which a user can belong to are:

- ▶ Primary group
This specifies a group that the OS assigns to the files that are created by the user. Each user must belong to a primary group.
- ▶ Secondary groups
This specifies one or more additional groups to which a user belongs.

In AIX 5L, there are three types of groups:

- ▶ User group
User groups must be created for people who have to share files on the system, such as those who work in the same department or those who are working on the same project. In general, create as few user groups as possible.
- ▶ System administrator groups
System administrator groups correspond to the SYSTEM group. SYSTEM group membership allows an administrator to perform some system maintenance tasks without having to operate with root authority.
- ▶ System-defined groups
There are several system-defined groups. The STAFF group is the default group for all the nonadministrative users created in the system. You can change the default group by using the **chsec** command to edit the `/usr/lib/security/mkuser.default` file. The SECURITY group is a system-defined group having limited privileges for performing security administration.

In both the Solaris and AIX 5L systems, the **groups** command lists the groups that a user belongs to. A user can have only one primary group at a time. However, a user can temporarily change the user's primary group to any other group in which the user is a member with the **newgrp** command.

When adding a user account, assign a primary group to a user or accept the default, which is the staff group. The primary group must already exist (if it does not exist, specify the group by a GID number). Group information can be managed through local files or name service table and maps. In the case of local files, they are usually located in the `/etc` directory.

In Solaris, it is the `/etc/group` file. The fields in each line of the group file are separated by colons. Therefore, the structure of each line looks as follows:

```
group-name:group-password:gid:user-list
```


Following is an example of this:

```
adm: :4:root,adm,adm
```

Generally, use the command line or a text editor for group administration-related tasks in Solaris. In AIX 5L, you can use the **smitty groups** fast path. It opens the screen shown in Figure 11-8.

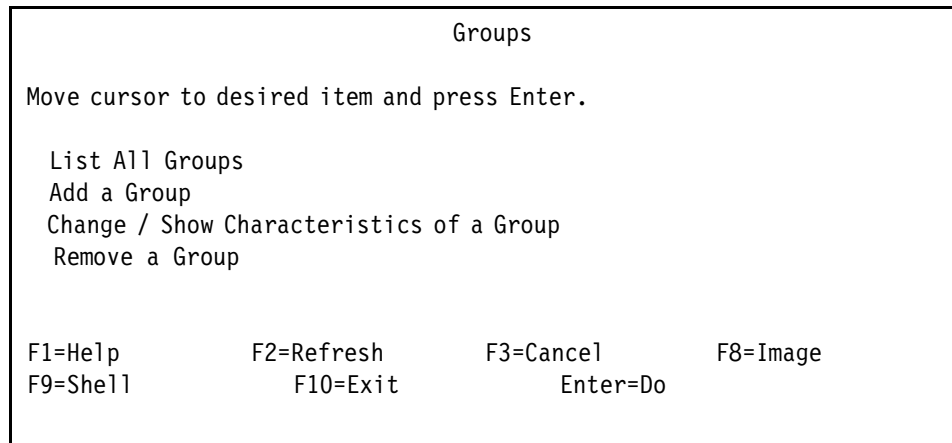


Figure 11-8 Smitty groups menu

In AIX 5L, there are two files related to groups administration, `/etc/group` and `/etc/security/group`.

11.8.1 Adding a group

The following section shows you how to add a group in Solaris and AIX 5L.

In Solaris

In Solaris, use the **groupadd** command. This command creates a new group definition on the system by adding the appropriate entry to the `/etc/group` file. The syntax is simple:

```
groupadd [ -g gid [ -o ] ] group
```

Following is an example of this:

```
groupadd -g 150 res_users
```

In AIX 5L

In AIX 5L, type **smitty mkgroup** at the command prompt to add a new group. The screen shown in Figure 11-9 is displayed. Enter all the necessary information and press Enter.

```

                                Add a Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry
Fields]
* Group NAME                                [res_users]
  ADMINISTRATIVE group?                    false
+
  Group ID                                [150]
#
  USER list                                [annie]
+
  ADMINISTRATOR list
[annie,harrison]      +
  Projects                                []
+

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset      F6=Command      F7=Edit      F8=Image
F9=Shell      F10=Exit      Enter=Do
```

Figure 11-9 Creating a new group

Alternatively, you can use the **mkgroup** command.

To create a new group account called **finance**, enter the command shown in Example 11-16. (Only the root user can issue this command.)

Example 11-16 Creating a new group account called finance

```
# mkgroup finance To create a new administrative group account called
payroll, type:
# mkgroup -a payroll
```

To create a new group account called **managers** and set yourself as the administrator, type the following:

```
# mkgroup -A managers
```

To create a new group account called managers and set the list of administrators to steve and mike, type:

```
# mkgroup adms=steve,mike managers
```

11.8.2 Modifying an existing group

This section shows you how to modify an existing group in Solaris or AIX 5L.

In Solaris

Use the **groupmod** command, which modifies the definition of the specified group by modifying the appropriate entry in the `/etc/group` file. The syntax is simple:

```
groupmod [ -g gid [ -o ] ] [ -n name ] group
```

Following is an example of this:

```
groupmod -g 271 -o res_users1
```

In AIX 5L

In AIX 5L, use **smitty chgroup** to access the screen shown in Figure 11-10 in order to modify an existing group. Select the name of the group you want to modify and press Enter.

```
Change Group Attributes

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Fields]
Group NAME                [staff]
Group ID                  [1]
#
ADMINISTRATIVE group?    false
+
USER list
[invscout,ipsec,sshd,r> +
ADMINISTRATOR list      []
+
Projects                  []
+

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command      F7=Edit       F8=Image
F9=Shell     F10=Exit        Enter=Do
```

Figure 11-10 Modifying group attributes

You can also use the **chgroup** command.

To add sam and carol to the finance group, which currently has only frank as a member, type:

```
chgroup users=sam,carol,frank finance
```

To remove frank from the finance group and retain sam and carol, and to remove the administrators of the finance group, type:

```
chgroup users=sam,carol adms= finance
```

In this example, two attribute values are changed. The name frank is omitted from the list of members, and the value for the adms attribute is left blank.

11.8.3 Deleting a group

This section describes how to delete a group in Solaris and AIX 5L.

In Solaris

Use the **groupdel** command. This deletes a group definition from the system. It deletes the appropriate entry from the `/etc/group` file. The synopsis of this command is:

```
groupdel group
```

In AIX 5L

In AIX 5L, use **smitty rmgroup**. In the screen that is displayed, select the name of the group you want to remove and press Enter.

Alternatively, you can use the **rmgroup** command:

```
rmgroup users
```

11.9 Checking for inconsistencies in passwords and group definitions

Both Solaris and AIX 5L OS contain tools that can be used to check a password file for any inconsistencies and to verify all the entries in the group file. The commands for performing these actions are **pwck** and **grpck** respectively.

The **pwck** command scans the password file and notes any inconsistencies. The checks include validation of the number of fields, login name, user ID, group ID, and whether the login directory and the program-to-use-as-shell exist.

In Solaris

The default password file checked is `/etc/passwd`. If the `-s` option is used with the **pwck** command, the protected password database is checked. The syntax for this command is:

```
/usr/sbin/pwck [file]
```

In AIX 5L, this command also scans the `/etc/security/passwd` file. The syntax for the **pwck** command is:

```
/usr/sbin/pwck
```

A sample output of the **pwck** command in AIX 5L is shown in Example 11-17.

Example 11-17 The pwck command

```
# pwck
3001-402 The user "imnadm" has an invalid password field in
/etc/passwd.
3001-414 The stanza for "imnadm" was not found in
/etc/security/passwd.
3001-402 The user "invscout" has an invalid password field in
/etc/passwd.
3001-414 The stanza for "invscout" was not found in
/etc/security/passwd.
3001-402 The user "lp" has an invalid password field in /etc/passwd.
3001-414 The stanza for "lp" was not found in /etc/security/passwd.
3001-421 The user "lp" does not have a stanza in /etc/security/user.
3001-402 The user "nuucp" has an invalid password field in
/etc/passwd.
3001-414 The stanza for "nuucp" was not found in /etc/security/passwd.
3001-402 The user "smith" has an invalid password field in
/etc/passwd.
3001-414 The stanza for "smith" was not found in /etc/security/passwd.
3001-402 The user "snapp" has an invalid password field in
/etc/passwd.
3001-414 The stanza for "snapp" was not found in /etc/security/passwd.
3001-402 The user "test" has an invalid password field in /etc/passwd.
3001-414 The stanza for "test" was not found in /etc/security/passwd.
```

The **grpck** command differs between Solaris and AIX 5L, but the general purpose is almost the same. In Solaris, **grpck** verifies all the entries in the group file. This verification includes checking the number of fields, group name, group ID, whether any login names exceed the limit specified in `NGROUPS_MAX`, and whether all the login names appear in the password file. The default group file is `/etc/group`.

The syntax of this command in Solaris is:

```
/usr/sbin/grpck [ file ]
```

Example 11-18 shows a sample output of the **grpck** command.

Example 11-18 A sample output of the grpck command

```
# grpck

rsgroup:103:annieh
      Duplicate group ID
```

In AIX 5L, the **grpck** command verifies the correctness of the group definitions in the user database files by checking the definitions for *all* the groups or for the groups specified by the Group parameter. If more than one group is specified, there must be a space between the groups.

The syntax of the **grpck** command in AIX 5L is:

```
grpck { -n | -p | -t | -y } { ALL | Group ... }
```

To verify that all the group members and administrators exist in the user database, and to have any errors reported, but not fixed, enter:

```
# grpck -n ALL
```

To verify that all the group members and administrators exist in the user database and to have errors fixed, but not reported, enter:

```
# grpck -p ALL
```

To verify the uniqueness of the group name and the group ID defined for the install group, use one of the following commands:

- ▶ # grpck -n install
- ▶ # grpck -t install
- ▶ # grpck -y install

The **grpck** command does *not* correct the group names and IDs. Therefore, the -n, -t, and -y flags report problems with group names and group IDs, but do *not* correct them.

11.10 Defining the system resource limits for users

In both Solaris and AIX 5L OS, you can use the **ulimit** command or the built-in shell functions. Basically, the syntax is the same (see `man ulimit` for the command syntax). The general purpose of using this command is to set the limitations on the system resources available to the current shell and its descendents.

In AIX 5L, the limits are defined in the `/etc/security/limits` file. The `/etc/security/limits` file is an ASCII file that contains stanzas specifying the process resource limits for each user. These limits are set by individual attributes within a stanza.

Each stanza is identified by a user name followed by a colon (`:`) and contains attributes in the `Attribute=Value` form. Each attribute is ended by a new line character, and each stanza is ended by an additional new line character. If you do not define an attribute for a user, the system applies the default values.

When you create a user with the `mkuser` command, the system adds a stanza for the user into the `/etc/security/limits` file. When the stanza is present, use the `chuser` command to change the user's limits. To display the current limits for a user, use the `lsuser` command. To remove users and their stanzas, use the `rmuser` command.

This `/etc/security/limits` file contains the default limits, as shown in Example 11-19.

Example 11-19 Default settings in `/etc/security/limits`

```
fsize = 2097151
core = 2097151
cpu = -1
data = 262144
rss = 65536
stack = 65536
nofiles = 2000
```

These values are used as default settings when a new user is added to the system. The values are set with the `mkuser` command when the user is added to the system, or changed with the `chuser` command. Limits are categorized as either soft or hard. With the `ulimit` command, you can change your soft limits up to the maximum limit set by the hard limits. You must, however, have root user authority to change the resource hard limits.

Many systems do not contain one or more of these limits. The limit for a specified resource is set when the Limit parameter is specified. The value of the Limit parameter can be a number in the unit specified with each resource. The value can also be unlimited. To set the specific ulimit to unlimited, use the value *unlimited*.

Note: Setting the default limits in the `/etc/security/limits` file sets system-wide limits, not just the limits taken on by a user when that user is created.

The current resource limit is printed when you omit the Limit parameter. The soft limit is printed unless you specify the -H flag. When you specify more than one resource, the limit name and the unit is printed before the value. If no option is provided, the -f flag is assumed.

In the following example, `ulimit` is used to set the file size limit to 51,200 bytes:

```
ulimit -f 100
```

11.11 Quick reference

Table 11-1 displays the tasks, commands, and the location of the files or information that is required to perform user management in Solaris and AIX 5L.

Table 11-1 Quick reference for user management

Task	Solaris	AIX 5L
Running multiple tasks in a GUI environment	admintool smc	Choose one of the following: <ul style="list-style-type: none"> ▶ <code>wsm</code> ▶ <code>smitty</code> ▶ The <code>smitty users</code> fast path
Adding users	<code>useradd</code>	<code>mkuser</code>
Removing users	<code>userdel</code>	<code>rmuser</code>
Displaying currently logged users	<ul style="list-style-type: none"> ▶ <code>who</code> or ▶ <code>w</code> 	<ul style="list-style-type: none"> ▶ <code>who</code> or ▶ <code>w</code>
Displaying users and their attributes	<ul style="list-style-type: none"> ▶ <code>listusers</code> ▶ <code>logins</code> 	<code>lsuser</code>
Password files	<ul style="list-style-type: none"> ▶ <code>/etc/passwd</code> and ▶ <code>/etc/shadow</code> 	<ul style="list-style-type: none"> ▶ <code>/etc/passwd</code> and ▶ <code>/etc/security/passwd</code>
Administering user password	<code>passwd</code>	<code>passwd</code> <code>chpasswd</code> or <code>pwdadm</code>
Modifying user account	<code>usermod</code>	<code>chuser</code>
System-wide environment file	<code>/etc/profile</code>	<ul style="list-style-type: none"> ▶ <code>/etc/profile</code> and ▶ <code>/etc/environment</code>
Profile template	<code>/etc/skel/.profile</code>	<code>/etc/security/.profile</code>

Task	Solaris	AIX 5L
Adding a group	groupadd	mkgroup
Group files	/etc/group	<ul style="list-style-type: none"> ▶ /etc/groupand ▶ /etc/security/group
Modifying a group	groupmod	chgroup
Deleting a group	groupdel	rmgroup
Checking password and group definition consistency	<ul style="list-style-type: none"> ▶ pwck and ▶ grpck 	<ul style="list-style-type: none"> ▶ pwck and ▶ grpck
Defining system resource limits for user	ulimit	<ul style="list-style-type: none"> ▶ /etc/security/limits or ▶ ulimit



Monitoring and performance

This chapter provides information about the commands available to monitor the utilization of, and display the statistics for the physical and logical resources of your system. Generally, many of the commands are the same on Solaris and AIX 5L, and many of the commands provide information about several resources. However, the output from the commands might differ significantly.

Certain tools are installed by default. With regard to other tools. It is recommended that you review the packages and install them if your installation requires the tools provided by the packages.

This chapter discusses the following topics:

- ▶ 12.1, “Monitoring memory” on page 360
- ▶ 12.1.1, “Solaris memory management” on page 360
- ▶ 12.1.2, “AIX 5L memory management” on page 360
- ▶ 12.5, “Monitoring the processors and the CPU” on page 368
- ▶ 12.6, “Physical media, software RAID, Logical Volume Manager, and file systems” on page 373
- ▶ 12.7, “Network” on page 375
- ▶ 12.8, “System and user processes” on page 376

12.1 Monitoring memory

Both Solaris and AIX 5L have different ways of monitoring specific resources. Some of them might appear to be contradicting each other if you do not understand what exactly is being monitored and how to interpret the output.

12.1.1 Solaris memory management

On Solaris, *swap* is the physical (disk) storage in slices on file systems, and is used for supplemental memory. Swap slices are used as virtual memory storage areas when the system does not have enough physical memory to handle the current processes.

Solaris' virtual memory system maps the physical copies of files on disk to virtual addresses in memory. Physical memory pages that contain the data for these mappings can be backed by regular files in the file system, or by swap space. If the memory is backed by swap space, it is referred to as *anonymous* memory because there is no identity assigned to the disk space that is backing the memory.

The Solaris environment uses the concept of *virtual swap space*, a layer between the anonymous memory pages and the physical storage or disk-backed swap space that actually back these pages. A system's virtual swap space is equal to the sum of all its physical (disk-backed) swap space plus a portion of the currently available physical memory¹.

On Solaris, swap is assigned to (and constrained by the size of) the tmpfs file system. It can be augmented by the use of swap files on other file systems.

12.1.2 AIX 5L memory management

AIX 5L uses the Virtual Memory Manager (VMM) to manage the allocation of real memory page frames and to resolve references by the program to virtual memory pages that are not currently in real memory. Therefore, on AIX 5L, "virtual memory" is the total amount of memory a process is using, both RAM and swap (Solaris term) or paging space (AIX 5L term).

¹ *Solaris Administration Guide: Basic Administration*, p.530

12.2 Virtual memory

The most frequently used command to monitor memory usage by a *process*, both resident and virtual, is **ps**, although, for a variety of reasons, it is probably *not* the most useful way to view *system* memory usage.

Following are the relevant columns of **ps** output:

▶ RSS

The resident set size of the process in kilobytes

▶ SZ

The total size of the process in virtual memory, including all the mapped files and devices, in pages (multiply SZ by the page size to get the byte size)

Solaris

Example 12-1 shows the Solaris **ps-e1y** output.

Example 12-1 The Solaris **ps -ely** output

```
# ps -ely | grep java
S  UID  PID  PPID  C  PRI  NI   RSS    SZ   WCHAN TTY        TIME  CMD
S    0 11366    1   0   70   30  66112 104368      ?  ?         4:00  java
```

The RSS of 66112 multiplied by eight (the page size on Solaris is 8192) = 528896 kilobytes

The SZ of 13046 multiplied by 8 = 104368 kilobytes.

To confirm this finding, on Solaris, use the following command:

```
# ps -eo pid,rss,vsz | grep 11366 (the Java process ID shown above)
11366 528896 104368 (units are kilobytes)
```

AIX 5L

Example 12-2 shows the AIX 5L **ps gv** output.

Example 12-2 The AIX 5L **ps gv** output

```
# ps gv
PID  TTY  STAT  TIME  PGIN  SIZE  RSS  LIM  TSIZ  TRS  %CPU  %MEM
COMMAND
14386  -   A  24:16  65  395416 395472 65536  39  56  0.1  14.0
java
```

To confirm these findings and convince yourself that SIZE and vsz represent the same thing, use the command shown in Example 12-3.

Example 12-3 Comparing SIZE and vsz output

```
> /usr/sysv/bin/ps -eo pid,rss,vsz,comm | grep 14386
PID  RSS  VSZ COMMAND
14386 395472 395416 java
```

12.2.1 The vmstat command

A much more useful tool for analyzing the use of (or requirement for) swap or paging space is **vmstat**. Output from **vmstat** on Solaris and AIX 5L *looks* similar, but the interpretation of the fields might vary. Consult the man pages on both the systems for a description of each of the fields. Example 12-4 and Example 12-6 show **vmstat** output from Solaris and AIX 5L respectively.

Example 12-4 shows the **vmstat** output from Solaris.

Example 12-4 The vmstat output from Solaris

```
# vmstat 2
kthr      memory          page        disk        faults      cpu
r  b  w   swap free re  mf pi po fr de sr s0 s1 s2 s3  in  sy  cs us sy id
0  0  0 5388904 3572472 1 10  0  0  0  0  0  0  0  0  230  64 133  0  1 99
0  0  0 5329432 3480648 0  4  0  0  0  0  0  0  0  0  0  257  43 201  0  0 100
0  0  0 5329432 3480648 16 24  0  0  0  0  0  0  0  0  254 138 196  0  0 99
0  0  0 5329432 3480648 0  0  0  0  0  0  0  0  0  0  353  36 244  0  9 91
0  0  0 5329368 3480584 16 24  0  0  0  0  0  0  0  0  513 139 338  0  1 99
0  0  0 5329368 3480584 0  0  0  0  0  0  0  0  0  0  388  31 257  0  1 99
0  0  0 5329368 3480584 0  0  0  0  0  0  0  0  0  0  258  39 196  0  0 100
0  0  0 5329368 3480584 16 24  0  0  0  0  0  0  0  0  263 137 193  0  0 100
[....]
```

In the swap column of the Solaris output, the numbers indicate the amount of swap space currently available, in this case, 5329432 kilobytes. That number is obtained from adding the available RAM to the amount of the available swap space. In this Solaris system example, the RAM is 4096 MB (4,194,204 KB).

Note: In this Solaris example, the amount of RAM is not included in the output of the **vmstat** command. However, it is included in the AIX 5L system.

Example 12-5 shows how much swap is defined.

Example 12-5 Swap size

```
# swap -l
swapfile          dev  swaplo blocks  free
/dev/dsk/c1t0d0s1 32,9   16 4194800 4194800
```

Blocks are 512 bytes. Thus, 4,194,800 blocks (2097400 kilobytes) is the amount of swap this machine has defined.

RAM (4194204 KB) + swap (2097400 KB) = 6291604 KB. By subtracting the swap figure shown in Example 12-5 from 6291604 KB, you can see how much total virtual memory is in use.

Example 12-6 shows the `vmstat` output from AIX 5L.

Example 12-6 The vmstat output from AIX 5L

```
# vmstat 2
```

System configuration: 1cpu=2 mem=1024MB ent=0.30

kthr		memory				page				faults				cpu				
r	b	avm	fre	re	pi	po	fr	sr	cy	in	sy	cs	us	sy	id	wa	pc	ec
2	0	117996	49393	0	0	0	0	0	0	3	256	438	0	1	99	0	0.01	3.0
1	0	117996	49393	0	0	0	0	0	0	5	229	512	0	1	99	0	0.01	2.9
2	0	117996	49393	0	0	0	0	0	0	6	210	463	0	1	99	0	0.01	2.7
2	0	117996	49393	0	0	0	0	0	0	5	210	480	0	1	99	0	0.01	2.5
2	0	117996	49393	0	0	0	0	0	0	2	210	467	0	1	99	0	0.01	2.5
2	0	117996	49393	0	0	0	0	0	0	2	210	461	0	1	99	0	0.01	2.5

The `avm` column of the AIX 5L output shows the number of *active virtual pages* (pages that have been accessed). Because the page size is 4096, multiply that column by four to determine the amount of active virtual memory in kilobytes. For more information, refer to the man pages and reference manuals for both the systems.

12.3 The `top` and `topas` commands

Another useful built-in command for monitoring system activity and performance on AIX 5L is `topas`. This is similar to the traditional `top` command available to Solaris admins as `SFWtop`. The `topas` command includes the same capabilities

along with a few more. For more information about SFWtop, refer to the following Web site:

<http://www.sunfreeware.com>

The Solaris Freeware **top** command shows load averages, high-level process status, CPU state, and memory data before it lists all the active processes with the associated resource usage.

Figure 12-1 shows the Solaris **top** command.

```

9.3.5.38 - PuTTY
load averages:  0.00,  0.00,  0.01
58 processes:  54 sleeping,  3 stopped,  1 on cpu
CPU states: 99.7% idle,  0.1% user,  0.2% kernel,  0.0% iowait,  0.0% swap
Memory: 4096M real, 2353M free, 1116M swap in use, 4164M swap free

  PID USERNAME  THR  PRI  NICE  SIZE  RES STATE   TIME  CPU COMMAND
  64  root         6   59   0 4032K 3288K sleep 66:55 0.09% picld
11366 root        33   29  10 101M  64M sleep 5:14 0.00% java
 303  root         1   59   0 2168K 1464K sleep 0:06 0.00% snmpdx
   1  root         1   59   0 1280K  752K sleep 0:05 0.00% init
 307  root         7   59   0 2592K 2112K sleep 0:04 0.00% mbiisa
22595 root         1   59   0 4488K 2688K sleep 0:02 0.00% sshd
6531  root         1   59   0 2216K 1272K cpu/O 0:00 0.00% top
5334  root         1   59   0 1312K 1064K stop  0:00 0.00% less
5304  root         1   59   0 1048K  840K stop  0:00 0.00% man
5333  root         1   59   0 1096K  824K stop  0:00 0.00% sh
11392 root         4   29  10 3496K 2752K sleep 0:00 0.00% remoteprovider
11404 root         4   29  10 3440K 2672K sleep 0:00 0.00% remoteprovider
11403 root         4   29  10 3408K 2624K sleep 0:00 0.00% remoteprovider
11396 root         4   29  10 3368K 2576K sleep 0:00 0.00% remoteprovider
11385 root         4   29  10 3416K 2560K sleep 0:00 0.00% remoteprovider
  
```

Figure 12-1 The Solaris **top** command

Example 12-7 shows the output from the AIX 5L **topas** command

Example 12-7 Output from the AIX 5L **topas** command

Topas Monitor for host:		example1	EVENTS/QUEUES		FILE/TTY	
Thu May 4 06:25:32 2006		Interval: 2	Cswitch	152	Readch	393
			Syscall	541	Writech	587
Kernel	0.1	#	Reads	1	Rawin	0
User	99.9	#####	Writes	1	Ttyout	281
Wait	0.0		Forks	0	Igets	0
Idle	0.0		Execs	0	Namei	0
			Runqueue	4.0	Dirblk	0
Network	KBPS	I-Pack	O-Pack	KB-In	KB-Out	Waitqueue
en4	0.4	1.0	1.0	0.1	0.4	0.0
en0	0.0	0.0	0.0	0.0	0.0	PAGING
lo0	0.0	0.0	0.0	0.0	0.0	MEMORY
			Faults	0	Real,MB	16383
			Steals	0	% Comp	63.2

Disk	Busy%	KBPS	TPS	KB-Read	KB-Writ	PgspIn	0	% Noncomp	12.0
hdisk2	0.0	0.0	0.0	0.0	0.0	PgspOut	0	% Client	2.5
hdisk7	0.0	0.0	0.0	0.0	0.0	PageIn	0		
hdisk5	0.0	0.0	0.0	0.0	0.0	PageOut	0	PAGING SPACE	
hdisk6	0.0	0.0	0.0	0.0	0.0	Sios	0	Size,MB	4096
hdisk4	0.0	0.0	0.0	0.0	0.0			% Used	0.7
hdisk0	0.0	0.0	0.0	0.0	0.0	NFS (calls/sec)		% Free	99.2
hdisk9	0.0	0.0	0.0	0.0	0.0	ServerV2	0		
hdisk3	0.0	0.0	0.0	0.0	0.0	ClientV2	0	Press:	
hdisk1	0.0	0.0	0.0	0.0	0.0	ServerV3	0	"h" for help	
						ClientV3	0	"q" to quit	

Name	PID	CPU%	PgSp	Owner
analysis	69786	25.2	2227.0	owner1
analysis	46208	25.2	2227.0	owner1
analysis	42386	25.2	2227.0	owner1
analysis	65014	24.8	2227.3	owner1
topas	55864	0.1	2.1	root
syncd	6492	0.0	0.6	root
lrud	1806	0.0	0.0	root
kbiod	7754	0.0	0.0	root
aioserve	18360	0.0	0.0	root
aioserve	32508	0.0	0.0	root
aioserve	20280	0.0	0.0	root

Topas Monitor for host: example2
Thu May 4 06:26:42 2006 Interval: 2

Kernel	User	Wait	Idle	EVENTS/QUEUES	FILE/TTY
23.2	76.2	0.0	0.6	Cswitch 19497	Readch 404
#####	#####			Syscall 611.2K	Writech 603
				Reads 1	Rawin 0
				Writes 1	Ttyout 284
				Forks 0	Igets 0
				Execs 0	Namei 0
				Runqueue 8.0	Dirblk 0
				Waitqueue 0.0	

Network	KBPS	I-Pack	O-Pack	KB-In	KB-Out	PAGING	MEMORY
en4	706.3	618.5	613.5	353.9	352.3	Faults 0	Real,MB 16383
en0	0.0	0.0	0.0	0.0	0.0	Steals 0	% Comp 35.0
lo0	0.0	0.0	0.0	0.0	0.0		

Disk	Busy%	KBPS	TPS	KB-Read	KB-Writ	PgspIn	0	% Noncomp	65.8
hdisk1	0.0	0.0	0.0	0.0	0.0	PgspOut	0	% Client	1.3
hdisk0	0.0	0.0	0.0	0.0	0.0	PageIn	0		
						PageOut	0	PAGING SPACE	
						Sios	0	Size,MB	4096
								% Used	0.7
						NFS (calls/sec)		% Free	99.2
						ServerV2	0		

Name	PID	CPU%	PgSp	Owner
mpp970	110116	12.5	295.7	owner2
mpp970	25342	12.5	2443.2	owner2
mpp970	72896	12.5	258.7	owner2

mpp970	45342	12.5	255.0	owner2	ClientV2	0	Press:
mpp970	60112	12.4	291.6	owner2	ServerV3	0	"h" for help
mpp970	92170	12.3	280.1	owner2	ClientV3	0	"q" to quit
mpp970	87976	12.3	285.9	owner2			
mpp970	88716	12.2	324.8	owner2			
syncd	7794	0.0	0.6	root			
nfsd	15222	0.0	0.0	root			
glbd	22192	0.0	0.7	root			
lrud	2838	0.0	0.0	root			
gil	4128	0.0	0.1	root			
rpc.lock	18576	0.0	0.0	root			
rpc.lock	73526	0.0	0.0	root			

12.4 AIX 5L paging and memory statistics

This section reproduces the paging statistics from *AIX 5L Performance Tools Handbook*, SG24-6039.

There are two parts to the paging statistics reported by **topas**. The first part is total paging statistics. This simply reports the total amount of paging available on the system and the percentages, free and used. The second part provides a breakdown of the paging activity. The reported items and their meanings are listed here:

- ▶ **Faults**
Reports the number of faults
- ▶ **Steals**
Reports the number of 4 KB pages of memory stolen by the VMM per second
- ▶ **Pgspln**
Reports the number of 4 KB pages read in from the paging space per second
- ▶ **PgspOut**
Reports the number of 4 KB pages written to the paging space per second
- ▶ **PageIn**
Reports the number of 4 KB pages read per second
- ▶ **PageOut**
Reports the number of 4 KB pages written per second
- ▶ **Sios**
Reports the number of input/output requests per second issued by the VMM

Memory statistics

Following are the memory statistics:

- ▶ Real
Shows the actual physical memory of the system in megabytes
- ▶ %Comp
Reports the real memory allocated to computational pages
- ▶ %Noncomp
Reports the real memory allocated to noncomputational pages
- ▶ %Client
Reports on the amount of memory that is currently used to cache remotely mounted files.

For more information about **topas**, refer to the **topas** man page. Table 12-1 shows the memory management tasks.

Table 12-1 Memory management tasks

Task	Solaris	AIX 5L
Memory Management		
Display how much RAM is on a machine	<ul style="list-style-type: none"> ▶ prtconf ▶ top 	<ul style="list-style-type: none"> ▶ bootinfo -r ▶ prtconf ▶ topas
Display how much RAM (RSS) a process is using	<ul style="list-style-type: none"> ▶ ps -ely ▶ ps -eo rss ▶ comm ▶ pmap -x pid 	<ul style="list-style-type: none"> ▶ ps ev ▶ /usr/sysv/bin/ps -ely ▶ svmon ▶ topas
Calculate the SIZE ^a of a running process	<ul style="list-style-type: none"> ▶ ps -ely ▶ ps -eo vsz ▶ comm ▶ ps -elf (w/SZ field multiplied by page size, generally 8192) 	<ul style="list-style-type: none"> ▶ /usr/sysv/bin/ps -ely ▶ ps -eo vsz ▶ comm ▶ svmon
Swap or Paging space		
Display how much swap has been defined	<ul style="list-style-type: none"> ▶ swap -l ▶ df -k ▶ top 	<ul style="list-style-type: none"> ▶ swap -l ▶ lsps -a ▶ topas

Task	Solaris	AIX 5L
Display how much total swap/paging space is in use	<ul style="list-style-type: none"> ▶ swap -l ▶ df -k ▶ top 	<ul style="list-style-type: none"> ▶ swap -l ▶ lsps -a ▶ topas ▶ svmon
Decrease swap/paging space	swap -r	<ul style="list-style-type: none"> ▶ rmpps ▶ chpps
Increase swap/paging space	<ul style="list-style-type: none"> ▶ mkfile <i>size filename</i> ▶ swap -a <i>filename</i> 	<ul style="list-style-type: none"> ▶ mkpps ▶ chpps
User shell resource limits		
Report user shell resource limits	ulimit -a	ulimit -a
Temporarily reset user shell resource limits	ulimit - <i>option newlimit</i>	ulimit - <i>option newlimit</i>
Permanently set user shell resource limits	vi /etc/system + reboot	vi /etc/security/limits (reboot not required)

a. SIZE is defined as the total size of the process in virtual memory, including RAM, swap, and all the mapped files and devices. Also called the “core image”.

12.5 Monitoring the processors and the CPU

Table 12-2 shows the differences in the CPU monitoring commands in Solaris and AIX 5L.

Table 12-2 CPU monitoring commands

Task	Solaris	AIX 5L
CPU monitoring and management		
Display how many CPUs the system has	<ul style="list-style-type: none"> ▶ prtconf ▶ psrinfo ▶ top 	<ul style="list-style-type: none"> ▶ prtconf ▶ topas ▶ lsdev -Cc processor
Display % of CPU usage by process	<ul style="list-style-type: none"> ▶ ps -eo pcpu ▶ comm 	<ul style="list-style-type: none"> ▶ ps -eo pcpu ▶ comm
Display CPU accumulated time by process	<ul style="list-style-type: none"> ▶ ps -eo time ▶ comm 	<ul style="list-style-type: none"> ▶ ps -eo time ▶ comm

Task	Solaris	AIX 5L
Display CPU utilization	<ul style="list-style-type: none"> ▶ sar ▶ cpustat ▶ top 	<ul style="list-style-type: none"> ▶ sar ▶ tprof ▶ topas ▶ netpmon
Review process queues	sar -q	sar -q
Display individual processor statistics in a multiprocessor system	mpstat	<ul style="list-style-type: none"> ▶ mpstat ▶ topas
Managing/Tuning I/O		
Display I/O statistics	<ul style="list-style-type: none"> ▶ iostat ▶ sar 	<ul style="list-style-type: none"> ▶ iostat ▶ topas ▶ filemon ▶ sar
Display or Manage I/O tuning parameters	vi /etc/system	<ul style="list-style-type: none"> ▶ ioo ▶ smit tuning
Load average for the past 1, 5, and 15 minutes	uptime	uptime
Display both CPU utilization and time per process	/usr/ucb/ps -agux	ps agux (not -agux)
Kernel attributes		
Display kernel parameters	<ul style="list-style-type: none"> ▶ sysdef ▶ nnd ▶ kstat 	<ul style="list-style-type: none"> ▶ lsattr ▶ vmo ▶ no ▶ smit tuning
Tune kernel parameters	<ul style="list-style-type: none"> ▶ vi /etc/system ▶ reboot 	<ul style="list-style-type: none"> ▶ vmo (formerly vmtune) ▶ smit tuning ▶ /etc/tunables/nextboot

12.5.1 Using sar to monitor CPU

The **sar** command reports the use of CPU during an interval. It can also collect data into a file for future examination and extraction.

To collect information into a file in order to provide historical data, run the following:

```
sar -o filename <interval> <# of intervals> >/dev/null
```

To extract the information of the file, use the following command:

```
sar -u -f filename -s <starting time> -e <ending time>
```

Example 12-8 shows an **sar** execution within an interval.

Example 12-8 Interval sar execution

```
# sar -u 10 3
AIX i19962c 1 5 000321944C00 05/01/02
17:17:39      %usr      %sys      %wio      %idle
17:17:49          0          1          0          99
17:17:59          0          0          0          100
17:18:09          0          0          0          100
Average          0          0          0          100
```

The syntax for AIX 5L and Solaris 9 is the same; the parameters on the example indicate:

```
-u Collect CPU usage data
10 Interval in seconds
 3 Number of intervals
```

The columns of the output provide the following information:

%usr Reports the percentage of time the CPU spent at the user level.

%sys Reports the percentage of time the CPU spent in execution of system functions.

%wio Reports the percentage of time the CPU was idle waiting for I/O to complete.

%idle Reports the percentage of time the CPU was idle, with no outstanding for I/O requests.

12.5.2 Using filemon to monitor CPU

On AIX 5L, the **filemon** command monitors the performance of the file system, and reports the I/O activity on behalf of the logical files, virtual memory segments, logical volumes, and physical volumes.

Example 12-9 shows the AIX 5L **filemon**.

Example 12-9 An AIX 5L filemon example

```
# filemon -O lf
```

Enter the "trcstop" command to complete filemon processing

```
Mon May 1 10:49:51 2006
```

```
System: AIX cdcaix12 Node: 5 Machine: 000C9A9F4C00
```

```
# find / -type f -exec cat > /dev/null 1>/dev/null 2>&1
      [just to create disk traffic and make the output interesting]
```

```
# trcstop
Cpu utilization: 60.7%
[filemon: Reporting started]
Most Active Files
```

#MBs	#opns	#rds	#wrs	file	volume:inode
2595.0	5	0	692641	null	
93.2	1	23868	0	setup.exe	/dev/hd2:10801
83.9	1	21485	0	wsmlinuxclient.exe	/dev/hd2:10802
44.3	1	11333	0	ibm-win32-jre.exe	/dev/hd2:10793
39.0	1	9982	0	setupAC.jar	/dev/hd3:6155
36.9	148	9457	0	unix	/dev/hd2:2467
36.9	1	9449	0	ibm-linux-jre.i386.rpm	/dev/hd2:10794
36.3	1	9281	0	libdb2e.a	/dev/hd2:198752
30.6	1	7821	0	libdb2e.a	/dev/hd2:194877
25.1	1	6417	0	libdb2.a	/dev/hd2:198718
23.1	1	5904	0	jfs.10.5.198718	/dev/hd2:198718
22.9	1	5875	0	libjitc_g.a	/dev/hd2:34980
22.4	1	5744	0	WebSphereConfig_backup__1143576677671	/dev/hd3:43010
15.9	1	4074	0	jfs.10.5.198718	/dev/hd2:198718
14.6	1	3727	0	db2o.o	/dev/hd2:198717
14.0	1	3572	0	libjvm_g.a	/dev/hd2:34961
13.2	1	3387	0	libite.a	/dev/hd2:18572
13.1	1	3347	0	DsmSnapin_PA_1_1_CH.ear	/dev/fs1v01:143491
11.8	1	3028	0	dsmsched.log	/dev/hd3:57
11.2	1	2872	0	invscoutClient_VPD_Survey	/dev/hd10opt:4098

Detailed File Stats

```
FILE: /dev/null
opens:                5
total bytes xfrd:    2721034165
writes:              692641 (0 errs)
```

Detailed File Stats

```
FILE: /dev/null
opens:                5
total bytes xfrd:    2721034165
writes:              692641 (0 errs)
  write sizes (bytes):  avg 3928.5 min      1 max      4096 sdev   720.5
```

```
write times (msec):  avg  0.234 min  0.002 max 26827.222 sdev  49.265

FILE: /usr/websm/pc_client/setup.exe  volume: /dev/hd2 (/usr)  inode: 10801
opens: 1
total bytes xfrd: 97763328
reads: 23868 (0 errs)
  read sizes (bytes):  avg 4096.0 min 4096 max 4096 sdev 0.0
  read times (msec):  avg 0.104 min 0.002 max 14.461 sdev 0.453

FILE: /usr/websm/pc_client/wsmlinuxclient.exe  volume: /dev/hd2 (/usr)  inode: 10802
opens: 1
total bytes xfrd: 88002560
reads: 21485 (0 errs)
  read sizes (bytes):  avg 4096.0 min 4096 max 4096 sdev 0.0
  read times (msec):  avg 0.084 min 0.002 max 8.061 sdev 0.324
[.....]
```

12.5.3 The procmon tool

Use this tool on systems running AIX 5L V5.3 or later. It allows you to view and manage the processes running on a system. It has a graphical interface and displays a table of process metrics that you can sort on the different fields that are provided. By default, the procmon tool displays the following information:

- ▶ How long a process has been running
- ▶ How much CPU resources the processes are using
- ▶ Whether the processes are being penalized by the system
- ▶ How much memory the processes are using
- ▶ How much I/O a process is performing
- ▶ The priority and nice values of a process
- ▶ The person who created a particular process

For more information about this tool, see the procmon section of the Performance Tools Guide and Reference in the System p AIX 5L Collaboration Center available on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

12.6 Physical media, software RAID, Logical Volume Manager, and file systems

Physical media must be partitioned and formatted with a file system unless it is used as a raw device. For this reason, this section differentiates between the physical media and the file systems. The commands that are used to monitor disk partitions, and are analogous with Solaris' slices are listed as physical media monitoring commands.

Software Redundant Array of Independent Disks (RAID) and Logical Volume Manager (LVM) provide complementary functions. Neither does LVM replace RAID, nor does software RAID replace LVM.

12.6.1 Physical media monitoring

Table 12-3 displays the physical media monitoring commands.

Table 12-3 Physical media monitoring commands

Task	Solaris	AIX 5L
Display, collect, or store system activity status	<code>sar</code>	<code>sar</code>
Display I/O statistics	<code>iostat</code>	<code>iostat</code>

12.6.2 Monitoring logical volumes and logical volume groups

Both Solaris and AIX 5L have Volume Managers, the Solaris Volume Manager and the AIX 5L Logical Volume Manager (LVM). Solaris Volume Manager (prior to Solaris 9, this tool was called Solstice Disk Suite) is discussed in Chapter 4, "Disks and file systems" on page 91.

Both the Solaris Volume Manager and the AIX 5L LVM manage your system's storage requirements, including creating, modifying, and using RAID 0 (concatenation and stripe) volumes, RAID 1 (mirror) volumes, and RAID 5 volumes, in addition to soft partitions and transactional log devices.

For more information about the Solaris Volume Manager, refer to the Solaris Volume Manager Administration Guide:

<http://docs.sun.com/app/docs/doc/817-2530>

The features of the LVM on AIX 5L simplifies the tasks of the system administrator. You can add disk space dynamically, mirror the information, spread the logical volumes to increase performance (RAID 0), relocate a logical volume and its content online, and move a group of disks from one system to another without losing data.

12.6.3 Software Redundant Array of Independent Disks

Table 12-4 illustrates software RAID monitoring commands.

Table 12-4 Software RAID monitoring commands

Task	Solaris	AIX 5L
Display status information for software RAID devices	metastat	<ul style="list-style-type: none"> ▶ smit lvm ▶ lsvg ▶ lslv ▶ lspv
Manage and monitor software RAID devices	<ul style="list-style-type: none"> ▶ metastat ▶ iostat 	<ul style="list-style-type: none"> ▶ smit lvm ▶ lvmstat ▶ iostat

12.6.4 Logical volume monitoring

Table 12-5 illustrates the logical volume monitoring commands.

Table 12-5 Logical volume monitoring commands

Task	Solaris	AIX 5L
Display logical volume attributes	metastat vxprint (Veritas)	<ul style="list-style-type: none"> ▶ lslv ▶ [wsm, smit] [lv,lslv] ▶ lsvg
Display physical volume attributes	format	<ul style="list-style-type: none"> ▶ lspv ▶ lslv -p <i>physical-volume</i>
Display volume group attributes	metastat	<ul style="list-style-type: none"> ▶ lsvg ▶ [wsm, smit] [vg,lsvg]
Display lvm i/o statistics	iostat vxstat (Veritas)	lvmstat

12.6.5 File systems

This chapter differentiates the file systems from the physical devices because a file system can extend beyond a single device. Examples of file systems that extend beyond a single device are hardware and software RAID drives and logical volumes.

Table 12-6 shows the file system monitoring commands.

Table 12-6 File system monitoring commands

Task	Solaris	AIX 5L
Display file system disk space usage information	df	df
Display individual file disk space usage	du	du
Display quota data	repquota	repquota
Display I/O statistics	iostat	► iostat ► lvmstat
Report disk operations/second	vmstat	vmstat

12.7 Network

Table 12-7 illustrates some network activity monitoring commands. Additional network performance information can be found in `/proc/slabinfo`.

Table 12-7 Network monitoring commands

Task	Solaris	AIX 5L
Graphical network protocol analyzer	ethereal	ethereal
Configure network device	ifconfig	ifconfig
Monitor traffic load	netstat	► netstat ► topas
Display network statistics, routing information, connections, and so on	netstat	netstat
Display Network File System (NFS) statistics	nfsstat	nfsstat
Send Internet Control Message Protocol (ICMP) echo request packets to network host	ping	ping
Display network packets	snoop	iptrace

Task	Solaris	AIX 5L
Test network connectivity using an User Datagram Protocol (UDP)	spray	spray
Dump and analyze network traffic	<ul style="list-style-type: none"> ▶ snoop ▶ tcpdump 	tcpdump

12.8 System and user processes

On both Solaris and AIX 5L, each process has a directory containing its state data. The directory is `/proc/nnnn`, where `nnnn` is the process ID (PID) number.

Table 12-8 Process monitoring commands

Task	Solaris	AIX 5L
Display interprocess communication facilities status	ipcs	ipcs
Display shared library dependencies	ldd	<ul style="list-style-type: none"> ▶ ldd ▶ dump -H executable
Display open files	lsof	lsof
Display dynamic library calls	ldd	dump
Display process status	ps	ps
Display process interdependencies in a tree format	pstree	proctree
Display, collect, or store system activity status	sar	sar
Traces system calls and signals	truss	truss
Display top CPU user for running processes and CPU and memory statistics	top	topas
Display virtual memory statistics	vmstat	vmstat



Security and hardening

This chapter describes the security resources in a migration scenario. It provides a basic overview of some of the security tools or functions that are available for AIX 5L when migrating from Solaris. However, it is not a complete guide to AIX 5L security. For more information, see the AIX 5L Security Guide in the System p AIX 5L Collaboration Center available on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

This chapter discusses the following topics:

- ▶ 13.1, “Hardware security” on page 378
- ▶ 13.2, “Additional security features” on page 381
- ▶ 13.3, “User and password policy” on page 382
- ▶ 13.4, “Securing the File Transfer Protocol” on page 383
- ▶ 13.6, “Access control list” on page 386
- ▶ 13.7, “Auditing” on page 389
- ▶ 13.8, “Light Directory Access Protocol” on page 390
- ▶ 13.9, “Secure Shell” on page 391
- ▶ 13.10, “Transmission Control Protocol Wrapper” on page 391
- ▶ 13.11, “Network File System” on page 393
- ▶ 13.12, “Sudo” on page 393
- ▶ 13.13, “Kerberos” on page 394
- ▶ 13.14, “IP Security Architecture and Internet Key Exchange” on page 395
- ▶ 13.15, “Pluggable Authentication Module and Loadable Authentication Module” on page 396

13.1 Hardware security

Solaris and AIX 5L servers provide mechanisms for hardware protection. The concepts about hardware protection that are discussed in this chapter are related to two layers before the operating system (OS).

The first layer is related to new servers, and is called System Controller in Solaris, and Hardware Management Console (HMC) in AIX 5L. This layer is a separated infrastructure with server management capability, for example, rebooting or obtaining an OS console. System Controllers on enterprise class Sun servers or IBM HMC can be responsible for one or more servers that might have multiple domains or logical partitions.

The second layer is directly related to a specific server, and is called OpenBoot™ PROM (OBP) in Solaris (SPARC) and Hardware Security features in AIX 5L.

13.1.1 System Controllers on Sun servers

There are different System Controllers for the Sun servers. The basis of security is related to network connections and encrypted protocols. However, it is recommended that you refer to specific documentation about your hardware. On enterprise class Sun servers, the System Controller is run with the Solaris OS.

For more information about securing System Controllers, refer to the following Web site:

<http://www.sun.com/documentation/>

13.1.2 OpenBoot PROM on Sun servers

As with System Controllers, this layer too is related to server models. Example 13-1 shows the security modes available on OBP. The command is executed in a Solaris prompt.

Example 13-1 OBP security modes

```
# eeprom |grep -i security
security-mode=none
security-password: data not available.
security-#badlogins=0
```

Another security feature that is available in Sun SPARC servers is disabling keyboard abort. SPARC-based systems can drop to the OBP level when the Solaris operating environment (OE) is running, using the keyboard abort

sequence (Stop+A keys combination). This can be disabled in Solaris V2.6 and newer OEs. This feature might be useful in uncontrolled laboratory environments to prevent users from bringing the systems down. If the OBP security mode is full or the command is enabled, the EEPROM settings cannot be altered without a password.

To disable the keyboard abort sequence, change the line “#KEYBOARD_ABORT=enable” in the /etc/default/kbd file to “KEYBOARD_ABORT=disable”.

If the system hangs or becomes unusable, it must be powered off to be reset. It will no longer be possible to create a crash dump from the OBP level on a running system for analysis.

13.1.3 Hardware Management Console on IBM servers

HMC for IBM servers are based on a Linux solution, but with specific security features such as restricted shell.

The security issues are automatically enabled on HMC installation, and new implementations or corrections are available on the patches distributed in the following link:

<http://www14.software.ibm.com/webapp/set2/sas/f/hmc/home.html>

13.1.4 IBM System p hardware security features

The IBM eServer pSeries provides the following hardware (including firmware) security features:

- ▶ Cover lock key
- ▶ Power-on password
- ▶ Privileged-access password
- ▶ Unattended start mode

Cover lock key

This security feature prevents the cover from being removed. You require a physical key to access the hardware components that are inside.

Power-on password

This password helps protect the information stored in your system. Every time you power on or reset your system, this password is required to continue the operation. When the system is powered on, it checks whether a power-on password is present. If it is present, and the “unattended start mode” is not set, it means that the machine's owner does not want the system to be used unless the

power-on password is provided. The system prompts for the power-on password. The user is given three attempts to enter the correct password. If the user fails to provide the correct password, the system goes into a “hung” state and must be powered off before continuing. This password helps to protect the information stored in the system.

Unattended start mode

To use this mode, a power-on password must be specified earlier. If an unattended start mode is enabled, the system boots from the defined boot device without the user having to enter the power-on password. Although the system can be booted without entering the power-on password, the keyboard controller is programmed to lock up until the power-on password is provided. This mode is ideal for servers that run unattended. After an electrical power failure, for example, the OS is rebooted without waiting for a user to enter the power-on password.

Privileged-access password

This password protects against the unauthorized starting of System Management Services, which is a built-in firmware that provides system management tools, including the setting and resetting of the power-on password and the privileged-access password. When the user presses one of the keys to access the System Management Services, the system checks to see if a privileged access password exists. If it does exist, the user is prompted to enter the privileged access password. The user is given three attempts to provide the correct password. If the user fails to do so, the system goes into a “hung” state and must be powered off before continuing.

If you set both the power-on and privileged-access passwords, only the privileged-access password is required to start the System Management Services. Information about password setting and the password required to start AIX 5L or the System Management Services are summarized in Table 13-1.

Table 13-1 System Management Services

Password setting	Starting AIX 5L	Starting System Management Services
None	Not required	Not required
Power-on	Power-on	Power-on
Privileged-access	Not required	Privileged-access
Both power-on and privileged-access	Power-on	Privileged-access

If you do not have a machine's password, the only way to get access to the system is by removing the system's battery. You must be aware that this procedure will erase all the firmware configuration data maintained in the nonvolatile random access memory (NVRAM), such as the error log and any configured IP addresses. In such a situation, you require the cover lock key to open the cover.

Note: Power-on passwords apply only to PCI-based RS/6000 machines. The implementation of these hardware security features are slightly different between the IBM eServer pSeries (RS/6000) models. For more precise information, refer to the User's Guide provided with your system.

It is recommended that both the power-on and privileged-access passwords are set, and the cover lock key is removed from the system. The cover lock key must be available when it is required, for example, during software or hardware maintenance. Depending on your system application, you might not have to use the power-on password. Even in such a situation, a privileged-access password must be set. Otherwise, anyone can start the System Management Services and bypass all the security points and access any file on the disks.

For more information about securing Logical Partitions on IBM eServer pSeries, refer to the following Web site:

http://www-03.ibm.com/servers/eserver/pseries/hardware/whitepapers/lpar_security.html

13.2 Additional security features

Additional security features are available for increasing the security in an AIX 5L environment during the installation process. To carry out an installation on a machine on which installation has already been carried out, use the preservation installation method.

Trusted Computing Base

The system administrator must determine how much trust can be given to a particular program. This includes considering the value of the information resources on the system when deciding how much trust is required for a program to be installed with privilege. The Trusted Computing Base (TCB) is a part of the system that is responsible for enforcing system-wide information security policies. By installing and using the TCB, you can define user access to the

trusted communication path, which allows secure communication between the users and the TCB. TCB features can only be enabled when the OS is installed. TCB allows you to access the trusted shell, trusted processes, and the secure attention key (SAK).

Controlled Access Protection Profile and Evaluation Assurance Level 4+

Beginning AIX 5L V5.2, system administrators can install a system with the Controlled Access Protection Profile (CAPP) and Evaluation Assurance Level 4+ (EAL4+) option during a base operating system (BOS) installation. A system with this option has restrictions on the software that is installed during BOS installation. Network access is also restricted.

For more information about how to work with TCB, CAPP, and EAL4+, refer to the AIX 5L V5.3 manual.

13.3 User and password policy

On Solaris 9, information about users is provided in the following files:

- ▶ `/etc/passwd` contains basic user information
- ▶ `/etc/shadow` contains the password and security parameters
- ▶ `/etc/default/passwd` contains the default security values

To manage these administrator work editing files, use the `admintool`, the Solaris Management Console, or the command line.

On AIX 5L servers, the files for basic user security are as follows:

- ▶ `/etc/passwd` contains basic user information (similar to Solaris)
- ▶ `/etc/security/passwd` contains password file
- ▶ `/etc/security/login.cfg` contains login rules file
- ▶ `/etc/security/user` contains users' rules file
- ▶ `/etc/security/limits` contains users' limits file

The `/etc/security/login.cfg`, `/etc/security/user`, and `/etc/security/limits` files contain all the information relating to the configuration options.

Information about security can be changed by using the command line, editing the files, the Web-based System Manager, or SMIT.

Figure 13-1 shows the screen that is displayed on using the `smit security` fast path.

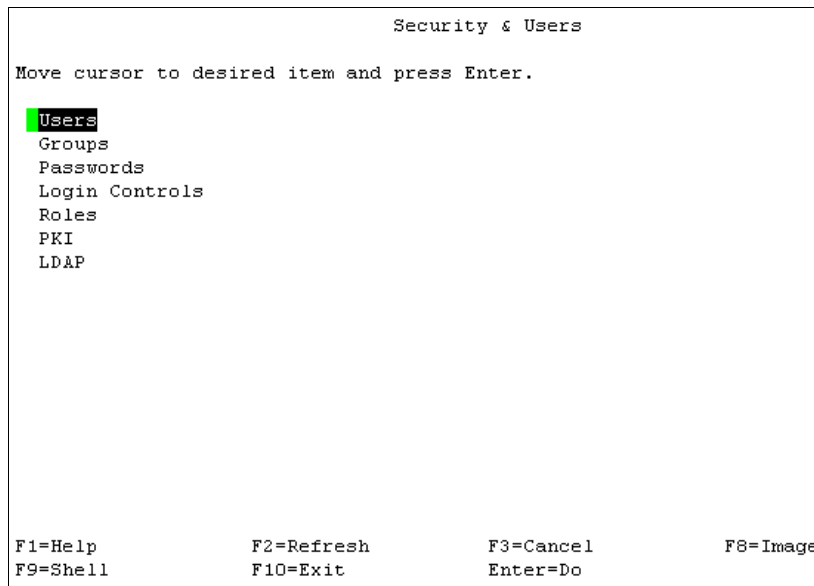


Figure 13-1 Using `smit security`

13.4 Securing the File Transfer Protocol

Table 13-2 compares security on File Transfer Protocol (FTP) on Solaris and AIX 5L.

Table 13-2 Comparing security on FTP

Task	Solaris	AIX 5L
List of users not allowed to use FTP	<ul style="list-style-type: none"> ▶ /etc/ftpusers or ▶ /etc/ftpd/ftpusers 	/etc/ftpusers
Pluggable Authentication Modules (PAM) authentication	/etc/pam.conf	/etc/pam.conf
Mean configuration file	/etc/ftpd/ftpass	/etc/ftpass.ctl

Anonymous File Transfer Protocol

If you work with an anonymous FTP in a Solaris environment, and you intend to migrate this configuration to an AIX 5L server, refer to the script available after AIX 5L installation on `/usr/samples/tcpip/anon.ftp`.

Changing the File Transfer Protocol server

Solaris and AIX 5L have open source FTP servers available for installation. Each one has different security features. In the AIX 5L toolbox CD-ROM, there are `ncftpd`, `proftpd`, and `wu-ftpd` RPM packages. If you work with one of these FTP servers on Solaris and intend to use the same on AIX 5L, perform installation through RPM.

13.5 Removing unused services

On all UNIX environments, it is a good practice to disable the services that you are not using. To check the opened ports, use the same command on Solaris and AIX 5L, as shown in Example 13-2.

Example 13-2 Checking the opened ports

```
# netstat -a |grep LISTEN
tcp4      0      0 *.daytime          *.*          LISTEN
tcp       0      0 *.ftp              *.*          LISTEN
tcp       0      0 *.telnet           *.*          LISTEN
tcp4      0      0 *.smtp             *.*          LISTEN
tcp4      0      0 *.time             *.*          LISTEN
tcp4      0      0 *.sunrpc           *.*          LISTEN
tcp4      0      0 *.smux             *.*          LISTEN
tcp       0      0 *.exec             *.*          LISTEN
tcp       0      0 *.login            *.*          LISTEN
tcp       0      0 *.shell            *.*          LISTEN
tcp4      0      0 *.rmt              *.*          LISTEN
tcp4      0      0 *.writesrv         *.*          LISTEN
tcp4      0      0 *.filenet-        *.*          LISTEN
```

The services are basically disabled in two places in Solaris and AIX 5L:

► `/etc/inetd.conf`

This file has a similar format on both the OS. To disable the service, remove the line or insert a “#” at the beginning of the line of the service to be removed. After making changes to the file, refresh the `inetd` daemon. Example 13-3 and Example 13-4 illustrate how to refresh `inetd` on Solaris and AIX 5L respectively.

Example 13-3 shows how to refresh inetd on Solaris.

Example 13-3 Refreshing inetd on Solaris

```
# ps -ef |grep inetd
  root   146      1  0   Apr 05 ?           0:00 /usr/sbin/inetd -s
  root 11579 11573  0 10:51:35 pts/3    0:00 grep inetd
# kill -HUP 146
```

Example 13-4 shows how to refresh inetd on AIX 5L.

Example 13-4 Refreshing inetd on AIX 5L

```
# refresh -s inetd
0513-095 The request for subsystem refresh was completed successfully.
#
```

► boot scripts

The boot process is different in Solaris and in AIX 5L. In Solaris, you have to change the first character of the start scripts from “S” to any other character. In AIX 5L, it is slightly different, because you have to check in two places:

– /etc/rc.* files

This is the main file that contains the services to be started is rc.tcpip.

To disable a service, remove or insert “#” at the beginning of the line of the service to be removed.

– /etc/rc.d/rc.d directory

As with Solaris, change the first character of the start script.

To check all the scripts that are being started, see Example 13-5 (in this case, only one service is started on rc2.d).

Example 13-5 Listing the services started on /etc/rc.d

```
# cd /etc
# ls -lR rc.d
total 8
drwxr-xr-x  2 root    system      256 Jan 10 11:23 init.d
-r-xr--r--  1 root    system     1586 Jun 21 2004 rc
drwxr-xr-x  2 root    system      256 May 10 10:44 rc2.d
drwxr-xr-x  2 root    system      256 Jan 10 11:23 rc3.d
drwxr-xr-x  2 root    system      256 Jan 10 11:23 rc4.d
drwxr-xr-x  2 root    system      256 Jan 10 11:23 rc5.d
drwxr-xr-x  2 root    system      256 Jan 10 11:23 rc6.d
drwxr-xr-x  2 root    system      256 Jan 10 11:23 rc7.d
drwxr-xr-x  2 root    system      256 Jan 10 11:23 rc8.d
```

```

drwxr-xr-x  2 root    system      256 Jan 10 11:23 rc9.d
rc.d/init.d:
total 0

rc.d/rc2.d:
total 16
-r-xr-xr-x  1 root    system      307 May 10 10:44 Ksshd
-r-xr-xr-x  1 root    system      308 May 10 10:44 Ssshd

rc.d/rc3.d:
total 0

rc.d/rc4.d:
total 0

rc.d/rc5.d:
total 0

rc.d/rc6.d:
total 0

rc.d/rc7.d:
total 0

rc.d/rc8.d:
total 0

rc.d/rc9.d:
total 0
#

```

These changes take effect at the next boot. For information about how to stop the service manually, refer to 9.3, “Starting and stopping the system services” on page 250.

13.6 Access control list

On Solaris 9 and AIX 5L, access control consists of protected information resources that specify who can be granted access to such resources. The owner of an information resource can grant other users read or write access rights for that resource.

An access control list (ACL) increases the quality of file access controls by adding extended permissions that modify the base permissions assigned to individuals and groups. With extended permissions, you can permit or deny file access to specific individuals or groups without changing the base permissions.

Table 13-3 shows the commands used to manage ACL in the Solaris 9 and the AIX 5L environments.

Table 13-3 Managing ACL

Task	Solaris	AIX 5L
Display the access control information of a file	getfacl	aclget
Edit the access control information of a file	N/A	acledit
Set the access control information of a file	setfacl	aclput

Note: The EDITOR environment variable must be specified with a complete path name, for example, export EDITOR=/usr/bin/vi. Otherwise, the **acledit** command fails.

In AIX 5L, an ACL of a file is organized in three layers:

- ▶ Base permissions
- ▶ Attributes
- ▶ Extended permissions

Base permissions

Base permissions are the traditional file access modes assigned to the file owner, file group, and other users. The access modes are read (r), write (w), and execute/search (x).

In an ACL, base permissions are in the following format, with the Mode parameter expressed as rwx, with a hyphen (-) replacing each unspecified permission.

Attributes

Three attributes can be added to an ACL:

- ▶ `setuid` (SUID)
Set-user-ID mode bit. This attribute sets the effective and saved user IDs of the process to the owner ID of the file on execution.
- ▶ `setgid` (SGID)
Set-group-ID mode bit. This attribute sets the effective and saved group IDs of the process to the group ID of the file on execution.
- ▶ `savetext` (SVTX)
Saves the text in a text file format.

Extended permissions

Extended permissions allow the owner of a file to define access to that file more precisely. Extended permissions modify the base file permissions (owner, group, and others) by permitting, denying, or specifying access modes for specific individuals, groups, or user and group combinations. Extended permissions are modified through the use of key words.

- ▶ `permit`
Grants the user or group specified access to a file
- ▶ `deny`
Restricts the user or group from using specified access to a file
- ▶ `specify`
Precisely defines the file access for the user or group

Example 13-6 shows how to check the ACL in AIX 5L.

Example 13-6 Checking the ACL in AIX 5L

```
# aclget /tmp/test
*
* ACL_type  AIXC
*
attributes:
base permissions
  owner(root): rw-
  group(system): r--
  others: r--
extended permissions
  disabled
```

13.7 Auditing

The auditing system is intended to record security-related information and to alert you about potential or actual violations of system security policy.

In Solaris 9, the auditing level is a part of the SolarisOE SunSHIELD™ Basic Security Module (BSM). The audit configuration is based on an analysis of the editable files available in the `/etc/security` directory. The `bsmconv` command is used to enable or disable the BSM in Solaris.

In the AIX 5L OS, the files used for audit configuration are located in `/etc/security/audit`.

The `audit` command controls system auditing through several key words. One key word must be included each time the command is given.

Following are the `audit` command key words.

- ▶ `start`
Starts the audit subsystem
- ▶ `shutdown`
Terminates the collection of audit records and resets the configuration information by removing the definition of classes from the kernel tables
- ▶ `off`
Suspends the auditing system, but leaves the configuration valid. Data collection pauses until the `audit on` command is given.
- ▶ `on`
Restarts the auditing system after a suspension if the system is properly configured, for example, if the `audit start` command was used initially and the configuration is still valid. If auditing is already started when the command is given, only bin data collection can be changed.
- ▶ `query`
Displays the current status of the audit subsystem

The auditing system follows the instructions established in the following configuration files:

- ▶ `/etc/security/audit/config`
- ▶ `/etc/security/audit/events`
- ▶ `/etc/security/audit/objects`
- ▶ `/etc/security/audit/bincmds`
- ▶ `/etc/security/audit/streamcmds`

Example 13-7 shows how to get the audit status.

Example 13-7 Audit query

```
# audit query
auditing off
bin processing off
audit events:
    none

audit objects:
    none
```

For complete information about how audit works on AIX 5L, refer to *Accounting and Auditing on AIX 5L*, SG24-6396, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246396.pdf>

Also refer to the auditing sections of AIX 5L Security Guide in the System p AIX 5L Collaboration Center available on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

13.8 Light Directory Access Protocol

The Light Directory Access Protocol (LDAP) defines a standard method for accessing and updating information in a directory (a database) either locally or remotely in a client/server model. The protocol is optimized for reading, browsing, and searching directories, and was originally developed as a lightweight front end to the X.500 Directory Access Protocol.

The LDAP method is used by a cluster of hosts to allow centralized security authentication and to access user and group information. This functionality is intended for use in a clustering environment in order to keep the authentication, users, and group information common across the cluster. The objects in LDAP are stored in an hierarchical structure. This is known as a Directory Information Tree (DIT). A good directory starts with the structural design of the DIT. The DIT must be designed carefully before implementing LDAP as a means of authentication.

In Solaris and AIX 5L, LDAP can be used for many integration scenarios. For more information about how LDAP works on AIX 5L, refer to *Integrating AIX into Heterogenous LDAP Environments*, SG24-7165, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg247165.html?open>

13.9 Secure Shell

On Solaris 9, Secure Shell (SSH) is installed as part of the default installation provided by Sun Microsystems™. Alternately, you can download and install OpenSSH from the following Web site:

<http://www.sunfreeware.com>

AIX 5L V5.3 works with OpenSSH, which is available on an installation CD. To install OpenSSH on AIX 5L, perform the following tasks:

1. Mount the installation CD-ROM.
2. Execute the command provided in Example 13-8. As part of the installation process, you will be asked to change the AIX 5L CDs for the installation of the prerequisites.

Example 13-8 OpenSSH installation

```
# /usr/lib/instl/sm_inst installp_cmd -a -Q -d '/dev/cd0' -b \  
'openssh_server' -f 'all' '-c' '-N' '-g' '-X' '-G' '-Y'
```

After installation, SSH is automatically started, and the system is prepared for SSH startup at the next boot.

The configurations file is located on `/etc/ssh`. If you are not using OpenSSH on Solaris, it is recommended that you rebuild the configuration in the migration scenario.

For more information about how OpenSSH works, refer to the following Web site:

<http://www.openssh.org/>

13.10 Transmission Control Protocol Wrapper

The Transmission Control Protocol (TCP) Wrapper software extends the abilities of `inetd` to provide support for all the server daemons under its control. By using this method, it is possible to provide logging support, return messages to connections, permit a daemon to only accept internal connections, and so on. Although some of these features can be provided by implementing a firewall, this not only adds an extra layer of protection, but goes beyond the amount of control a firewall can provide.

On Solaris 9, you can activate TCP wrappers by specifying the follow parameter in the `/etc/default/inetd` configuration file:

```
ENABLE_TCPWRAPPERS=YES
```

You can also download the other version of TCP Wrapper from the following Web site:

<http://www.sunfreeware.com>

Perform the following tasks for the installation on AIX 5L:

1) Download the installation package from the following Web site:

<http://www.bullfreeware.com/>

2) Change file permission to executable and execute it, as shown in Example 13-9.

Example 13-9 Executing TCP Wrapper on AIX 5L

```
# pwd
/tmp/tcp
# ls
tcp_wrappers-7.6.1.0.exe
# chmod 750 tcp_wrappers-7.6.1.0.exe
# ./tcp_wrappers-7.6.1.0.exe
UnZipSFX 5.32 of 3 November 1997, by Info-ZIP (Zip-Bugs@lists.wku.edu).
  inflating: tcp_wrappers-7.6.1.0.bff
  inflating: tcp_wrappers-7.6.1.0.bff.asc
#
```

3) Run the installation command, as shown in Example 13-10.

Example 13-10 TCP Wrapper installation

```
# /usr/lib/instl/sm_inst installp_cmd -a \
> -d /tmp/tcp -f freeware.tcp_wrappers -c -N -g -X -G -Y
```

After the installation, you have to set up in a similar mode on the Solaris server. The configuration is based on the following files:

- ▶ /etc/hosts.allow
- ▶ /etc/hosts.deny
- ▶ /etc/inetd.conf

In Example 13-11, the original FTP line on `/etc/inetd.conf` has been changed in order to facilitate a new entry related to TCP Wrapper. The first line of the example is the original line, and the second line has been changed to work with TCP Wrapper.

Example 13-11 Changing the original FTP line on `/etc/inetd.conf`

```
#ftp      stream tcp6    nowait root    /usr/sbin/ftpd      ftpd
ftp       stream tcp6    nowait root    /usr/local/bin/dept.  ftpd
```

In the migration scenario, if you intend to use the same rules on `/etc/hosts.allow` and `/etc/hosts.deny`, you can copy the files from Solaris to AIX 5L because the formats are the same.

Note: Remember to refresh `inetd` after changing the `/etc/inetd.conf` file. To perform this task, use the `refresh -s inetd` command.

13.11 Network File System

The default NFS, which is available on Solaris 9, is based on NFS V3. AIX 5L V5.3 is fully compatible with this version in the migration scenario. However, you can improve the NFS security using NFS V4.

NFS V4 protocol focuses on adding the security schemes built into the protocol.

AIX 5L V5.3 also has an NFS4 ACL-enabled. This is an RFC optional feature.

For more information about securing NFS4, refer to *Securing NFS in AIX An Introduction to NFS v4 in AIX 5L Version 5.3*, SG24-7204, which is available on the Web at:

<http://www.redbooks.ibm.com/redbooks/pdfs/sg247204.pdf>

13.12 Sudo

Sudo (superuser do) is a program that allows users to run programs in the guise of another user (normally in the guise of the system's super user) by logging the commands.

Sudo is a freeware software and is distributed under an Internet Systems Consortium (ISC) license. For more information, refer to the following Web site:

<http://www.gratisoft.us/sudo/>

For Solaris 9, the package download is available in the following Web site:

<http://www.sunfreeware.com>

For AIX 5L, you can download it from the following Web site:

<http://www-03.ibm.com/servers/aix/products/aixos/linux/download.html>

You can also install it from the Toolbox CD-ROM.

The main configuration file is called *sudoers*. In a migration scenario, if AIX 5L and Solaris have the same user configuration (names), you can copy the file from the source to the target server. It is important to check if you are working with the same version.

To install sudo, perform the following tasks:

1. Perform a download of sudo RPM, and put the file on the target server (AIX 5L).
2. Install the package (Example 13-12).

Example 13-12 Installing sudo

```
# pwd
/tmp/sudo
# ls -l
total 328
-rw-r----- 1 root    system      165382 May 10 10:14
sudo-1.6.7p5-3.aix5.1.ppc.rpm
# rpm -ivh sudo-1.6.7p5-3.aix5.1.ppc.rpm
sudo
#####
#
```

3. Copy the configuration file from Solaris or build another one.

Any modification to the configuration file is automatically applied. For more information, refer to the following Web site:

<http://www.gratisoft.us/sudo/>

13.13 Kerberos

Kerberos is a network authentication service that provides a means of verifying the identities of principals on physically insecure networks. Kerberos provides mutual authentication, data integrity, and privacy under the realistic assumption that network traffic is vulnerable to capture, examination, and substitution.

On Solaris, Kerberos is based on the Sun Enterprise™ Authentication Mechanism™ Key Distribution Center (SEAM KDC). The AIX 5L Network Authentication Service client is interoperable at the Kerberos protocol level (RFC1510). However, because Solaris kadmind daemon interface is incompatible with the Network Authentication Service clients, you cannot use the **kadmin** command (or **kadm5_***** APIs) to administer a Solaris-based Kerberos database. The Solaris kadmind daemon interface is also incompatible with MIT-based clients. AIX 5L clients can use KRB5A to authenticate against SEAM.

However, principal management must be performed on the Solaris system using the Solaris tools.

For the migration scenario, check the compatibilities and examples in the following Web sites:

- ▶ http://www-03.ibm.com/servers/aix/whitepapers/aix_kerberos.pdf
- ▶ http://publib16.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixbman/security/kerberos_questions_troubleshooting.htm

13.14 IP Security Architecture and Internet Key Exchange

IP Security Architecture (IPsec) and the Internet Key Exchange (IKE) are available in Solaris 9 and AIX 5L. IPsec provides cryptographic protection for IP datagrams in IPv4 and IPv6 network packets. IPsec is an effective tool in securing network traffic.

The IKE framework supports automated negotiation of Security Associations, and automated generation and refreshing of cryptographic keys.

The SMIT tool has options to perform the tasks related to IPsec and IKE. The fast paths are `smit ipsec4` and `smit ipsec6`.

Figure 13-2 shows the first screen that opens on issuing `smit ipsec4`.

```
Configure IP Security (IPv4)

Move cursor to desired item and press Enter.

Start/Stop IP Security
Basic IP Security Configuration
Advanced IP Security Configuration

F1=Help          F2=Refresh       F3=Cancel        F8=Image
F9=Shell         F10=Exit         Enter=Do
```

Figure 13-2 Using `smit ipsec4`

The basic configuration allows setting tunnels with a minimum number of the required parameters. Simple filter rules to control all the traffic through the tunnel are automatically generated. A tunnel definition must match the corresponding tunnel definition on the remote host.

Advanced configuration allows the manipulation of the IP Security Filter rules, lists the supported encryption algorithms, and allows the use of IP Security Diagnostic facilities such as tracing and logging.

13.15 Pluggable Authentication Module and Loadable Authentication Module

In the recent past, the Pluggable Authentication Module (PAM) framework became a standard method of authentication in the industry. PAM provides a means of separating authentication technologies from authentication services, allowing different services to potentially follow independent authentication paths.

The `/usr/lib/libpam.a` library was provided in AIX 5L V5.1 in order to give the PAM applications the ability to make use of the PAM framework. This solution did not allow the existing AIX 5L security services to utilize the PAM framework.

Further, PAM functions were integrated into AIX 5L V5.2 through the use of the existing AIX 5L Loadable Authentication Module (LAM) scheme and the creation of a PAM AIX 5L LAM module, `/usr/lib/security/PAM`. Users defined to use the PAM AIX 5L LAM module for their registry can be routed to PAM for authentication, effectively “PAM-enabling” all the existing AIX 5L security services. The module `/usr/lib/security/pam_aix` was also provided in order to allow the existing PAM applications access AIX 5L security services through the PAM interface.

The enhancements to the AIX 5L V5.3 PAM implementation are focused on PAM application compatibility, better AIX 5L base OS integration, and improved configuration support.

For more information about PAM on AIX 5L, refer to *AIX 5L Differences Guide Version 5.3 Edition*, SG24-7463, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg247463.html?Open>



Backup and restore

This chapter discusses the backup tools that are available for migration from Solaris to AIX 5L. It includes the backup and compression tools and the differences in their usage.

This chapter discusses the following topics:

- ▶ 14.1, “Local tape, CD, or DVD operating system backup” on page 400
- ▶ 14.2, “Remote operating system backup” on page 406
- ▶ 14.3, “Volume group backup” on page 410
- ▶ 14.4, “File system or directory backup” on page 412
- ▶ 14.5, “Raw devices backup” on page 415
- ▶ 14.6, “AIX 5L SysBack (IBM Tivoli Storage Manager for System Backup and Recovery)” on page 415
- ▶ 14.7, “Compression tools” on page 417
- ▶ 14.8, “Managing tape backup media” on page 417

14.1 Local tape, CD, or DVD operating system backup

The main objective of an image backup is to provide a resource for recovering the operating system (OS) in case of a disaster. The disaster's cause can be an operational problem (human error) or a hardware problem.

In the Solaris environment, no specific tool exists for an image backup, but there are two possible workaround solutions, *ufsdump* backup and *flash archive* backup.

In AIX 5L, there is a useful tool for this task called *mksysb*.

14.1.1 Solaris ufsdump backup

The most widely used solution for local OS backup is *ufsdump*. It works for UNIX file system (UFS), which is the standard disk-based file system used by Solaris.

This solution is not totally supported by the vendor for online backup because *ufsdump* is not designed to work on a mounted file system. It reads directly from the raw device. Therefore, the file system must be inactive. Otherwise, the output of *ufsdump* might be inconsistent, and restoring files correctly might be impossible. The file systems are inactive when they are unmounted, on ready only status, or if the system is in single-user mode. A file system is not considered inactive if one tree of the file system is quiescent while another tree has files or directories being modified.

In a disaster scenario, you must boot from the CD-ROM to perform the restore from *ufsdump*.

14.1.2 Solaris flash archive

This method is slightly different from *ufsdump* backup because flash archive does not save some network settings, such as the *hosts*, *nsswitch.conf*, and *resolv.conf*. This is because the purpose of flash archive is for the flash installation function to *clone* to another machine on the network. The command used for performing this task is **flarcreate**.

In a restoration scenario, as with *ufsdump*, you must boot from the installation CD-ROM.

For more information about **flarcreate** for OS backup, refer to the man pages and documentation available on the Web at:

http://www.sun.com/bigadmin/content/submitted/flash_archive.html

14.1.3 AIX 5L tape image backup

The `mksysb`, which is used for AIX 5L image backup, is a helpful tool in disaster recovery scenarios. This tool generates a bootable system image, and when restoring, you can boot directly from this backup tape.

The `mksysb` command creates a bootable image of all the mounted file systems on the rootvg volume group.

The tape format includes a Base Operating System (BOS) boot image, a BOS install image, and a dummy table of contents (TOC), followed by the system backup (root volume group) image. The root volume group image is in a backup-file format, starting with the data files, followed by any optional map files.

User-defined paging spaces, unmounted file systems, and raw devices are not backed up.

To perform a `mksysb` backup of a system and exclude some data file systems from the system, edit the `/etc/exclude.rootvg` file.

`Mksysb` processing excludes the files using the `grep` format. The file list that the exclusions are matched against are relative to the root directory. If, for example, you want to exclude the file system and `/tmp` from your `mksysb` backup, add the following:

```
^./tmp/
```

Ensure that there are no empty lines in this file. List the contents of the file, as shown in Example 14-1.

Example 14-1 Listing the `exclude.rootvg` file

```
# cat /etc/exclude.rootvg  
^./tmp/  
#
```

Run the `mksysb` command using the `-e` flag to exclude the contents of the `exclude.rootvg` file, as shown in Example 14-2.

Example 14-2 Running the `mksysb`

```
# mksysb -e /dev/rmt0  
Creating information file (/image.data) for rootvg.  
Creating tape boot image.....  
bosboot: Boot image is 29316 512 byte blocks.  
Creating list of files to back up.  
Backing up 2679 files.....
```

2679 of 2679 files (100%)
0512-038 mksysb: Backup Completed Successfully.
bosboot: Boot image is 29316 512 byte blocks.

Following are the most common options used on mksysb:

- ▶ -e use exclude filelist /etc/exclude.rootvg
- ▶ -v verbose filelist
- ▶ -X expand /tmp automatically if needed
- ▶ -i generates volume group and file system information for future use by install process

Following is an example of an mksysb option:

```
/usr/bin/mksysb '-e' '-v' '-i' '-X' /dev/rmt0
```

Refer to the mksysb man pages for more information about the options.

You can use either the System Management Interface Tool (SMIT) or the Web-based System Manager (WebSM) to perform an image backup, as shown in Figure 14-1 and Figure 14-2.

The fast path on SMIT is `smit mksysb`. Figure 14-1 shows the screen that appears on using the fast path.

```

                                     Back Up the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                     [Entry Fields]

WARNING: Execution of the mksysb command will
         result in the loss of all material
         previously stored on the selected
         output medium. This command backs
         up only rootvg volume group.

* Backup DEVICE or FILE                [/dev/rmt0]
Create MAP files?                       no
EXCLUDE files?                          yes
List files as they are backed up?       yes
Verify readability if tape device?     no
Generate new /image.data file?          yes
EXPAND /tmp if needed?                  yes
Disable software packing of backup?     no
Backup extended attributes?             yes
Number of BLOCKS to write in a single output []
(Leave blank to use a system default)

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command         F7=Edit           F8=Image
F9=Shell        F10=Exit           Enter=Do
```

Figure 14-1 Using `smit mksysb`

Figure 14-2 shows the WebSM backup.

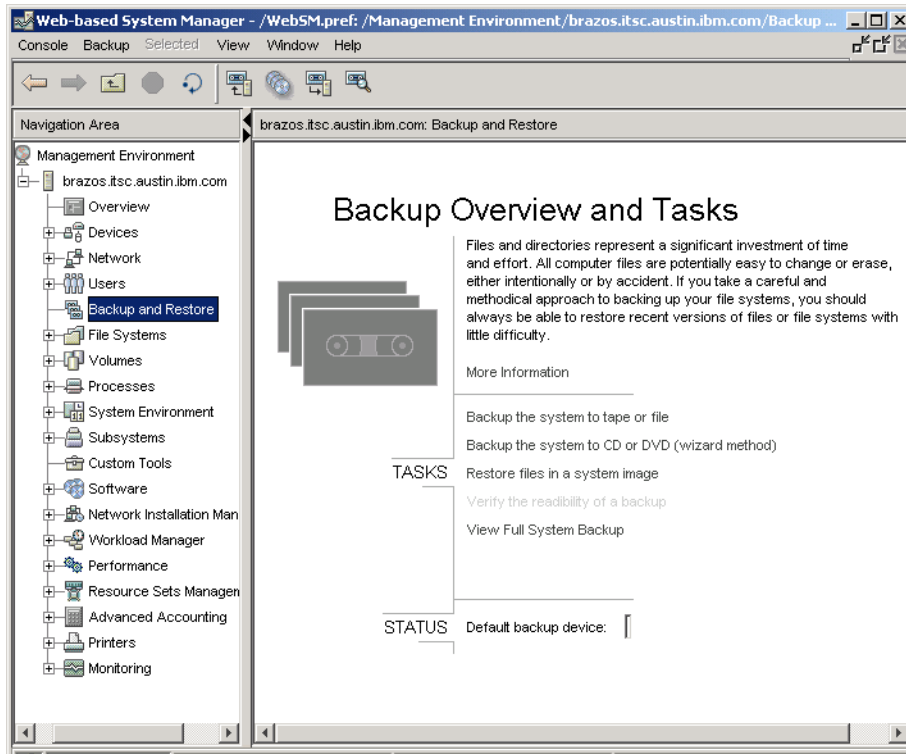


Figure 14-2 WebSM backup

For more details about how to use SMIT and WebSM, refer to Chapter 9, “Managing system resources” on page 239.

For more detailed information about how to back up and restore resources, refer to Chapter 10 of *IBM Certification Study Guide eServer p5 and pSeries Administration and Support for AIX 5L Version 5.3*, SG24-7199, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/SG247199.html?Open>

14.1.4 AIX 5L CD or DVD image backup

The `mkcd` command creates a system backup image (`mksysb`) to CD-Recordable (CD-R) or DVD-Recordable (DVD-R, DVD-RAM) from the system rootvg or from a `mksysb` image created earlier. It also creates a volume group backup image (`savevg`) to CD-R from a user-specified volume group or from a `savevg` image created earlier.

For the DVD media, system backups made with the **mkcd** command have a limitation, in that, they expect the media to be 4.7 GB or larger per side. The **mkcd** command does not process the next volume until it writes over 4 GB on the current volume. Thus, the use of smaller media results in corruption when it goes beyond the media's capacity.

With the **mkcd** command, you can create bootable and nonbootable CDs in Rock Ridge (ISO9660) or Universal Disk Format (UDF).

See the **-L** flag for details about creating DVD-sized images. What applies to CDs also applies to DVDs, except where specified otherwise.

To create multivolume CDs because the volume group image does not fit on one CD, the **mkcd** command provides instructions for CD replacement and removal until all the volumes are created.

As with **mksysb**, **mkcd** can also be managed by the **smit** tool, using the fast path **smit mkcd**, or the **WebSM**.

For **WebSM**, refer to the wizard method shown in Figure 14-2 on page 404.

When using **smit mkcd**, the first question is whether you want to generate a new image or use an existing one. Figure 14-3 shows the first screen of **smit mkcd**.

```
                                Use an existing mksysb image?

Move cursor to desired item and press Enter.

  1 yes
  2 no

F1=Help          F2=Refresh          F3=Cancel
F8=Image         F10=Exit           Enter=Do
/=Find          n=Find Next
```

Figure 14-3 First screen of **smit mkcd**

The second screen of `smit mkcd` (Figure 14-4) assumes that you want to generate a new image.

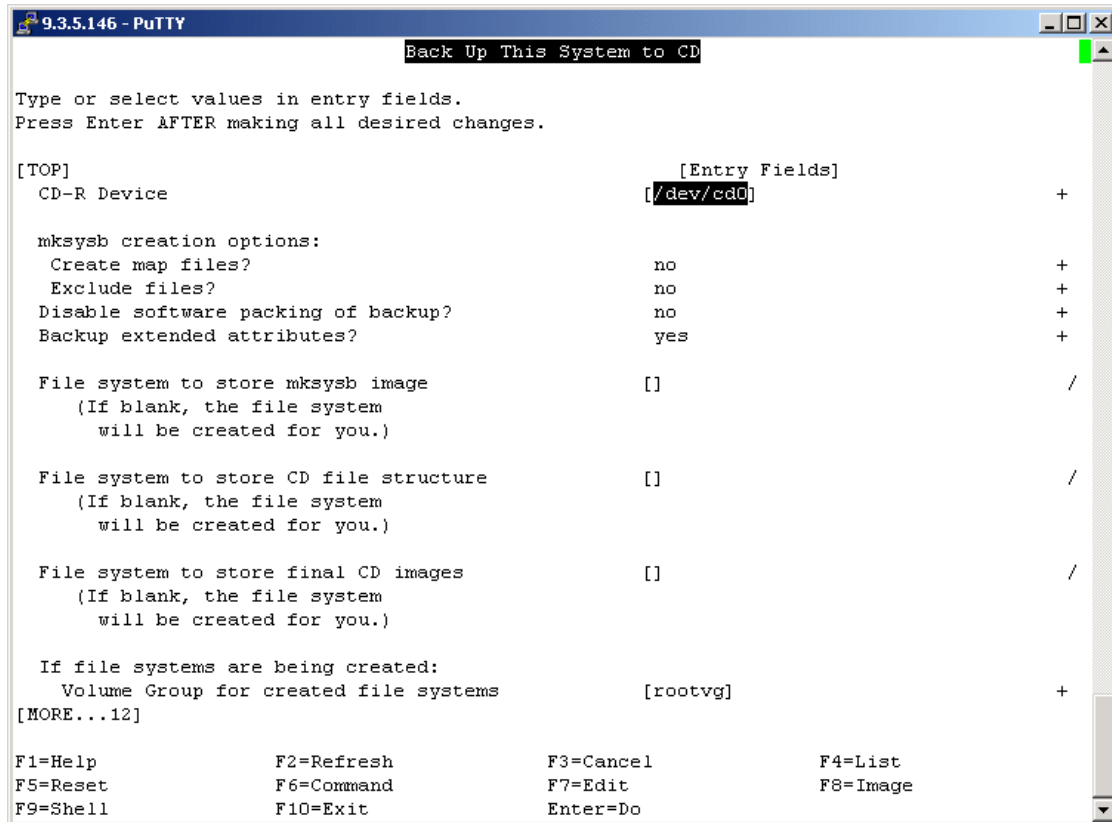


Figure 14-4 Second screen of `smit mkcd`

For more information, refer to *IBM Certification Study Guide eServer p5 and pSeries Administration and Support for AIX 5L Version 5.3*, SG24-7199, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/SG247199.html?Open>

14.2 Remote operating system backup

In the Solaris environment, `ufsdump` and `flash archive` are available for local or remote tapes. In the same mode as `ufsdump` on Solaris, you can use `rdump` on AIX 5L. On both the OS, these commands do not generate a bootable tape for restore.

These resources are useful for other backups, but can cause problems for image solutions.

The best solution on AIX 5L for a remote image backup is to work with the Network Installation Manager (NIM).

14.2.1 Creating an mksysb image of the machine using the Network Installation Manager

An mksysb resource represents a file that is a system backup image created by using the **mksysb** command. This type of resource can be used as the source for the installation of a client. The mksysb image must reside on the hard disk of a machine in the NIM environment in order to be defined as a resource. It cannot be located on a tape or on other external media.

An mksysb resource can be defined from an image that already exists on the hard disk of the NIM master or a NIM client. If such an image does not exist, it can be created when the resource is defined. To create the image when the resource is defined, specify the name of the NIM client that will be the source for the system backup, and set the `mk_image` attribute to “yes” in the command to define the mksysb resource. Use an `exclude_files` resource to list any files and directories that must not be included in the backup image.

Assumptions

Following are the assumptions:

- ▶ You already have a NIM master server set up and running.
- ▶ The machine being backed up is defined as a NIM client.

For more information about NIM, refer to Chapter 3, “Operating system installation” on page 47.

The easiest way to create the mksysb resource and define it as a resource in the NIM environment is to use **smit nim_mkres**.

In the screen that opens (Figure 14-5), select **mksysb** as the desired resource.

```
Resource Type

Move cursor to desired item and press Enter. Use arrow keys to scroll.

[MORE...7]
  exclude_files = files to be excluded when creating a mksysb or savev
  lpp_source    = source device for optional product images
  installp_bundle = an installp bundle file
  fix_bundle    = fix (keyword) input file for the cust or fix_query o
  bosinst_data  = config file used during base system installation
  image_data    = config file used during base system installation
  vg_data      = config file used during volume group restoration
  mksysb       = a mksysb image
  script        = an executable file which is executed on a client
  resolv_conf   = configuration file for name-server information
[MORE...4]

F1=Help          F2=Refresh          F3=Cancel
F8=Image         F10=Exit           Enter=Do
/=Find          n=Find Next
```

Figure 14-5 Creating an mksysb image of NIM client using **smit nim_mkres**

Provide the values for the required fields in the screen that is displayed (Figure 14-6). Use the **Help** and **LIST** options to find the correct values.

```

Define a Resource

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[TOP]                                [Entry Fields]
* Resource Name                       [aix53_04_mksysb_res]
* Resource Type                       mksysb
* Server of Resource                   [master] +
* Location of Resource                 <xport/nim/mksysb/530/ /
Comments                              []

Source for Replication                 [] +
-OR-
System Backup Image Creation Options:
  CREATE system backup image?         yes +
  NIM CLIENT to backup                 [trinity] +
  PREVIEW only?                       no +
  IGNORE space requirements?          no +
[MORE...10]

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit         Enter=Do

```

Figure 14-6 SMIT NIM operation to create and define an mksysb resource

In Figure 14-6, an mksysb image of the NIM client Trinity is made and stored on the NIM master in /export/nim/mksysb/530/.

Note: Trinity is not necessarily the host name of the machine. It is the NIM resource name for *this* NIM client. The mksysb resource name is aix53_04_mksysb_res.

Restoring an mksysb image using the Network Installation Manager server

It is important to ensure that when you restore an mksysb image to a NIM client, the spot resource defined for this client is the same AIX 5L version and is at the same maintenance level as the mksysb image.

The example client machine referenced in Figure 14-6 on page 409 can be restored from the NIM master, using the following command:

```
nim -o bos_inst -a source=mksysb -a mksysb=aix53_04_mksysb_res \
-a spot=aix5304_cd_spot -a boot_client=yes trinity
```

14.3 Volume group backup

In the Solaris environment, no command is included in the basic OS to perform volume group backup and restore. In such a situation, the administrator is responsible for selecting the necessary areas and using the available tools such as `ufsdump`, `tar`, `cpio`, `dd`, and so on.

In AIX 5L, there are specific commands for this task, **savevg** and **restvg**.

The **savevg** command finds and backs up all the files belonging to a specified volume group. A volume group must be varied on, and the file systems must be mounted. The **savevg** command uses the data file created by the **mkvgdata** command. This file can be one of the following:

- ▶ `/image.data`

Contains information about the root volume group (`rootvg`). The **savevg** command uses this file to create a backup image that can be used by NIM to reinstall the volume group to the current system or to a new system.

- ▶ `/tmp/vgdata/vgname/vgname.data`

Contains information about a user volume group. The `vgname` variable reflects the name of the volume group. The **savevg** command uses this file to create a backup image that can be used by the **restvg** command to remake the user volume group.

Note: The **savevg** command does not generate a bootable tape if the volume group is the root volume group.

The **restvg** command restores the user volume group and all its containers and files, as specified in the `/tmp/vgdata/vgname/vgname.data` file (where `vgname` is the name of the volume group) contained within the backup image created by the **savevg** command.

The **restvg** command restores a user volume group. The `bosinstall` routine reinstalls the root volume group (`rootvg`). If the **restvg** command encounters a `rootvg` volume group in the backup image, the **restvg** command exits with an error.

If a “yes” value has been specified in the `EXACT_FIT` field of the `logical_volume_policy` stanza of the `/tmp/vgdata/vgname/vgname.data` file, the **restvg** command uses the map files to preserve the placement of the physical partitions for each logical volume. The target disks must be of the same size or larger than the source disks specified in the `source_disk_data` stanzas of the `vgname.data` file.

The `smit` is available for volume group backup and restore. Use the fast paths `smit savevg` and `smit restvg`, as shown in Figure 14-7 and Figure 14-8 respectively.

```

                                Back Up a Volume Group to Tape/File

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]

WARNING: Execution of the savevg command will
         result in the loss of all material
         previously stored on the selected
         output medium.

* Backup DEVICE or FILE          [ ]          +/
* VOLUME GROUP to back up       [ ]          +
List files as they are backed up? no          +
Generate new vg.data file?     yes          +
Create MAP files?               no          +
EXCLUDE files?                  no          +
EXPAND /tmp if needed?         no          +
Disable software packing of backup? no          +
Backup extended attributes?    yes          +
Number of BLOCKS to write in a single output [ ]          #
(Leave blank to use a system default)
Verify readability if tape device? no          +
Back up Volume Group information files only? no          +

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command         F7=Edit           F8=Image
F9=Shell        F10=Exit           Enter=Do

```

Figure 14-7 Using `smit savevg`

```

Remake a Volume Group

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                     [Entry Fields]
* Restore DEVICE or FILE                [ ]          +/-
SHRINK the filesystems?                 [ ]          +
Recreate logical volumes and filesystems only?  no          +
PHYSICAL VOLUME names                   [ ]          +
  (Leave blank to use the PHYSICAL VOLUMES listed
  in the vname.data file in the backup image)
Use existing MAP files?                  yes         +
Physical partition SIZE in megabytes     [ ]          +#
  (Leave blank to have the SIZE determined
  based on disk size)
Number of BLOCKS to read in a single input [ ]          #
  (Leave blank to use a system default)
Alternate vg.data file                   [ ]          /
  (Leave blank to use vg.data stored in
  backup image)

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit      Enter=Do

```

Figure 14-8 Using `smit restvg`

The `mkcd` command can also generate a backup from a volume group to a CD or DVD media:

```
# mkcd -d /dev/cd1 -v vname
```

Refer to the `mkcd` man pages for more information about the available options.

14.4 File system or directory backup

Table 14-1 shows the numerous tools available for performing different types of backups.

Table 14-1 Tools available for performing backups

Task	Solaris	AIX 5L
Local backup and restore of files and file systems	<ul style="list-style-type: none"> ▶ <code>ufsdump/ufsrestore</code> ▶ <code>vxdump/vxrestore</code> 	<code>backup/restore</code>
Remote backup and restore of files and file systems	<ul style="list-style-type: none"> ▶ <code>ufsdump/ufsrestore</code> ▶ <code>vxdump/vxrestore</code> 	<code>rdump/rrestore</code>

Task	Solaris	AIX 5L
Create tape archives and add or extract files	tar	tar
Copy files into and out of archive storage and directories	cpio	cpio
Extract, write, and list members of archive files. Copy files and directory hierarchies	pax	pax
Convert and copy a file	dd	dd
Copy the contents of a logical volume to a new logical volume	N/A	cp1v

The different tools on AIX 5L is described in this section.

cp1v

The **cp1v** is not used for tape or CD and DVD backup. The **cp1v** command copies the contents of SourceLogicalVolume to a new or existing DestinationLogicalVolume. The SourceLogicalVolume parameter can be a logical volume name or a logical volume ID. The **cp1v** command creates a new logical volume with a system-generated name by using the default syntax. The system-generated name is displayed.

Use the `smit cplv` fast path to run this command (Figure 14-9).

```
Copy a Logical Volume

Move cursor to desired item and press Enter.

Copy over an existing logical volume
Copy to a user created logical volume
Copy to a system created logical volume

F1=Help          F2=Refresh      F3=Cancel      F8=Image
F9=Shell         F10=Exit       Enter=Do
```

Figure 14-9 Using `smit cplv`

Attention: Do not copy from a larger logical volume containing data to a smaller logical volume. Doing so results in a corrupted file system because some data, including the superblock, is not copied. This command fails if the `cplv` creates a new logical volume and the volume group is varied on in the concurrent mode.

rdump

The `rdump` command copies file systems by i-node from the local machine to a remote machine. The files are copied, using the backup command format, to a device on the remote machine. The device is accessed by using a remote server on the remote machine. You must have root authority to execute the `rdump` command.

You must also define a local machine running the `rdump` command in the `/.rhosts` file of the target remote machine.

To back up a file system, specify the `-Level` and `FileSystem` parameters to indicate the files you want to back up. Use the `-Level` parameter to back up either all the files on the system (a full backup) or only the files that have been modified since a specific full backup (an incremental backup). The possible levels are 0 - 9. If you do not supply a level, the default level is 9. A level 0 backup includes all

the files on the file system. A level *n* backup includes all the files modified since the last level *n* - 1 (*n* minus 1) backup. The levels, in conjunction with the `-u` flag, provide a method of maintaining an hierarchy of incremental backups for each file system.

rrestore

This copies the file systems backed up earlier from a remote machine's device to the local machine. The **rrestore** command accepts only the backup formats created when a file system is backed up by `i-node`.

14.5 Raw devices backup

There are some applications or databases that save information on logical volumes without any file system. In this case, the UNIX administrator cannot see the information, but has to perform the backup of this data. The most common command that is used for this task is **dd**, which is available on many UNIX and Linux platforms. If you have such a scenario in AIX 5L, and the target copy area is another logical volume, consider using the **cp1v** command, which is described in “`cplv`” on page 413.

The raw devices backup and restore solutions can also be used if you have a scenario in which the source area has many files. This solution is useful for reducing the backup time.

14.6 AIX 5L SysBack (IBM Tivoli Storage Manager for System Backup and Recovery)

IBM Tivoli Storage Manager for System Backup and Recovery is an advanced backup and recovery product for AIX 5L. It is traditionally known as Sysback for AIX 5L. In Sysback V5.6, the product was integrated with IBM Tivoli Storage Manager and renamed IBM Tivoli Storage Manager for System Backup and Recovery. In this book, IBM Tivoli Storage Manager for System Backup and Recovery is referred to by its traditional name of Sysback.

Although Sysback is now named IBM Tivoli Storage Manager for System Backup and Recovery, it does not require an IBM Tivoli Storage Manager server to be functional.

A large amount of information is available for Sysback. However, this book does not aim to provide a complete coverage of Sysback. It only provides an introduction to Sysback's capabilities and links to dedicated Sysback documentation.

Sysback provides the following functionalities:

- ▶ Remote backup restore and installation capabilities
- ▶ Support for multiple media formats:
 - Stand-alone tape
 - Tape autochangers
 - Automated tape libraries
 - File on disk
 - Recordable CD and DVD
- ▶ Backup and recovery of nonrootvg volumes groups
- ▶ Raw logical volumes support
- ▶ Optional coexistence with NIM (refer to Chapter 3, "Operating system installation" on page 47)
- ▶ Optional integration with Tivoli Storage Manager, including bare-metal recovery and installation of AIX 5L from the images stored in Tivoli Storage Manager
- ▶ Central management and automation of backups
- ▶ Offline split mirror backup options
- ▶ System cloning

One of the biggest advantages of Sysback, which is also a time-saving one, is when Sysback is integrated with a Tivoli Storage Manager server for managing the AIX 5L recovery images. Integration with a Tivoli Storage Manager server allows Tivoli Storage Manager to automatically manage AIX 5L recovery images along with other enterprise backups, thus avoiding the necessity to manually manage mksysb images. If you have a Tivoli Storage Manager installation, the use of Sysback that is integrated with Tivoli Storage Manager is worth considering when migrating from Solaris to AIX 5L.

For more information about Sysback, refer to *IBM Tivoli Storage Manager: Bare Machine Recovery for AIX with SYSBACK*, REDP-3705, and the following Web sites:

- ▶ <http://www-306.ibm.com/software/tivoli/products/storage-mgr-sysback/>
- ▶ <http://publib.boulder.ibm.com/infocenter/tivihelp/v1r1/index.jsp?topic=/com.ibm.itsmsbr.doc/bmrug56517.htm>

For information about using Sysback with Tivoli Storage Manager, refer to *IBM Tivoli Storage Manager Implementation Guide*, SG24-5416, which is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg245416.html?Open>

14.7 Compression tools

The compression tools are similar on AIX 5L V5.3 and Solaris 9. The following tools are available for both the OS:

- ▶ compress and uncompress
- ▶ bzip2, bunzip2, bzip2recover
- ▶ gzip, gunzip, and gzcac
- ▶ gzexe
- ▶ pack, pcat, and unpack
- ▶ zip, zipcloak, zipnote, and zipsplit

The zip, zipcloak, zipnote, and zipsplit tools are *not* available on the default installation of AIX 5L V5.3. You can install them from the toolkit CD-ROM or download the package from the following Web site:

<http://www-03.ibm.com/servers/aix/products/aixos/linux/download.html>

After downloading, perform installation as shown in Example 14-3.

Example 14-3 Zip installation

```
# rpm -ivh zip-2.3-3.aix4.3.ppc.rpm
zip
#####
```

14.8 Managing tape backup media

In the Solaris server, you are used to working with the **mt** command for tape backup management. In AIX 5L, you can use **mt** or **tctl** commands to perform this task.

Tape verification

AIX 5L has a specific command for tape verification. The **tapechk** command performs rudimentary consistency checking on an attached streaming tape device. Some hardware malfunctions of a streaming tape drive can be detected

by simply reading a tape. The **tapechk** command provides a way to perform tape reads at the file level.

Because the streaming tape drive cannot back up over physical data blocks or files, the **tapechk** command rewinds the tape to its starting position prior to each check. This command either checks the data for the next number of files specified by the **Number1** parameter or skips the next number of the files specified by the **Number2** parameter. If you do not specify any parameters, the **tapechk** command rewinds the tape and checks only the first physical block.

The **tapechk** command uses the device in the **TAPE** environment variable if it is defined. Otherwise, the default tape device is **/dev/rmt0**.

Copy between tapes

Solaris and AIX 5L OS have the **tcopy** utility for copying the magnetic tape that is mounted on the tape drive specified by the source argument. The only assumption made about the contents of a tape is that there are two tape marks at the end.

When only a source drive is specified, **tcopy** scans the tape and displays information about the sizes of the records and the tape files. If a destination is specified, **tcopy** makes a copy of the source tape on the destination tape, with the blocking preserved. When it copies, **tcopy** produces the same output that it does when only scanning a tape.

Tape management command and options

In the Solaris server, you are used to working with the **mt** command for tape management. In AIX 5L, the **mt** and **tct1** are exactly the same. The options of the **mt** and **tct1** commands are similar on both the platforms. Refer to the corresponding man pages for details.

Tape names on Solaris and AIX 5L

See Table 14-2 and Table 14-3 to understand the special files for tapes on Solaris and AIX 5L.

Table 14-2 shows a summary of tape special files on Solaris.

Table 14-2 Summary of tape special files on Solaris

Special file name	Rewind	Compression
/dev/rmt/x	yes	no
/dev/rmt/xc	yes	yes
/dev/rmt/xn	no	no

Special file name	Rewind	Compression
/dev/rmt/xcn	no	yes

Table 14-3 shows a summary of tape special files on AIX 5L.

Table 14-3 Summary of tape special files on AIX 5L

Special file name	Rewind on closing	Retention on open	Bytes per inch
/dev/rmt*	yes	no	Density setting #1
/dev/rmt/*.1	no	no	Density setting #1
/dev/rmt/*.2	yes	yes	Density setting #1
/dev/rmt/*.3	no	yes	Density setting #1
/dev/rmt/*.4	yes	no	Density setting #2
/dev/rmt/*.5	no	no	Density setting #2
/dev/rmt/*.6	yes	yes	Density setting #2
/dev/rmt/*.7	no	yes	Density setting #2



High availability and clustering overview

This chapter provides high-level information about the clustering options that are available on AIX 5L when migrating from a Solaris cluster environment. It also provides references for more indepth information and how-to documentations for the AIX 5L clustering options.

This chapter discusses the following topics:

- ▶ 15.1, “Introduction to clustering” on page 422
- ▶ 15.2, “Solaris clustering software” on page 422
- ▶ 15.3, “AIX 5L clustering software” on page 424

15.1 Introduction to clustering

Clustering is a technique that is used to group a number of computers. It is commonly used to provide increased application availability, known as *High Availability (HA) Clustering*, or Parallel Clusters, which is commonly known as *High Performance Computing Clusters*. The most common type of clustering encountered is HA clustering.

15.2 Solaris clustering software

Following are the clustering options available on Solaris, both commercial and open source:

- ▶ Sun Cluster
- ▶ Veritas Cluster Server
- ▶ Linux HA on Solaris

15.2.1 Sun cluster

This is Sun's own HA clustering product that is native to Solaris. Sun Cluster V3.1 provides the following features:¹

- ▶ Solaris kernel integration
- ▶ Disk path mirroring
- ▶ Diskless failover
- ▶ Dynamic reconfiguration
- ▶ Versioning framework
- ▶ Support for Solaris on both Scalable Processor ARChitecture (SPARC) and x86-based hardware
- ▶ Cluster agents (support for industry-leading applications), both in failover and scalable modes
- ▶ Remote shared memory
- ▶ Application traffic stripping (load balancing between nodes)
- ▶ Veritas Volume Manager and file system
- ▶ Disaster recovery to an alternate mirrored site
- ▶ Single-node cluster for testing and development

¹ This list is a sample of Sun Cluster V3.1 features. For a complete feature listing, refer to the following Web site: http://www.sun.com/software/cluster/features_benefits.xml

- ▶ Supports up to 16 nodes in the cluster
- ▶ Global devices and file services
- ▶ Solaris resource manager integration
- ▶ One-click failover to a disaster recovery site

15.2.2 Veritas Cluster Server for Solaris

This is a cross-platform HA clustering product. It is available for Solaris, AIX 5L, HP-UX, Linux, and Microsoft Windows. Some of the features provided by Veritas Cluster Server (SCV) are:²

- ▶ Allows companies to link multiple, independent HA clusters in multiple sites into a single, highly available disaster recovery framework
- ▶ Allows administrators to monitor, manage, and report on multiple Veritas clusters on different platforms from a single Web-based console
- ▶ Supported on Solaris, HP-UX, AIX 5L, Linux, VMware, and Windows operating system (OS) platforms using default configurations for most database, application, and storage vendors
- ▶ Fire Drill feature effectively creates a carbon copy of live production data and automates the complete application testing process
- ▶ Reduces the number of vendors in the data center by using Cluster Server as the clustering tool for local and remote failover across multiple platforms
- ▶ Increases administrator efficiency through enhanced visualization, automation of common reporting tasks, centralized operational control for global applications, and centralized policy-based notifications
- ▶ Reduces training and labor costs and software licensing and support by using the same clustering tool across all the OS platforms
- ▶ Tests your disaster recovery plans when it is convenient for the IT staff, without impacting the production environment
- ▶ Supports up to 32 servers in a single cluster
- ▶ Supports a broad range of applications through bundled agents
- ▶ Global cluster option
- ▶ Integration with various data replication solutions, including:
 - Veritas Storage Foundation
 - EMC Symmetrix Remote Data Facility (SRDF)

² For a complete list, see:
http://eval.veritas.com/mktginfo/products/Datasheets/High_Availability/vcs_datasheet.pdf

- Veritas Volume Replicator
- Hitachi TruCopy
- Hewlett-Packard Continuous Access
- IBM Peer-to-Peer Remote Copy (PPRC)

15.2.3 Linux high availability on Solaris

While not known as a HA clustering Solution for Solaris, it is possible to use Linux HA software to build a Solaris HA cluster. Linux HA is an opensource HA clustering solution that aims to “Provide a high-availability (clustering) solution for Linux which promotes reliability, availability, and serviceability (RAS) through a community development effort.”³

15.3 AIX 5L clustering software

There are four main clustering solutions that are commonly used with AIX 5L:

- ▶ AIX 5L High Availability Cluster Multi Processing (HACMP)
- ▶ HACMP extended distance (HACMP/XD)
- ▶ Veritas Cluster Server
- ▶ AIX 5L Cluster Systems Management (CSM)

15.3.1 AIX 5L HACMP

HACMP is AIX 5L’s native High Availability Clustering Solution. HACMP V5.3 provides the following features:⁴

- ▶ Helps reduce unplanned outages and improves system availability
- ▶ Offers ease-of-use through configuration wizards, auto discovery, and a Web-based interface
- ▶ Backup systems can be located at a remote site for geographic disaster recovery
- ▶ Provides failover on demand to enable system maintenance without service interruption
- ▶ Up to 32 servers can participate in a HACMP cluster
- ▶ HACMP can be configured to react to events that are not severe enough to interrupt system operations, such as process failure or exhaustion of system resources

³ <http://www.linux-ha.org>

⁴ *An HACMP Cookbook*, SG24-4553

(<http://www.redbooks.ibm.com/abstracts/sg244553.html?0pen>)

- ▶ Cluster test tool that allows evaluation of cluster behavior under a set of specified circumstances
- ▶ Enhanced security mechanisms protect the integrity and operation of a cluster
- ▶ Web-based cluster management enables configuration, monitoring, and management of a cluster from a Web browser
- ▶ Automated nightly cluster verification reduces the risk of a change to the cluster interfering with a future cluster operation or failover
- ▶ HACMP File Collections provide an easy way of maintaining file synchronization across a cluster
- ▶ Supports Veritas Foundation Suite V4.0
- ▶ Ability to define cluster-wide application dependencies in order to streamline and simplify failover of complex, multitier applications
- ▶ Workload Manager for AIX 5L provides resource balancing between applications
- ▶ Supports cluster multiprocessing, for example, the ability to run the same application on multiple nodes in the cluster with shared or concurrent access to the same data
- ▶ HACMP Smart Assist (optional package) simplifies the implementation of HACMP for IBM DB2, Oracle®, and IBM WebSphere environments by reading the application configuration data and configuring HACMP accordingly
- ▶ An HACMP cluster can be a subset of a CSM cluster to allow for enhanced management
- ▶ Supports General Parallel File System (GPFS). GPFS for AIX 5L is a high-performance, shared-disk file system using standard UNIX file system interfaces, and providing concurrent access to data from all the nodes in a cluster.

15.3.2 AIX 5L HACMP/XD

This is the extended distance feature of HACMP. It supports all the features of HACMP with additional features to support a geographically dispersed cluster:

- ▶ Geographic Logical Volume Manager (GLVM) provides remote data mirroring through IP and enables failover to remote sites using the mirrored data. GLVM integrates with AIX 5L LVM to completely manage data synchronization during production, failover, and recovery.
- ▶ Automatic failover to another geographic site

- ▶ Support for IBM Enterprise Storage Systems (ESS)/Metro Mirror, enabling automatic failover of disks that are Metro Mirror pairs. This automates the management of Metro Mirror and minimizes recovery after an outage, for either local or geographically dispersed clusters.
- ▶ Support for IBM TotalStorage PPRC/Metro Mirror for storage area network (SAN) Volume Controller
- ▶ Support for Enterprise Remote Copy Management Facility (eRCMF) for ESS/Metro Mirror
- ▶ High-Availability Geographic Cluster (HAGEO) for unlimited distance IP-based mirroring

An *HACMP Cookbook*, SG24-4553 covers a wide range of topics from planning and implementation to management and maintenance of an HACMP cluster. It is available on the Web at:

<http://www.redbooks.ibm.com/abstracts/sg244553.html?open>

HACMP/XD product manuals are available on the Web at:

http://www-03.ibm.com/servers/eserver/pseries/library/hacmp_docs.html

An overview of HACMP is available in the following Web site:

<http://www-03.ibm.com/systems/p/software/hacmp.html>

For more information about the Veritas Cluster Server, refer to:

http://seer.support.veritas.com/docs/CLUSTERSERVER_index.htm

15.3.3 AIX 5L Cluster Systems Management

Cluster Systems Management (CSM) is available for both AIX 5L and Linux. A CSM cluster can include both AIX 5L and Linux nodes. CSM is not an HA cluster such as HACMP. However, an HACMP cluster can be a subset of a CSM cluster.

CSM provides a single point of control for managing a large number of AIX 5L or Linux hosts. It is commonly included with IBM System Cluster 1600 and IBM System Cluster 1350™ systems. CSM provides the following features, which greatly reduce the management effort required to manage a cluster of AIX 5L or Linux hosts:⁵

- ▶ Controls multiple machines from a single point
 - Configuration file management

⁵ <http://www-03.ibm.com/servers/eserver/clusters/software/csm.html>

Cluster Systems Management Cookbook for pSeries, SG24-6859

(<http://www.redbooks.ibm.com/abstracts/sg246859.html?open>)

- Distributed command execution
- ▶ Monitoring with automated responses
- ▶ Predefined functions for common tasks and monitors
- ▶ Management by groups within the cluster
- ▶ Integrates with NIM for installation of nodes and software updates
- ▶ Security configuration across the cluster is performed automatically
- ▶ Software diagnostic tools for analyzing software components and servers
- ▶ Remote hardware control
- ▶ Fully scriptable command line
- ▶ Role-based access control for administrators
- ▶ Web-based management
- ▶ Ability to create custom power control methods, console methods, MAC methods, postinstall scripts, CFM prescripts and postscripts, sensors, conditions, responses, and probes
- ▶ Optional HA management server to remove single point of failure (SPOF) for the cluster manager

CSM is installed as part of AIX 5L with a 60-day trial license included. Common uses for CSM include Web server farms, high-performance computing (HPC) clusters, and large groupings of machines that benefit from a single point of management.

CSM is differentiated from other cluster management solutions:

- ▶ Supports the installation and updating of software to System x™ and System p Linux and AIX 5L
- ▶ Controls the installation of Linux and AIX 5L
- ▶ Provision of power status, hardware status, information, and diagnostic probes
- ▶ Provision of hardware monitoring and application events that can be responded to automatically
- ▶ Provision of a single point of control for AIX 5L and Linux nodes with a single consistent interface for the administrator
- ▶ Automatic set up of security for the cluster using OpenSSH or remote shell
- ▶ CSM monitoring infrastructure can be easily customized to suit customer requirements
- ▶ Modular design and the use of open source tools

- ▶ Commands can be run across the entire cluster or a subset of the cluster
- ▶ CSM can synchronize files across the cluster or a subset of the cluster

Additional clustering software that can be used with CSM include, but is not limited to:

- ▶ IBM General Parallel File System (GPFS)
- ▶ Parallel Operating Environment (POE) for AIX 5L

Cluster Systems Management Cookbook for pSeries, SG24-6859, covers a wide range of topics including the introduction to CSM, installation, advanced features, cluster administration, and HA management server.

CSM product manuals are located on the Web at:

<http://www-03.ibm.com/servers/eserver/pseries/library/clusters/aix.html>

For an overview of CSM, refer to the following Web site:

<http://www-03.ibm.com/servers/eserver/clusters/software/csm.html>



Troubleshooting

This chapter describes the differences in troubleshooting between Solaris and AIX 5L.

This chapter discusses the following topics:

- ▶ 16.1, “The booting process” on page 430
- ▶ 16.2, “Core files” on page 433
- ▶ 16.3, “Crash or system dumps” on page 436
- ▶ 16.4, “Logs” on page 438
- ▶ 16.5, “File systems” on page 440
- ▶ 16.8, “Packages” on page 443
- ▶ 16.9, “Root password recovery” on page 443
- ▶ 16.10, “Network” on page 445
- ▶ 16.11, “Tracing the system and user processes” on page 447

16.1 The booting process

Sometimes a system does not boot properly. It might hang at a point in the boot process or reboot continuously.

16.1.1 Boot troubleshooting: Solaris

In Solaris, you can perform interactive boots, device reconfiguration boots, single-user boots, and verbose boots to correct a faulty system that does not boot anymore. If the system is severely damaged, and the file systems are corrupted, you can boot from an external device such as a CD, a DVD, or the network, to repair the system.

Solaris logs the boot process to a log file only if `/etc/syslog.conf` is configured to record `kern.debug` and higher messages.

16.1.2 Boot troubleshooting: AIX 5L

In AIX 5L, messages from the boot process are automatically logged to `/var/adm/ras/bootlog`.

In the event that the system does not boot at all, refer to the AIX 5L V5.3 Installing AIX 5L manual, particularly the section titled “Troubleshooting a system that does not boot from the hard disk”.

This enables you to get a system prompt so that you can attempt to recover data from the system or perform corrective action that enables the system to boot from the hard disk¹.

Notes: This procedure is intended only for experienced administrators who have knowledge of how to boot or recover data from a system that is unable to boot from the hard disk. Most administrators must not attempt this procedure, and instead follow local problem reporting procedures.

This procedure is not intended for administrators who have just completed a new installation, because the system will not contain data that has to be recovered. If you are unable to boot from the hard disk after completing a new installation, follow your local problem reporting procedures.

¹ Instructions are from AIX 5L V 5.3 Installing AIX manual.

The following steps summarize the procedure for accessing a system that will not boot:

1. Boot the system from Volume 1 of the Base Operating System (BOS) CD-ROM or a bootable tape 2.
2. Select **Maintenance Options**.
3. Recover data or perform corrective action using the system prompt.

Light-emitting diode codes in AIX 5L

When booting, you can observe the different light-emitting diode (LED) codes on the LED panel of the machine at different boot stages. These codes are useful in debugging any problem that might arise when booting. The boot procedures are implemented in different ways, depending on the type of the AIX 5L machine.

There are mainly two types of machines:

- ▶ The RS/6000 family of machines was launched in 1990 and has, over the years, changed to adopt new technology as it becomes available. The first RS/6000 machines were based around the Micro Channel Architecture (MCA) and had a number of features common to each machine in the range, in particular, a three-digit LED and a three-position key mode switch.
- ▶ In recent years, the RS/6000 family has migrated to Peripheral Component Interconnect (PCI) bus technology. Initial machines of this type (7040 and 7248) did not have the three-digit LED or three-position key mode switch of the earlier MCA machines. Subsequent PCI machines have LED displays or liquid crystal displays (LCD), but none have the three-position key mode switch.

Following are some of the LED codes that are displayed on MCA systems:

- ▶ 292
Initializing a Small Computer System Interface (SCSI) adapter. Required to run the disk containing AIX 5L.
- ▶ 252
Locating the diskette drive or reading from a bootable diskette media
- ▶ 243 or 233
Booting from a device listed in the nonvolatile random access memory (NVRAM) boot list. Usually hdisk0, a bootable CD-ROM, or an mksysb tape.
- ▶ 551
This is an indication that all the devices in the machine are configured correctly and the machine is ready to vary on the root volume group.

- ▶ 517 or 553
After these two LEDs are displayed, any problem that is experienced is more than likely to be AIX 5L-related as opposed to hardware-related.
- ▶ 581
TCP/IP configuration is taking place. If this number stays on the LED panel for a long time, look at your TCP/IP settings and routing information after you are able to log in to the system.
- ▶ c31
This code indicates that the system is awaiting input from you on the keyboard. This is usually encountered when booting from a CD-ROM or an mksysb tape. This is normally the dialog to select the system console.
- ▶ c32 or c33
These codes tell you that the boot process is nearly complete. Shortly afterwards, you must see the output on the panel from the AIX 5L boot process starting various software subsystems.
- ▶ 551, 555, or 557
If the system hangs at these LED codes, the known causes might be:
 - A corrupted file system
 - A corrupted journaled file system (JFS or JFS2) - log device
 - Failing fsck (file system check) caused by a bad file system helper
 - A bad disk in the machine that is a member of the rootvg
- ▶ 552, 554, or 556
If the system hangs at these LED codes, the known causes might be:
 - A corrupted file system
 - A corrupted journaled file system (JFS or JFS2) - log device
 - A bad IPL device record or bad IPL device magic number. (The magic number indicates the device type.)
 - A corrupted copy of the Object Data Manager (ODM) database on the boot logical volume.
 - A hard disk in an inactive state in the root volume group.

For a complete list of LED and other error and information codes, refer to the IBM System p and AIX 5L Information Center on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/index.jsp>

The following publications also contain a listing of the codes:

- ▶ *RS/6000 & eServer pSeriesDiagnostics Information for Multiple Bus Systems*, SA38-0509-23
- ▶ *IBM Certification Study Guide eServer p5 and pSeries Administration and Support for AIX 5L Version 5.3*, SG24-7199 (Section 4.4.3 “Common boot LED codes”)

16.2 Core files

Core files are created when an application or process terminates abnormally. These core files are used by the developers and support staff to determine the cause of abnormal termination, and to troubleshoot the respective program that generated the core file.

16.2.1 Management of core files: Solaris

In Solaris, core files are managed with the `coreadm` command. You can have a per-process core file path that is enabled by default, and creates a core file in the current directory. In addition, you can create a global core file path that is disabled by default, and creates another core file in the global directory you specify.

The per-process core is created with read and write rights only for the owner of the process. The global core is created with read and write rights for the root only.

You can also expand the default core file name to include useful information such as the process identification number (PID), Effective User Identifier (EUID), and Effective Group ID (EGID).

Setuid programs do not produce a core by default, but this behavior can be changed with the `coreadm` command. You can then use the `pstack`, `pmap`, `pldd`, `pflags`, and `pcrred` tools to show information about the core file. You can inspect core files with the `mdb` utility.

16.2.2 Management of core files: AIX 5L

In AIX 5L V5.3, AIX 5L provides the **chcore** command as the interface for changing core file administration settings. The configurable settings for **chcore** are:

- ▶ **-c**: {on | off | default}
Setting for core compression
- ▶ **-d**
Changes the default setting for the system
- ▶ **-l path**
Directory path for stored core files
- ▶ **-n** {on | off | default}
Setting for core naming, for example, *core.pid.ddhhmmss*, where:
 - *pid*: process ID
 - *dd*: Day of the month
 - *hh*: Hours
 - *mm*: Minutes
 - *ss*: Seconds
- ▶ **-p** {on | off | default}
Setting for core location
- ▶ **-R registry**
Specifies the loadable I&A module.

16.2.3 Determining which process failed and caused a core file

In both Solaris and AIX 5L, when troubleshooting system problems that have dumped core, you must determine which process caused the core file.

On Solaris, you can determine which process caused a core file with the **file** command, as shown in Example 16-1.

Example 16-1 Using the Solaris file command to examine a core file

```
# ls -l core*  
-rw-r--r--  1 root    other    330102876 May 16 09:12 core.12606  
# file core.12606  
core.12606:      ELF 64-bit MSB core file SPARCV9 Version 1, from  
'dmserv'
```

Likewise, on AIX 5L, the **file** command shows you which process caused the core file, as shown in Example 16-2.

Example 16-2 Using the AIX 5L file command to examine a core file

```
# ls -l core*
-rw-r--r--  1 root    system    4624347 May 16 09:30 core.245080
# file core.245080
core.245080: AIX core file 32-bit, IBM.CSMAgentRMD
```

Table 16-1 shows core file administration.

Table 16-1 .Core file administration

Task	Solaris	AIX 5L
Modify core file settings, for example, name	coreadm	chcore (new w/AIX 5L V5.3)
Determine which process caused the core	file <i>core-filename</i>	file <i>core-filename</i>
Control size of core file	<ul style="list-style-type: none"> ▶ coreadm ▶ ulimit -c ▶ vi /etc/system 	<ul style="list-style-type: none"> ▶ chcore ▶ ulimit -c ▶ vi /etc/security/limits
Force a running process to dump core (without stopping the process)	gcore	gencore
Gather core file and associated binaries and libraries	explorer (obtained from SunSolve)	snapcore
Examine core file	<ul style="list-style-type: none"> ▶ pstack ▶ pmap ▶ pidd ▶ pflags and ▶ pcrred 	<ul style="list-style-type: none"> ▶ adb ▶ dbx
Debugger	<ul style="list-style-type: none"> ▶ adb ▶ gdb ▶ mdb 	<ul style="list-style-type: none"> ▶ adb ▶ dbx
Trace a process	truss	truss^a

a. Refer to 16.11, “Tracing the system and user processes” on page 447.

16.3 Crash or system dumps

When a system crashes, it can save an image of the physical memory at the time of the crash on the default dump device for further analysis. System crashes can be because of software problems or hardware problems.

Note: Crash/system dumps can occur spontaneously, they can be induced intentionally when the system is still accessible at a command level, and they can be *forced* by turning the key mode switch to the Service position and pressing the function keys Ctrl+Alt_Num_Pad 1.

Management of crash dump files: Solaris

In Solaris, when a system crashes, it writes a copy of the physical memory to the dump device. After reboot, the **savecore** command is executed to save the crash dump files from the dump device to the configured savecore directory in the form of `unix.X` and `vmcore.X` files, where X is the dump sequence number. The crash dump files are used by Sun support to diagnose the problem. The default directory for saving the crash dump files is `/var/crash/hostname`.

You can inspect the crash dump files with the `mdb` utility. The default dump device is the swap space of the system, but it can be changed to a separate partition. You can generate a crash dump of a running system with the **savecore -L** command if you configure a separate dump partition. To manage the crash dump configuration and the content, use the **dumpadm** command.

In Solaris, there is no OS-level command to cause a system dump.

Management of crash dump files: AIX 5L

In AIX 5L, when a system crashes, it writes a copy of the physical memory to the dump device specified by the **sysdumpdev** command or, by default, to `/dev/hd6` (default primary dump device) or `/dev/sysdumpdev` (default secondary dump device).

If you have access to the console or tty, you can induce a system dump on AIX 5L with the **sysdumpstart** command. If you cannot access the console or tty, try one of the following methods to induce a system dump:

- ▶ If there is a keyboard attached to the system unit, start a dump by using the dump key sequences (Ctrl+Alt_Num_Pad 1 and Ctrl+Alt_Num_Pad 2). The dump key sequences allow you to start a dump to the primary or the secondary dump device.
- ▶ Use the Reset button to start a dump to the primary dump device. To start a dump, turn the Key Mode switch to the Service position and press the Reset button.

As in Solaris, the **savecore** command on AIX 5L is executed at reboot in order to move the dump files from the dump device to the specified directory.

By default, in AIX 5L, a cron job runs a **dumpcheck** at 3 p.m. each day to determine if sufficient disk space is available to store a system dump on the dump device and copy it to the target location. Example 16-3 shows how to ensure that a scheduled dump check is in force at your site.

Example 16-3 Default dump check cron job

```
# crontab -l | grep dump
# 0 15 * * * /usr/lib/ras/dumpcheck >/dev/null 2>&1
```

For more information, refer to the chapter “System Dump Facility” in the System p AIX 5L Collaboration Center available on the Web at:

<http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp>

Table 16-2 and Table 16-3 show the main Solaris and AIX 5L crash dump management and related network analysis tools.

Table 16-2 Crash/system dump management

Topic	Solaris	AIX 5L
Crash dump utilities	<ul style="list-style-type: none"> ▶ dumpadm ▶ savecore 	<ul style="list-style-type: none"> ▶ sysdumpdev ▶ sysdumpstart
Crash configuration	view /etc/dumpadm.conf	sysdumpdev -l
Crash analyzing tools	mdb	pstat
Crash dump default store directory	/var/crash	/var/adm/ras
Generate a system dump	N/A	<ul style="list-style-type: none"> ▶ sysdumpstart ▶ smit dump
Save a crash dump that has already been generated	savecore	savecore
System dump file administration	dumpadm	sysdumpdev
Examine a system dump	mdb	<ul style="list-style-type: none"> ▶ /usr/lib/errdead ▶ kdb

Table 16-3 Network analysis tools

Task	Solaris	AIX 5L
Browse network traffic	ethereal	ethereal

Task	Solaris	AIX 5L
Dump and analyze network traffic	<ul style="list-style-type: none"> ▶ tethereal ▶ snoop 	tcpdump
Network crash dump utilities	mdb	trcdead
Network crash storage location	/var/crash/hostname	/var/adm/ras

16.4 Logs

System logs are useful for troubleshooting. The logs are the first thing you must check if something goes wrong. Even if the system is stable and running well, it is a good idea to inspect the system logs periodically. There might be an indication of symptoms that will potentially affect the availability of the system.

16.4.1 Syslogging

Both Solaris and AIX 5L use **syslogd** to record various system warnings and errors. The syslogd daemon is configured by default to send the most critical messages to the console in addition to logging them to files. In both the systems, use `/etc/syslog.conf` to configure where system messages will be logged. Both the systems provide log rotation capabilities to prevent the log files from growing too big.

Chapter 3, “Operating system installation” on page 47 of this IBM Redbook provides more details about the specific differences in logging between Solaris and AIX 5L, and describes how log file rotation is performed on each system.

Important: By default, not much is being logged through the syslog daemon, that is, the `/etc/syslog.conf` file in the default settings does not capture much logging except perhaps to the console. Remember that if problems occur and there is no logging in place at that time, it is necessary to modify the `/etc/syslog.conf` file, restart/refresh/kill -HUP the syslogd process, and wait for the problem to recur in order to capture the logging, if indeed any logging of the event did take place.

16.4.2 Differences in logging between Solaris and AIX 5L

In addition to the syslog daemon used in Solaris and all the other UNIX systems, AIX 5L provides management and error logging of hardware, operating systems, application messages, and errors through the use of the Error Logging Subsystem. In AIX 5L, /usr/lib/errdemon constantly checks the /dev/error file, analyzing its contents and writing the data to the /var/adm/ras/errlog. When the **errpt** command is invoked, it reads the /var/adm/ras/errlog and reports to standard out in the manner determined by the error notification database /etc/objrepos/errnotify.

Example 16-4 shows how to query the settings of AIX 5L errdemon.

Example 16-4 Query the settings of AIX 5L errdemon

```
# /usr/lib/errdemon -l
Error Log Attributes
-----
Log File           /var/adm/ras/errlog
Log Size           1048576 bytes
Memory Buffer Size  32768 bytes
Duplicate Removal  true
Duplicate Interval 10000 milliseconds
Duplicate Error Maximum 1000
```

Example 16-5 shows the AIX 5L **errpt -a** output.

Example 16-5 AIX 5L errpt -a output

```
LABEL:JFS_FS_FULL
IDENTIFIER:369D049B

Date/Time:      Tue Jan 17 11:16:31 EST
Sequence Number: 323
Machine Id:     00C15EEF4C00
Node Id:        aaaco11
Class:          0
Type:           INFO
Resource Name:  SYSPFS

Description
UNABLE TO ALLOCATE SPACE IN FILE SYSTEM

Probable Causes
FILE SYSTEM FULL
```

Recommended Actions
 USE FUSER UTILITY TO LOCATE UNLINKED FILES STILL REFERENCED
 INCREASE THE SIZE OF THE ASSOCIATED FILE SYSTEM
 REMOVE UNNECESSARY DATA FROM FILE SYSTEM

Detail Data
 MAJOR/MINOR DEVICE NUMBER
 000A 0004
 FILE SYSTEM DEVICE AND MOUNT POINT
 /dev/hd4, /

Note: It is possible to make the **errdemon** write its **errprt** output to the syslog output file. For details, refer to 1.5, “Errprt and syslog in AIX 5L” on page 15.

Table 16-4 summarizes how to manage syslog in Solaris and AIX 5L.

Table 16-4 *Managing syslog*

Task	Solaris	AIX 5L
Daemon for syslog	<code>/usr/sbin/syslogd</code>	<code>/usr/sbin/syslogd</code>
Configuration file for syslog	<code>/etc/syslog.conf</code>	<code>/etc/syslog.conf</code>
Refresh syslogd after a change to the configuration file	<code>kill -HUP syslogd-pid</code>	<code>refresh -p syslogd-pid</code>
Diagnostics messages for bootup problems	<code>/var/adm/messages</code> (if kern.debug messages are being logged)	<code>/var/adm/ras/bootlog</code>

16.4.3 Application logging

Most applications that run on Solaris and AIX 5L produce log files. Consult the documentation for the specific application to find out where they are and how to interpret them.

16.5 File systems

If your server crashes, or has somehow powered off without actually flushing the buffer and unmounting the file systems, you will have some *dirty* file systems and might end up with inconsistencies in those file systems. This is the reason why, on each boot, the initialization scripts run **fsck** on selected file systems from

`/etc/vfstab` in Solaris and `/etc/filesystems` in AIX 5L. If they are not unmounted properly, the **fsck** program scans for inconsistencies. Usually, the **fsck** program runs in a noninteractive mode, automatically fixing minor inconsistencies. However, if there are some major problems, it switches to manual mode and lets the operator make the decisions.

If you are in a situation where you have to manually fix the file system with **fsck**, it is a good idea to back up the partition before attempting to fix the file system, especially if you have valuable data on it. In both the operating systems, you can run **fsck -y** to automatically fix any type of problem, be it minor or major.

16.5.1 Journaled file systems

Generally, when a system crashes or is shut down abruptly, the mounted file systems are considered dirty and **fsck** will have to be used. With the introduction of Journaled File Systems in the earlier versions of both Solaris and AIX 5L, a transactional log called a journal is created to preserve the integrity of the file system.

On AIX 5L, all the file systems are journaled by default. On Solaris, file systems that are greater than one tera byte in size are journaled automatically, but smaller file systems are not. To enable journaling on those smaller file systems on Solaris, put a logging option in the mount options column of the intended file system in the `/etc/vfstab` file.

Even for journaled file systems, it is a good practice to perform a forced **fsck -f** at scheduled intervals in order to ensure that everything is fine. This is because journaling a file system does *not* prevent a kernel or other software bug from causing a file system inconsistency.

16.5.2 Remote file systems

You might notice that a remote file system did not get mounted at bootup, or that you are not able to mount it manually. Consider the following troubleshooting methods in both Solaris and AIX 5L.

In the NFS server, perform the following tasks:

1. Check `/etc/dfs/dfstab` (Solaris) or `/etc/exports` (AIX 5L) to ensure that the file systems are being shared or exported correctly. If not, correct the configuration files and use **share** or **exportfs** (for both Solaris and AIX 5L) to share or export the file system.
2. Verify that the `rpcbind` (Solaris) or `portmap` (AIX 5L) service is running.
3. Verify that `nfsd`, the NFS server daemon, is running.

4. Display the registered portmap processes.

In the client, perform the following tasks:

1. Use the **showmount -e *nfsserver*** command to display the exported subdirectories of the server.
2. Check `/etc/vfstab` (Solaris) or `/etc/filesystems` (AIX 5L) for the mount options.
3. Check `/etc/mnttab` (Solaris) or **smit mount** (AIX 5L) for the currently mounted file systems.
4. Ping the target server.

Table 16-5 shows some of the commands used in this process.

Table 16-5 RFS troubleshooting commands

Task	Solaris	AIX 5L
Display shared or exported file systems	share	exportfs
Display mounted file systems	df	df
Display detailed information about mounted file systems	mount	mount
Display NFS server's export list	showmount -e <i>hostname</i> dfshares	showmount -e <i>hostname</i>
Display registered rpcbind/portmap processes	rpcinfo -p <i>hostname</i>	rpcinfo -p <i>hostname</i>
Display open files	lsof (freeware)	lsof (freeware)

16.6 Software Redundant Array of Independent Disks

For troubleshooting problems with RAID devices, refer to Chapter 6, “Device management” on page 157, Chapter 4, “Disks and file systems” on page 91, and Chapter 12, “Monitoring and performance” on page 359.

16.7 Logical volumes

For troubleshooting problems with logical volumes, refer to Chapter 4, “Disks and file systems” on page 91 and Chapter 12, “Monitoring and performance” on page 359.

16.8 Packages

For troubleshooting problems with software packages, refer to Chapter 3, “Operating system installation” on page 47 and Chapter 5, “Software management” on page 133.

16.9 Root password recovery

There are cases when the root password is lost. This section explains how to change the root password in such instances.

Root password recovery: Solaris

In Solaris, perform the following steps to change a lost root password:

1. Stop the system or perform a power off and on cycle.
2. Boot in single-user mode from a CD-ROM/DVD or from a network boot/install server.
3. Mount the root (/) file system in read/write mode.
4. Remove the root password from the /etc/shadow file and save the file.
5. Unmount the root file system.
6. Reboot the system.
7. The root password is not set. Press Enter at the password prompt when you login as root.

Root password recovery: AIX 5L

This procedure describes how to recover the access to root privileges when the system’s root password is unavailable or is unknown. This procedure requires some system downtime. If possible, schedule your downtime when it least impacts your workload to protect yourself from a possible loss of data or functionality.

The information in this how-to was tested using AIX 5L V5.2. If you are using a different version or level of AIX 5L, the results you obtain might vary significantly.

Perform the following tasks:

1. Insert the product media for the same version and level as the current installation, into the appropriate drive.
2. Power on the machine.

3. When the screen of icons appears, or when you hear a double beep, press the F1 key repeatedly until the System Management Services menu appears.
4. Select **Multiboot**.
5. Select **Install From**.
6. Select the device that holds the product media and then select **Install**.
7. Select the **AIX Version** icon.
8. Define your current system as the system console by pressing the F1 key and then press Enter.
9. Select the number of your preferred language and press Enter.
10. Choose **Start Maintenance Mode for System Recovery** by typing 3 and press **Enter**.
11. Select **Access a Root Volume Group**. A message displays, explaining that you will not be able to return to the Installation menus without rebooting, if you change the root volume group at this point.
12. Type 0 and press Enter.
13. Type the number of the appropriate volume group from the list and press Enter.
14. Select **Access this Volume Group and start a shell** by typing 1 and press Enter.
15. At the # (number sign) prompt, type the **passwd** command in the command line prompt to reset the root password (Example 16-6).

Example 16-6 Using the passwd command

```
# passwd
Changing password for "root"
root's New password:
Enter the new password again:
```

16. To write everything from the buffer to the hard disk, and reboot the system, type the following:

```
sync;sync;sync;reboot
```

When the login screen appears, the password you set in step 15 must now allow access to the root privileges.

16.10 Network

The basic network monitoring commands are described in Chapter 7, “Network services” on page 183. Although networking problems can be hard to diagnose, sophisticated tools are available on both Solaris and AIX 5L systems.

The Solaris snoop command

The **snoop** command (Example 16-7) allows you to capture and inspect the network packages for troubleshooting problems or producing reports on network traffic at your site. It shows both the inbound and the outbound network traffic.

Example 16-7 Example of the snoop command

```
# snoop
Using device /dev/ce (promiscuous mode)
  dragoon -> thishost      TCP D=22 S=3470 Ack=40140624 Seq=1231624672 Len=0
Win=16160
  thishost -> dragoon      TCP D=3470 S=22 Push Ack=1231624672 Seq=40140624
Len=136 Win=49640
  dragoon -> thishost      TCP D=22 S=3470 Ack=40140760 Seq=1231624672 Len=0
Win=17520
prov001.xyz.com -> (broadcast) ARP C Who is 8.7.3.102, kingston.xyz.com ?
prov001.xyz.com -> (broadcast) ARP C Who is 8.7.3.214, 8.7.3.214 ?
berlin.berlin.xyz.com -> (broadcast) ARP C Who is 8.7.3.31, prov007.xyz.com ?
berlin.berlin.xyz.com -> (broadcast) ARP C Who is 8.7.3.116, lpar06.xyz.com ?
prov009.xyz.com -> 8.7.3.45  UDP D=12347 S=12347 LEN=408
  thishost -> dragoon      TCP D=3470 S=22 Push Ack=1231624672 Seq=40140760
Len=132 Win=49640
  thishost -> dhcp001.xyz.com DNS C 45.3.7.8.in-addr.arpa. Internet PTR ?
dhcp001.xyz.com -> thishost      DNS R 45.3.7.8.in-addr.arpa. Internet PTR
prov001.xyz.com.
  thishost -> dhcp001.xyz.com DNS C prov001.xyz.com. Internet Addr ?
dhcp001.xyz.com -> thishost      DNS R prov001.xyz.com. Internet Addr 8.7.3.39
  thishost -> dhcp001.xyz.com DNS C 102.3.7.8.in-addr.arpa. Internet PTR ?
dhcp001.xyz.com -> thishost      DNS R 102.3.7.8.in-addr.arpa. Internet PTR
kingston.xyz.com.
```

The AIX 5L iptrace and ipreport commands

In AIX 5L, the **iptrace** command creates a binary trace file that can then be interpreted by the **ipreport** command (Example 16-8).

Important: The `iptrace` command starts a background process and continues to run, building the binary trace file, until you issue a `kill -15 iptrace-pid`. Remember that `^C` does *not* stop `iptrace`.

Example 16-8 Example of iptrace/ipreport

```
# iptrace /tmp/network-trace
# [319506]
^C
# kill -15 319506
# iptrace: unload success!

# ipreport /tmp/network-trace
IPTRACE version: 2.0

====( 60 bytes received on interface en0 )==== 17:00:00.538246379
ETHERNET packet : [ 00:09:12:48:3c:02 -> ba:8e:30:00:40:02 ] type 800
(IP)
IP header breakdown:
  < SRC =      8.7.3.151 > (dragoon)
  < DST =      8.7.2.174 > (brazos.xyz.com)
  ip_v=4, ip_hl=20, ip_tos=0, ip_len=40, ip_id=16252, ip_off=0 DF
  ip_ttl=127, ip_sum=a009, ip_p = 6 (TCP)
TCP header breakdown:
  <source port=3166(qrepos), destination port=23(telnet) >
  th_seq=332340814, th_ack=3852040861
  th_off=5, flags<ACK>
  th_win=17478, th_sum=b07a, th_urp=0

====( 66 bytes transmitted on interface en0 )==== 17:00:00.538290634
ETHERNET packet : [ ba:8e:30:00:40:02 -> 00:09:12:48:3c:02 ] type 800
(IP)
IP header breakdown:
  < SRC =      8.7.2.174 > (brazos.xyz.com)
  < DST =      8.7.3.151 > (dragoon)
  ip_v=4, ip_hl=20, ip_tos=0, ip_len=52, ip_id=31489, ip_off=0 DF
  ip_ttl=60, ip_sum=a778, ip_p = 6 (TCP)
TCP header breakdown:
  <source port=23(telnet), destination port=3166(qrepos) >
  th_seq=3852040861, th_ack=332340814
  th_off=5, flags<PUSH | ACK>
  th_win=65535, th_sum=cc8d, th_urp=0
00000000      23205b32 39353130 325d0d0a      |# [295102].. |
```

Table 16-6 shows troubleshooting for network problems.

Table 16-6 Troubleshooting: Network problems

Task	Solaris	AIX 5L
Display interface settings	<code>ifconfig</code>	<code>ifconfig</code>
Display interface status and statistics	<code>netstat -i</code>	<code>netstat -i</code>
Configure interface	<code>ifconfig</code>	<code>ifconfig</code>
Check various network statistics	<code>netstat</code>	<code>netstat</code>
Check DNS resolver	<code>view /etc/resolv.conf</code>	<ul style="list-style-type: none"> ▶ <code>view /etc/resolv.conf</code> ▶ <code>smit namerslv</code>
Check name services configuration	<code>view /etc/nsswitch.conf</code>	<code>view /etc/netsvc.conf</code>
Display kernel network parameters	<ul style="list-style-type: none"> ▶ <code>ndd /dev/ip (\?)parameter</code> ▶ <code>ndd /dev/tcp (\?)parameter</code> 	<code>no -a</code>
Configure kernel network parameters	<code>ndd -set driver parameter</code>	<code>no -option Tunable</code>
Check for network link	<code>ndd driver link_status</code>	<code>netstat -v grep -i link</code>
Query DNS	<ul style="list-style-type: none"> ▶ <code>nslookup</code> ▶ <code>dig</code> 	<code>nslookup</code>
Check routing table	<code>netstat -r</code>	<code>netstat -a</code>
Check ARP entries	<code>arp -a</code>	<code>arp -a</code>
Test for connectivity	<code>ping</code>	<code>ping</code>
Check IP path	<code>traceroute</code>	<code>traceroute</code>
Capture network packets	<code>snoop</code>	<code>iptrace</code>

16.11 Tracing the system and user processes

Solaris provides the `ps` and `top` commands (`top` is optionally installable on Solaris from the Companion CD) that are used to display the state of the running processes. The `ps` command gives you a point-in-time snapshot of the system and application processes. The `top` command gives you an iterative and interactive display of the system processes.

Whether you use the **ps** or the **top** command, the important columns in the output of these commands to monitor are %CPU, STAT, START or STIME, and TIME.

AIX 5L too provides the **ps** and **topas** commands.

Refer to Chapter 12, “Monitoring and performance” on page 359 for more information about and examples of **ps**, **top**, and **topas**.

Table 16-7 provides an overview of the command sets used in troubleshooting the system and user processes.

Table 16-7 Troubleshooting: System and user processes

Task	Solaris	AIX 5L
Trace system calls and signals	truss	truss
Print shared library dependencies	▶ ldd ▶ dump	▶ ldd ▶ dump
Report IPC status	ipcs	
Display and manage system resources available to a user or process	▶ ulimit ▶ view /etc/system	▶ ulimit ▶ view /etc/security/limits
Identify which user or process is using a file or socket	fuser	fuser
Send signals to processes	kill pkill	kill
List current processes	ps	ps
List current processes in an interactive, iterative format	top (on companion CD)	topas
Report system activity	sar	sar
Display virtual memory statistics	vmstat	vmstat
Display I/O statistics	iostat	iostat
Display system error log	dmesg	errpt
Perform memory test	N/A	rmss

16.12 Using the truss command in troubleshooting

In both Solaris and AIX 5L, the **truss** command is useful for troubleshooting because it allows you to see all the tasks a process is performing when it executes, including system calls, dynamically loaded user-level function calls, received signals, and incurred machine faults.

You can start a process with **truss**, so that you see the startup (useful for troubleshooting startup problems), or you can use **truss** as an existing process (useful for troubleshooting).

Because “trussing” a process adds load to a system both in terms of CPU and disk usage if you are saving the output to a file, you should use it only for troubleshooting, turning it on to capture a specific event, and turning it off as soon as possible after the event. If trussing must be performed for a longer period of time, use **top** (Solaris) or **topas** (AIX 5L) to monitor the resources used by the process you are tracking *and* the **truss** process.

Important: If you start a process with **truss**, stopping the **truss** stops the process. However, if you start **truss** on an already running process, you can kill **truss** without stopping the process.

Because the **truss** commands on Solaris and AIX 5L are almost identical, the examples provided here are from the **truss** run on AIX 5L.

Using the truss command

Example 16-9 shows the use of **truss** to trace a command finding every file on the system and sorting them by size. In this case, the truss option only uses the **-o** option to direct the output to a file.

In this example, the **truss** with no options wrote a 68mb file of output to `/tmp/truss.out`.

Example 16-9 Example of truss output

```
# truss -o /tmp/truss.out find / -type f -exec ls -l {} \; | sort -nbr +9
execve("/usr/bin/find", 0x2FF22AB4, 0x2FF22ADC)  argc: 9
__loadx(0x010001C0, 0x2FF1ABE0, 0x00003E80, 0xF11B588C, 0x00000000) = 0x201BAD00
__loadx(0x02000000, 0x2FF1EB40, 0x00003E80, 0x201BAD00, 0x00000000) = 0x00000000
__loadx(0x07000000, 0xF11B5880, 0x00000003, 0x201BAD00, 0x00000000) = 0x201C9C28
__loadx(0x07000000, 0xF11B589C, 0x00000003, 0x201BAD00, 0x00000000) = 0x201C9C34
sbrk(0x00000000) = 0x201CF000
sbrk(0x00010010) = 0x201CF000
__loadx(0x02000000, 0x2FF1EB40, 0x00003E80, 0x00000000, 0x201CF008) = 0x00000000
```

```

loadquery(2, 0x201CF0C8, 0x00001000)          = 0
kfcntl(0, F_GETFL, 0x00000000)                = 67110914
kfcntl(1, F_GETFL, 0x00000000)                = 1
kfcntl(2, F_GETFL, 0x00000000)                = 67110914
kfcntl(2, F_GETFL, 0x00000000)                = 67110914
__loadx(0x01070380, 0x2FF1AB70, 0x00003E80, 0x20000A10, 0x00000000) = 0xF119C050
__loadx(0x0A040000, 0xD0388668, 0x2FF22FFC, 0x0000D0B2, 0x00000000) = 0x00000000
__loadx(0x0A040000, 0xD038868C, 0x2FF22FF8, 0x0000D0B2, 0x00000000) = 0x00000000
loadquery(2, 0x201CF0C8, 0x00001000)          = 0
__loadx(0x02000200, 0x201CA908, 0x00003E80, 0xF119C050, 0x00000000) = 0x00000000
__loadx(0x07000000, 0x200008E4, 0x00000001, 0xF119C050, 0x201D0678) = 0xF11DF4E4
statx(".", 0x2FF228D0, 76, 0)                  = 0
open(".", O_RDONLY)                             = 3
getdirent64(3, 0x201D0718, 4096)               = 2704
klseek(3, 0, 0, 0x00000000)                    = 0
kfcntl(3, F_GETFD, 0x00000000)                 = 0
kfcntl(3, F_SETFD, 0x00000001)                 = 0
__loadx(0x07000000, 0x20000908, 0x00000001, 0xF119C050, 0x201D0678) = 0xF11DF4F0
close(3)                                         = 0
_sigaction(30, 0x2FF229C0, 0x2FF229D0)         = 0
unamex(0x20001D08)                              = 0
statx(".", 0x2FF228D0, 76, 0)                  = 0
open(".", O_RDONLY)                             = 3
getdirent64(3, 0x201D1738, 4096)               = 2704

```

As you can see from the output shown in Example 16-10, when **topas** was running along with **truss**, the **truss** command was using more of the CPU than the **find** command being trussed.

Example 16-10 Topas output when the truss was running

```

Topas Monitor for host:   comaix12              EVENTS/QUEUES  FILE/TTY
Wed May 17 13:47:41 2006 Interval: 2          Cswitch    5137  Readch  3064.4K
                                                            Syscall   26390  Writech  66909
Kernel  47.0  |#####| Reads    2490  Rawin    0
User    14.2  |#####| Writes   5521  Ttyout   374
Wait    0.0  |#####| Forks    95   Igets    0
Idle    38.8  |#####| Execs    94   Namei    1997
                                                            Runqueue   1.0  Dirblk   0
Network KBPS  I-Pack  O-Pack  KB-In  KB-Out  Waitqueue  0.0
en0     0.7   3.0    0.5    0.3    0.4
sit0    0.0   0.0    0.0    0.0    0.0  PAGING
lo0     0.0   0.0    0.0    0.0    0.0  Faults  13157  Real,MB  4095
                                                            Steals     0   % Comp   27.4
Disk    Busy%  KBPS    TPS  KB-Read  KB-Writ  PgpsIn    0   % Noncomp  73.5

```

hdisk0	1.5	40.0	2.5	0.0	40.0	PgspOut	0	% Client	37.8
hdisk1	0.0	0.0	0.0	0.0	0.0	PageIn	0		
hdisk2	0.0	0.0	0.0	0.0	0.0	PageOut	10	PAGING SPACE	
cd0	0.0	0.0	0.0	0.0	0.0	Sios	2	Size,MB	2560
								% Used	1.6
Name	PID	CPU%	PgSp	Owner		NFS (calls/sec)		% Free	98.3
truss	29840	18.5	0.4	root		ServerV2	0		
find	26286	4.8	0.3	root		ClientV2	0	Press:	
topas	23198	0.2	1.5	root		ServerV3	0	"h" for help	
java	14386	0.2	387.1	root		ClientV3	0	"q" to quit	
syncd	4706	0.0	0.6	root					
db2dasst	21696	0.0	2.6	db2					
muxatmd	9654	0.0	0.5	root					
db2fmcd	18098	0.0	0.8	root					
java	14016	0.0	157.0	root					
gil	2580	0.0	0.1	root					
db2dasrr	17906	0.0	2.1	dasusr1					

Example 16-11 shows an example of **truss** with multiple options. In this example, **truss** saves and reports on much more data for troubleshooting than in Example 16-10 because it is printing the environment information and showing the forked processes.

In this case, the **find** command failed when it ran the /tmp file system out of disk space because the /tmp/truss-options.out file grew to 900 MB.

Example 16-11 Example of truss output

```
# truss -o /tmp/truss-options.out -fae -xall -rall -wall find / -type f -exec ls -l
{} \; | sort -nbr +9
24214: execve(0x2FF21DE8, 0x2FF22A9C, 0x2FF22AC4)          argc: 9
24214: argv: find / -type f -exec ls -l {} ;
24214: envp: _=/usr/bin/truss LANG=C LOGIN=root SSH_TTY=/dev/pts/0
24214:
PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:/usr/bin/X11:/sbin:/usr/local/bin:/data2/IBM/
ITM/bin:/usr/local/bin
24214: LC_FASTMSG=true CGI_DIRECTORY=/var/docsearch/cgi-bin LOGNAME=root
24214: MAIL=/usr/spool/mail/root LOCPATH=/usr/lib/nls/loc
24214: PS1=[grtaix12:root:/tmp] > CANDLEHOME=/data2/IBM/ITM
24214: DOCUMENT_SERVER_MACHINE_NAME=localhost USER=root AUTHSTATE=compat
24214: ISC_HOME=/data1/IBM/ISC601 DEFAULT_BROWSER=netscape
24214: SHELL=/usr/bin/ksh ODMDIR=/etc/objrepos
24214: JAVA_HOME=/data1/IBM/ISC601/AppServer/java DOCUMENT_SERVER_PORT=49213
24214: HOME=/home/root SSH_CONNECTION=9.3.4.151 1056 9.48.205.115 22
24214: SSH_CLIENT=9.3.4.151 1056 22 TERM=xterm MAILMSG=[YOU HAVE NEW MAIL]
```

```

24214: ITECONFIGSRV=/etc/IMNSearch PWD=/tmp
24214: DOCUMENT_DIRECTORY=/usr/docsearch/html TZ=CST6CDT
24214: ENV=/home/root/.kshrc ITECONFIGCL=/etc/IMNSearch/clients
24214: ITE_DOC_SEARCH_INSTANCE=search MAILCHECK=60
24214: A_z=! LOGNAME="*MAILCHECK
24214: NLSPATH=/usr/lib/nls/msg/%L/%N:/usr/lib/nls/msg/%L/%N.cat
24214: __loadx(0x010001C0, 0x2FF1ABE0, 0x00003E80, 0xF11B588C, 0x00000000) =
0x201BAD00
24214: __loadx(0x02000000, 0x2FF1EB40, 0x00003E80, 0x201BAD00, 0x00000000) =
0x00000000
[.....]
24214: _sigaction(0x00000002, 0x2FF189A0, 0x2FF189B0) = 0x00000000
24214: kfork() = 0x00004896
18582: kfork() (returning as child ...) = 0
18582: fchdir(3) = 0
18582: execve("/usr/bin/ls", 0x20001FF8, 0x2FF22AF4) argc: 3
18582: argv: ls -l /var/adm/cron/at.deny
18582: envp: _=/usr/bin/truss LANG=C LOGIN=root SSH_TTY=/dev/pts/0
[.....]
18582: kfcntl(1, F_GETFL, 0x00000001) = 1
18582: close(1) = 0
18582: kfcntl(2, F_GETFL, 0x200173A0) = 67110914
18582: _exit(0)
24214: kwaitpid(0x20001C88, 0xFFFFFFFF, 0x00000004, 0x00000000, 0x00000000) =
0x00004896
24214: _sigaction(0x00000003, 0x2FF189A0, 0x2FF189B0) = 0x00000000
24214: _sigaction(0x00000002, 0x2FF189A0, 0x2FF189B0) = 0x00000000
24214: statx(0x200020C0, 0x20001D98, 0x00000080, 0x00000009) = 0x00000000
24214: statx(0x200020C0, 0x20001E98, 0x000000B0, 0x00000011) = 0x00000000
24214: _sigaction(0x00000003, 0x2FF189A0, 0x2FF189B0) = 0x00000000
24214: _sigaction(0x00000002, 0x2FF189A0, 0x2FF189B0) = 0x00000000
24214: kfork() = 0x00004898
18584: kfork() (returning as child ...) = 0
18584: fchdir(3) = 0
18584: execve("/usr/bin/ls", 0x20001FF8, 0x2FF22AF4) argc: 3

```

Important: If **truss** is to be long-running, guard against running a file system out of space by wrapping the **truss** around an already running process, monitoring the size of the output file, killing the **truss** process occasionally, removing the output files, and restarting **truss**.

Example 16-12 shows the **topas** output from the **truss-with-options** command.

Example 16-12 The topas output from the truss-with-options command

Topas Monitor for host: comaix12						EVENTS/QUEUES	FILE/TTY		
Wed May 17 14:45:20 2006 Interval: 2						Cswitch	10324	Readch	7028.4K
						Syscall	46620	Writech	406.6K
Kernel	29.0	#####				Reads	6065	Rawin	0
User	29.5	#####				Writes	14147	Ttyout	242
Wait	0.0					Forks	30	Igets	0
Idle	41.5	#####				Execs	17	Namei	974
						Runqueue	1.0	Dirblk	0
Network	KBPS	I-Pack	O-Pack	KB-In	KB-Out	Waitqueue	0.0		
en0	0.8	6.5	0.5	0.5	0.3				
sit0	0.0	0.0	0.0	0.0	0.0	PAGING		MEMORY	
lo0	0.0	0.0	0.0	0.0	0.0	Faults	4431	Real,MB	4095
						Steals	216	% Comp	27.1
Disk	Busy%	KBPS	TPS	KB-Read	KB-Writ	PgspIn	0	% Noncomp	73.8
hdisk0	9.0	394.0	25.5	0.0	394.0	PgspOut	11	% Client	33.8
hdisk1	0.0	0.0	0.0	0.0	0.0	PageIn	0		
hdisk2	0.0	0.0	0.0	0.0	0.0	PageOut	98	PAGING SPACE	
cd0	0.0	0.0	0.0	0.0	0.0	Sios	34	Size,MB	2560
								% Used	2.6
Name	PID	CPU%	PgSp	Owner		NFS (calls/sec)		% Free	97.3
truss	28470	4.0	0.6	root		ServerV2	0		
find	24214	0.8	0.4	root		ClientV2	0	Press:	
topas	11682	0.5	1.2	root		ServerV3	0	"h" for help	
syncd	4706	0.0	0.6	root		ClientV3	0	"q" to quit	
db2dasst	21696	0.0	2.6	db2					
muxatmd	9654	0.0	0.5	root					
db2fmcd	18098	0.0	0.8	root					
java	14386	0.0	387.1	root					
java	14016	0.0	157.0	root					
gil	2580	0.0	0.1	root					
db2dasrr	17906	0.0	2.1	dasusr1					
X	6454	0.0	3.0	root					
rpc.lock	13470	0.0	0.0	root					
nfsd	5268	0.0	0.0	root					
java	20918	0.0	29.7	root					
db2fmcd	18098	0.0	0.8	root					
java	14016	0.0	157.0	root					
gil	2580	0.0	0.1	root					
db2dasrr	17906	0.0	2.1	dasusr1					

Important: `Truss` is probably not a good tool to use to troubleshoot a performance problem because it is likely to put a greater load on the system than the process it is reporting on.

Appendixes

Appendix A, “Tasks reference” on page 457 provides quick reference tables that present methods for accomplishing equivalent tasks in Solaris and AIX 5L.

Appendix B, “Quick reference: Comparable commands and configuration files” on page 499 provides quick reference tables for comparing configuration files, comparable commands, and common commands.

Appendix C, “AIX 5L Object Data Manager” on page 503 provides a detailed review of the AIX 5L Object Data Manager features and functions.



A

Tasks reference

This appendix contrasts the common tasks for the Solaris and the AIX 5L operating systems (OS). Tasks are grouped according to major categories. Each major category is contained within a table. The tables also include file location information and other pertinent information relating to the category to which they belong.

This reference provides information about Solaris and AIX 5L in the following categories:

- ▶ “Packaging” on page 459
- ▶ “Installation and upgrading tasks” on page 459
- ▶ “Booting and shutting down” on page 461
- ▶ “User management tasks” on page 464
- ▶ “Device management and configuration” on page 465
- ▶ “Network management and configuration” on page 466
- ▶ “Network File System management and configuration” on page 470
- ▶ “Monitoring and performance” on page 471
- ▶ “Displaying system information” on page 476
- ▶ “Starting and stopping system services” on page 477
- ▶ “Scheduling services” on page 477
- ▶ “Quotas” on page 479
- ▶ “Accounting” on page 480

- ▶ “AIX 5L management tools” on page 480
- ▶ “Backup and restore” on page 481
- ▶ “Printer management and configuration” on page 482
- ▶ “Disk and file system management” on page 484
- ▶ “Troubleshooting” on page 494

Packaging

Table A-1 provides information about the differences in the Solaris and AIX 5L packaging-related tasks.

Table A-1 Packaging comparison

Unit	Solaris	AIX 5L
Smallest installable unit	<ul style="list-style-type: none"> ▶ Package ▶ Patch 	File set
Single installable image. Must be distributed and installed as a unit.	Package	Licensed program product (LPP)
Logical grouping of packages	<ul style="list-style-type: none"> ▶ Software cluster ▶ Patch cluster 	<ul style="list-style-type: none"> ▶ Technical level or Service pack (OS) ▶ Software bundle
Logical grouping of packages and software clusters	Software configuration clusters, for example: <ul style="list-style-type: none"> ▶ Core: Required operating system files ▶ User system support: Core plus window environment ▶ Developer system support: User plus the development environment ▶ Entire distribution: Developer system plus enhanced features ▶ Entire distribution plus original equipment manufacturer (OEM): Entire distribution plus third-party hardware drivers (on Scalable Processor ARChitecture (SPARC) only) 	<ul style="list-style-type: none"> ▶ Core: Required base operating system (BOS) files ▶ Optional software products ▶ Licensed program products ▶ User-defined software bundles ▶ File set installation packages

Installation and upgrading tasks

Table A-2 provides information about the differences in the Solaris and AIX 5L installation and upgrading tasks.

Table A-2 Installation and upgrading tasks

Task	Solaris	AIX 5L
Install packages	pkgadd	installp -a

Task	Solaris	AIX 5L
Display installed packages	<ul style="list-style-type: none"> ▶ <code>pkginfo</code> or ▶ <code>pkgparam</code> 	<code>lspp -a</code>
Remove software package	<code>pkgrm</code>	<code>installp -u</code>
Upgrade or install a package	<code>pkgadd</code>	<code>install_all_updates</code>
Verify correct installation	<code>pkgchk</code>	<code>lppchk -v</code>
Install a patch	<code>patchadd</code>	<code>instfix -i</code>
List contents of installed package	<code>/usr/sbin/pkgchk -l package grep pathname</code>	<code>lspp -f</code>
Check which file belongs to a package	<code>/usr/sbin/pkgchk -lp somefile</code>	<code>lspp -w /pathname/filename</code>
Check package information	<code>pkginfo -l</code>	<code>lspp -al grep fileset</code>
Remove a patch	<code>patchrm</code>	<ul style="list-style-type: none"> ▶ <code>installp -r</code> (if applied but not committed) or ▶ <code>smitty reject</code>
Display installed patches	<code>showrev -p</code>	<code>instfix -ia</code>
Install OS on another disk (alternate disk installation)	Live Upgrade	<code>alt_disk_install</code>
Create an installation server for network installation	<code>setup_install_server install_dir_path</code>	<code>nimconfig</code>
Create a boot server for network installation	<code>setup_install_server -b bootdirpath</code>	<code>smitty nim_config_env</code>
Set up a client for network installation	<code>add_install_client</code>	<code>smitty nim_mkmac</code>

Booting and shutting down

Table A-3 provides information that shows the differences in the process and locations of items that are involved in booting and shutting down a system in Solaris and AIX 5L.

Table A-3 Booting and shutdown tasks

Task	Solaris	AIX 5L
Boot process	<p>Phases:</p> <ol style="list-style-type: none"> 1. OpenPROM: Display system information, run Power-On Self-Test (POST), load bootblk, and locate ufsboot. 2. Boot programs: bootblk loads and executes the ufsboot. 3. Kernel initialization: ufsboot loads and executes the core kernel, initializes core kernel data structures, loads other kernel modules based on the <code>/etc/system</code> file, and starts <code>/sbin/init</code> program. 4. <code>init</code>: Starts other processes based on the <code>/etc/inittab</code> file. 5. <code>/sbin/rcX</code> runs the corresponding <code>/etc/rcX.d</code> scripts to start other components. 	<p>Phases:</p> <ul style="list-style-type: none"> ▶ Read Only Storage (ROS): Check the system board, perform POST, locate the boot image, load the boot image into memory, begin system initialization, and execute phase 1 of the <code>/etc/rc.boot</code> script. ▶ Base device configuration: Start Configuration Manager to configure base devices ▶ System boot: Start <code>init</code> process phase 2, switch to hard disk root file system, start other processes defined by records in the <code>/etc/inittab</code> file, and execute phase 3 of the <code>/etc/rc.boot</code> script.
Default kernel location	<ul style="list-style-type: none"> ▶ <code>/kernel</code>: Contains common components ▶ <code>/platform/platform-name/kernel</code>: Contains the platform-specific kernel components ▶ <code>/platform/hardware-class-name/kernel</code>: Contains kernel components specific to this hardware class ▶ <code>/usr/kernel</code>: Contains kernel components common to all platforms within a particular CPU set 	<p>Kernel and kernel extension modules are stored in two directories:</p> <ul style="list-style-type: none"> ▶ <code>/usr/lib/boot</code> ▶ <code>/usr/lib/drivers</code>

Task	Solaris	AIX 5L
Default kernel modules location	<p>Each of the subdirectories mentioned in the preceding cell might contain the following subdirectories:</p> <ul style="list-style-type: none"> ▶ drv: Contains loadable device drivers ▶ exec: Contains modules that run programs stored in different file formats ▶ fs: Contains file system modules ▶ misc: Contains miscellaneous system-related modules ▶ sched: Contains OS schedulers ▶ strmod: Contains loadable System V STREAMS modules ▶ sys: Contains loadable system calls ▶ cpu: Contains CPU-type specific modules ▶ tod: Contains time-of-day hardware modules ▶ sparcv9: Contains 64-bit versions of specific modules 	
System-run levels		
Run level S or s	Single-user level (boot -s). Only some file systems are mounted as opposed to run level 1.	m, M, s, S: Single-user mode (maintenance level)
Run level 0	Shuts down the OS. Does not attempt to turn off the power. Returns to OpenPROM OK prompt.	0-1: Reserved for future use
Run level 1	Administrative single-user mode. Can access all the available file systems. User logins disabled.	
Run level 2	Multiuser, without Network File System (NFS) resources shared	2: Multiuser mode, with NFS resources shared (default run level)

Task	Solaris	AIX 5L
Run level 3	Multiuser, with NFS resources shared (default run level for Solaris). The login is text or graphical, depending on the console capabilities.	<ul style="list-style-type: none"> ▶ 3-9: Defined according to the user's preferences ▶ a, b, c: Starts processes assigned to the new run levels while leaving the existing processes at the current level running, ▶ Q, q: init command to reexamine the <code>/etc/inittab</code> file <p>Note: When a level from 1 to 9 is specified, the <code>init</code> command kills processes at the current level and restarts any processes associated with the new run level based on the <code>/etc/inittab</code> file</p>
Run level 4	N/A (alternate multiuser)	
Run level 5	Power-down state, shuts down the OS, and tries to turn power off if supported by the system	
Run level 6	Reboot	
Determine a system's run level	who -r	who -r
Change a system's run level	<ul style="list-style-type: none"> ▶ telinit run-level-number ▶ init run-level-number 	<ul style="list-style-type: none"> ▶ telinit run-level-number ▶ init run-level-number
Startup script	<code>/sbin/rc run-level-number</code>	<code>/etc/rc</code>
Start new kernel	N/A	bosboot -k
Display or alter the list of boot devices	boot	bootlist
Boot methods		
Default boot mode	boot or, if <code>auto-boot</code> is set to <code>true</code> , it is automatic ^a .	bosboot
Single-user mode	boot -s	shutdown -m
Recovery boot mode	<ul style="list-style-type: none"> ▶ boot cdrom ▶ boot net 	bosboot -M serv
Interactive start of services while booting	N/A	bosboot -M [Norm serv both]
Emergency boot mode	N/A	shutdown -Fr now
Shut down and reboot	<ul style="list-style-type: none"> ▶ reboot ▶ shutdown -i 6 	<ul style="list-style-type: none"> ▶ reboot (single user only) ▶ shutdown -r now
Shut down	<ul style="list-style-type: none"> ▶ halt ▶ poweroff ▶ shutdown 	<ul style="list-style-type: none"> ▶ halt ▶ poweroff ▶ shutdown

a. The commands listed in this column assume that you are in the OpenPROM prompt.

User management tasks

Table A-4 provides information that shows the differences in AIX 5L and Solaris user management-related tasks.

Table A-4 Quick reference for user management

Task	AIX 5L	Solaris
Running multiple tasks in a graphical user interface (GUI) environment	Chose one of the following: <ul style="list-style-type: none"> ▶ wsm ▶ smitty ▶ The smitty users fast path 	<ul style="list-style-type: none"> ▶ admintool ▶ smc
Adding user	mkuser	useradd
Removing user	rmuser	userdel
Displaying currently logged users	<ul style="list-style-type: none"> ▶ who or ▶ w 	<ul style="list-style-type: none"> ▶ who or ▶ w
Displaying users and their attributes	lsuser	listusers logins
Password files	<ul style="list-style-type: none"> ▶ /etc/passwd and ▶ /etc/security/passwd 	<ul style="list-style-type: none"> ▶ /etc/passwd and ▶ /etc/shadow
Administering users' passwords	<ul style="list-style-type: none"> ▶ passwd ▶ chpasswd ▶ pwdadm 	passwd
Modifying user account	chuser	usermod
System-wide environment file	<ul style="list-style-type: none"> ▶ /etc/profile and ▶ /etc/environment 	/etc/profile
Profile template	/etc/security/.profile	/etc/skel/.profile
Adding a group	mkgroup	groupadd
Group files	<ul style="list-style-type: none"> ▶ /etc/group and ▶ /etc/security/group 	/etc/group
Modifying a group	chgroup	groupmod
Deleting a group	rmgroup	groupdel

Task	AIX 5L	Solaris
Checking password and group definition consistency	<ul style="list-style-type: none"> ▶ pwck and ▶ grpck 	<ul style="list-style-type: none"> ▶ pwck and ▶ grpck
Defining system resource limits for user	<ul style="list-style-type: none"> ▶ /etc/security/limits or ▶ ulimit 	ulimit

Device management and configuration

Table A-5 provides information that shows the differences between the AIX 5L and the Solaris device management and configuration tasks.

Table A-5 Quick reference for device management

Task	AIX 5L	Solaris 9
Run multiple tasks in a GUI environment	<ul style="list-style-type: none"> ▶ smit ▶ Web-based System Manager 	smc
Configure a device (dynamic reconfiguration)	cfgmgr	<ul style="list-style-type: none"> ▶ cfgadm and ▶ devfsadm
Add a device with the command line	mkdev	devfsadm
Remove a Small Computer System Interface (SCSI) device	rmdev^a	<ul style="list-style-type: none"> ▶ luxadm (for Sun storage only) ▶ devfsadm -C
Change attributes for a device	chdev	No equivalent
List devices	<ul style="list-style-type: none"> ▶ lsdev^b ▶ prtconf ▶ lscfg 	<ul style="list-style-type: none"> ▶ prtconf ▶ sysdef ▶ dmesg
List the configuration attributes for devices.	lsattr -E1	No equivalent
List VPD (serial number, model, vendor, part number) of a device.	lscfg -v1	No equivalent

a. It can change the state of a device from available to defined, or it can delete the ODM entries for a device.

b. Can be used to query configured devices if used with -C option (upper case) or supported devices if used with the -P option.

Multipath Input/Output management

Table A-6 provides an overview of Multipath I/O (MPIO) management commands in AIX 5L.

Table A-6 Multipath I/O management commands

Command	Function
mkpath	Adds another path to a device
rmpath	Removes a path from a device
chpath	Changes status or attribute associated with a path
lspath	Displays information about paths to an MPIO-capable device
iostat -m	Displays statistics for each path on each disk
smitty mpio	Gives you all the options you want for MPIO maintenance, including disabling all the activity down a particular parent adapter, enabling or disabling all the paths (although you can never disable the last path to a device), changing path priorities, and so on
lsattr -E1	Displays the attributes of a device
chdev	Changes the attributes of a device

Network management and configuration

Table A-7, Table A-8, Table A-9, Table A-10, and Table A-11 provide information about the differences in Solaris and AIX 5L network management and configuration tasks.

Table A-7 shows the network commands and configuration files.

Table A-7 Network commands and configuration files

Task	Solaris	AIX 5L
Configure TCP/IP interface	Edit the following files: <ul style="list-style-type: none"> ▶ /etc/hostname.* ▶ /etc/inet/* ▶ /etc/defaultrouter ▶ /etc/defaultdomain ▶ /etc/nodename ▶ /etc/netmasks 	[smit,wsm] tcpip

Task	Solaris	AIX 5L
Display interface settings	ifconfig	ifconfig
Display interface status and statistics	<ul style="list-style-type: none"> ▶ netstat -i ▶ ifconfig 	<ul style="list-style-type: none"> ▶ netstat -i ▶ ifconfig
Configure interface	ifconfig	ifconfig
Check various network statistics	netstat	netstat
Change name server or domains	vi /etc/resolv.conf	<ul style="list-style-type: none"> ▶ namerslv ▶ vi /etc/resolv.conf ▶ smitty namerslv
Specify name services search order	vi /etc/nsswitch.conf	vi /etc/netsvc.conf
Display kernel network parameters	<ul style="list-style-type: none"> ▶ ndd /dev/ip \? ▶ ndd /dev/tcp \? 	no -a
Configure kernel network parameters	ndd -set driver parameter	<ul style="list-style-type: none"> ▶ smit performance or ▶ no -o Tunable=NewValue
Check for network link	<ul style="list-style-type: none"> ▶ ndd or ▶ kstat 	<ul style="list-style-type: none"> ▶ smit performance or ▶ netstat -v interface grep -i link
Set up Dynamic Host Configuration Protocol (DHCP)	<ul style="list-style-type: none"> ▶ dhcpconfig ▶ dhcpgmr ▶ dhcpinfo ▶ dhtadm ▶ pntadm 	<ul style="list-style-type: none"> ▶ dhcpsconf ▶ dhcpaction ▶ dhcprd ▶ bootptodhcp ▶ dadmin
Check routing table	<ul style="list-style-type: none"> ▶ netstat -r ▶ route 	<ul style="list-style-type: none"> ▶ netstat -r ▶ route ▶ smitty route
Modify routing table	route	<ul style="list-style-type: none"> ▶ smitty route ▶ route
Test for connectivity	ping	ping
Check IP path	traceroute	traceroute
Capture network packets	snoop	<ul style="list-style-type: none"> ▶ tcpdump ▶ iptrace/ipreport

Table A-8 shows the network analysis tools.

Table A-8 Network analysis tools

Task	Solaris	AIX 5L
Browse network traffic	ethereal	ethereal
Dump and analyze network traffic	<ul style="list-style-type: none"> ▶ tethereal ▶ snoop 	tcpdump
Network crash dump utilities	mdb	trcdead
Network crash storage location	<i>/var/crash/hostname</i>	<i>/var/adm/ras</i>

Table A-9 shows the routing commands.

Table A-9 Routing commands

Task	Solaris	AIX 5L
Check routing table	<ul style="list-style-type: none"> ▶ netstat -r ▶ route 	<ul style="list-style-type: none"> ▶ netstat -r ▶ [smit, wsm] route ▶ route
Modify routing table	route	smit route
Specify static routing - ipv4	<ul style="list-style-type: none"> ▶ route add [default] ipaddr ▶ vi /etc/defaulter w/ipaddr 	<ul style="list-style-type: none"> ▶ route add default or ▶ [smit, wsm] route
Specify static routing - ipv6	<ul style="list-style-type: none"> ▶ route add [default] ipaddr ▶ ndpd - daemon 	route add -inet6 default IPv6 router address
Specify dynamic routing - ipv4	If <i>/etc/defaultrouter</i> file is empty, in.rdisc and in.routed daemons are started at reboot	<ul style="list-style-type: none"> ▶ vi /etc/rc.tcp and ▶ uncomment gated or routed gated and routed daemons are started at reboot
Dynamic routing - ipv6 daemon	ripngd	ndpd-router

Table A-10 shows managing inetd subsystems.

Table A-10 Managing inetd subsystems

Task	Solaris	AIX 5L
Configuring the inetd subservers (ftp, telnet, rlogin, ssh, and so on)	<ul style="list-style-type: none"> ▶ vi /etc/services ▶ vi /etc/default/inetd ▶ vi /etc/init.d/inetsvc ▶ vi /etc/inetd.conf 	smit inetdconf
Starting the inetd subsystem	/usr/sbin/inetd -s	smit inetd
Stopping the inetd subsystem	/etc/init.d/inetsvc stop	smit inetd
Starting the inetd subservers (ftp, telnet, rlogin, and so on)	/usr/sbin/in.daemon	startsrc -t <i>subservername</i>
Stopping the inetd subservers (ftp, telnet, rlogin, and so on)	kill <i>in.daemon-pid</i>	stopsrc -t <i>subservername</i>
Changing inetd configuration	vi /etc/inetd.conf	smit inetdconf
Refreshing inetd after configuration change	kill -HUP <i>inetd process</i>	If smit inetdconf was used, no refresh required
Querying inetd subservices	ps -ef grep 'in\.'	lssrc -t <i>subservername</i>

Table A-11 shows the DHCP commands.

Table A-11 DHCP commands

Task	Solaris	AIX 5L
Configuring DHCP	<ul style="list-style-type: none"> ▶ DHCP Manager (GUI) ▶ dhcplib (GUI) ▶ dhcpconfig ▶ dhtadm ▶ pntadm 	<ul style="list-style-type: none"> ▶ dhcpsconf (GUI) ▶ dhcpaction ▶ dhcprd ▶ bootptodhcp ▶ dadmin
Daemon name	in.dhcpd	dhcpsd
Querying information about the DHCP server	dhcpinfo	lssrc -ls dhcpsd

Task	Solaris	AIX 5L
Stopping and starting the DHCP server	<ul style="list-style-type: none"> ▶ Dhcp Manager (X Windows) ▶ <code>dhcpcmgr</code> (Java GUI) ▶ <code>/etc/init.d/dhcp stop</code> or <code>start</code> 	<ul style="list-style-type: none"> ▶ <code>[smit, wsm] tcpip</code> or ▶ <code>[startsrc, stopsrc] -s dhcpsd</code>

Network File System management and configuration

Table A-12 provides information that shows the differences in Solaris and AIX 5L NFS management and configuration tasks.

Table A-12 NFS differences in Solaris and AIX 5L

Tasks and configuration file	Solaris	AIX 5L
Manually start or stop the NFS server and client daemons	<ul style="list-style-type: none"> ▶ <code>/etc/init.d/nfs.server start</code> ▶ <code>/etc/init.d/nfs.server stop</code> ▶ <code>/etc/init.d/nfs.client start</code> ▶ <code>/etc/init.d/nfs.client stop</code> 	<ul style="list-style-type: none"> ▶ <code>startsvc -g nfs</code> ▶ <code>stopsvc -g nfs</code> or ▶ <code>[wsm, smit] nfsconfigure</code>
Mount a resource on an NFS client	<code>mount -F nfs server://resource /mntpoint</code>	<code>mount server://resource /mntpoint</code>
NFS server general configuration file	<code>/etc/default/nfs</code>	<code>[wsm, smit nfsconfigure]</code>
Share all exported file systems	<code>shareall</code>	<code>exportfs -a</code>
Share a new file system	<code>share -F nfs ...directory</code>	<code>exportfs directory</code>
Configuration file of shared file systems	<code>/etc/dfs/dfstab</code>	<code>/etc/exports</code>
Add or remove shared or exported directories	<ul style="list-style-type: none"> ▶ <code>vi /etc/dfs/dfstab</code> and ▶ <code>unshare directory</code> or ▶ <code>unshareall</code> 	<ul style="list-style-type: none"> ▶ <code>[wsm, smit]</code> ▶ <code>[mknfsexp/rmnfsexp]</code>
Show mounted file systems	<ul style="list-style-type: none"> ▶ <code>mount</code> ▶ <code>df</code> ▶ <code>cat /etc/mnttab</code> 	<ul style="list-style-type: none"> ▶ <code>mount</code> ▶ <code>df</code>

Monitoring and performance

The following sections further illustrate command and task differences.

Memory management

Table A-13 shows memory management in Solaris and AIX 5L.

Table A-13 Memory management

Task	Solaris	AIX 5L
Memory management		
Display how much random access memory (RAM) is on a machine	<ul style="list-style-type: none"> ▶ prtconf ▶ top 	<ul style="list-style-type: none"> ▶ bootinfo -r ▶ prtconf ▶ topas
Display how much RAM (RSS) a process is using	<ul style="list-style-type: none"> ▶ ps -ely, ▶ ps -eo rss,comm ▶ pmap -x pid 	<ul style="list-style-type: none"> ▶ ps ev ▶ /usr/sysv/bin/ps -ely ▶ svmon ▶ topas
Calculate the SIZE ^a of a running process	<ul style="list-style-type: none"> ▶ ps -ely, ▶ ps -eo vsz,comm, ▶ ps -elf (w/SZ field multiplied by page size, generally 8192) 	<ul style="list-style-type: none"> ▶ /usr/sysv/bin/ps -ely ▶ ps -eo vsz,comm ▶ svmon
Swap and Paging space		
Display how much swap has been defined	<ul style="list-style-type: none"> ▶ swap -l ▶ df -k, top 	<ul style="list-style-type: none"> ▶ swap -l ▶ lsps -a ▶ topas
Display how much total swap/paging space is in use	<ul style="list-style-type: none"> ▶ swap -l ▶ df -k, top 	<ul style="list-style-type: none"> ▶ swap -l ▶ lsps -a ▶ topas ▶ svmon
Decrease swap/paging space	<ul style="list-style-type: none"> ▶ swap -r 	<ul style="list-style-type: none"> ▶ rmpps ▶ chpps
Increase swap/paging space	<ul style="list-style-type: none"> ▶ mkfile size filename ▶ swap -a filename 	<ul style="list-style-type: none"> ▶ mkpps ▶ chpps
User shell resource limits		

Task	Solaris	AIX 5L
Report user shell resource limits	<code>ulimit -a</code>	<code>ulimit -a</code>
Temporarily reset user shell resource limits	<code>ulimit -option newlimit</code>	<code>ulimit -option newlimit</code>
Permanently set user shell resource limits	<code>vi /etc/system + reboot</code>	<code>vi /etc/security/limits</code> [reboot not required]

a. SIZE is defined as the total size of the process in virtual memory, including RAM, swap, and all the mapped files and devices. Also called the *core image*.

Processors and CPU

Table A-14 shows the differences in the CPU monitoring commands between Solaris and AIX 5L.

Table A-14 CPU monitoring commands

Task	Solaris	AIX 5L
CPU monitoring and management		
Display how many CPUs the system has	<ul style="list-style-type: none"> ▶ <code>prtconf</code> ▶ <code>psrinfo</code> ▶ <code>top</code> 	<ul style="list-style-type: none"> ▶ <code>prtconf</code> ▶ <code>topas</code> ▶ <code>lsdev -Cc processor</code>
Display %CPU usage by process	<ul style="list-style-type: none"> ▶ <code>ps -eo pcpu</code> ▶ <code>comm</code> 	<ul style="list-style-type: none"> ▶ <code>ps -eo pcpu</code> ▶ <code>comm</code>
Display CPU accumulated time by process	<ul style="list-style-type: none"> ▶ <code>ps -eo time</code> ▶ <code>comm</code> 	<ul style="list-style-type: none"> ▶ <code>ps -eo time</code> ▶ <code>comm</code>
Display CPU utilization	<ul style="list-style-type: none"> ▶ <code>sar</code> ▶ <code>cpustat</code> ▶ <code>top</code> 	<ul style="list-style-type: none"> ▶ <code>sar</code> ▶ <code>tprof</code> ▶ <code>topas</code> ▶ <code>netpmon</code>
Review process queues	<code>sar -q</code>	<code>sar -q</code>
Display individual processor statistics in a multiprocessor system	<code>mpstat</code>	<ul style="list-style-type: none"> ▶ <code>mpstat</code> ▶ <code>topas</code>
Managing and Tuning I/O		
Display I/O statistics	<ul style="list-style-type: none"> ▶ <code>iostat</code> ▶ <code>sar</code> 	<ul style="list-style-type: none"> ▶ <code>iostat</code> ▶ <code>topas</code> ▶ <code>filemon</code> ▶ <code>sar</code>

Task	Solaris	AIX 5L
Display/Manage I/O tuning parameters	<code>vi /etc/system</code>	<ul style="list-style-type: none"> ▶ <code>ioo</code> ▶ <code>smit tuning</code>
Load average for the past 1, 5, and 15 minutes	<code>uptime</code>	<code>uptime</code>
Display both CPU utilization and time per process	<code>/usr/ucb/ps -agux</code>	<code>ps agux</code> (not <code>-agux</code>)
Kernel attributes		
Display kernel parameters	<ul style="list-style-type: none"> ▶ <code>sysdef</code> ▶ <code>nnd</code> ▶ <code>kstat</code> 	<ul style="list-style-type: none"> ▶ <code>lsattr</code> ▶ <code>vmo</code> ▶ <code>no</code> ▶ <code>smit tuning</code>
Tune kernel parameters	<code>vi /etc/system</code> and reboot	<ul style="list-style-type: none"> ▶ <code>vmo</code> (formerly <code>vmtune</code>) ▶ <code>smit tuning</code> ▶ <code>/etc/tunables/nextboot</code>

Physical media

Table A-15 shows the physical media monitoring commands.

Table A-15 Physical media monitoring commands

Task	Solaris	AIX 5L
Display, collect, or store system activity status	<code>sar</code>	<code>sar</code>
Display I/O statistics	<code>iostat</code>	<code>iostat</code>

Software Redundant Array of Independent Disks

Table A-16 shows the software RAID monitoring commands.

Table A-16 Software RAID monitoring commands

Task	Solaris	AIX 5L
Display status information for software RAID devices	<code>metastat</code>	<ul style="list-style-type: none"> ▶ <code>smit lvm</code> ▶ <code>lsvg</code> ▶ <code>lslv lspv</code>

Task	Solaris	AIX 5L
Monitor software RAID devices	<ul style="list-style-type: none"> ▶ metastat ▶ iostat 	<ul style="list-style-type: none"> ▶ smit lvm ▶ vmstat ▶ iostat

Logical volumes

Table A-17 shows the logical volume monitoring commands.

Table A-17 Logical volume monitoring commands

Task	Solaris	AIX 5L
Display logical volume attributes	<ul style="list-style-type: none"> ▶ metastat ▶ vxprint (Veritas) 	<ul style="list-style-type: none"> ▶ lslv ▶ [wsm, smit] [lv,lslv] ▶ lsvg
Display physical volume attributes	format	<ul style="list-style-type: none"> ▶ lspv ▶ lslv -p <i>physical-volume</i>
Display volume groups attributes	metastat	<ul style="list-style-type: none"> ▶ lsvg ▶ [wsm, smit] [vg,lsvg]
Display Logical Volume Manager (LVM) I/O statistics	<ul style="list-style-type: none"> ▶ iostat ▶ vxstat (Veritas) 	lvmstat

File systems

Table A-18 shows the file system monitoring commands.

Table A-18 File system monitoring commands

Task	Solaris	AIX 5L
Display file system disk space usage information	df	df
Display individual file disk space usage	du	du
Display quota data	repquota	repquota
Display I/O statistics	iostat	<ul style="list-style-type: none"> ▶ iostat ▶ lvmstat
Report disk operations per second	vmstat	vmstat

Network

Table A-19 illustrates some of the network activity monitoring commands. Additional network performance information can be found in `/proc/slabinfo`.

Table A-19 Network monitoring commands

Task	Solaris	AIX 5L
Graphical network protocol analyzer	<code>ethtereal</code>	<code>ethtereal</code>
Configure network device	<code>ifconfig</code>	<code>ifconfig</code>
Monitor traffic load	<code>netstat</code>	► <code>netstat</code> ► <code>topas</code>
Display network statistics, routing information, connections, and so on	<code>netstat</code>	<code>netstat</code>
Display NFS statistics	<code>nfsstat</code>	<code>nfsstat</code>
Send Internet Control Message Protocol (ICMP) echo request packets to network host	<code>ping</code>	<code>ping</code>
Display network packets	<code>snoop</code>	<code>iptrace</code>
Test network connectivity using a User Datagram Protocol (UDP) protocol	<code>spray</code>	<code>spray</code>
Dump and analyze network traffic	► <code>snoop</code> ► <code>tcpdump</code>	<code>tcpdump</code>

System and user processes

Table A-20 shows the process monitoring commands.

Table A-20 Process monitoring commands

Task	Solaris	AIX 5L
Display interprocess communication facilities status	<code>ipcs</code>	<code>ipcs</code>
Display shared library dependencies	<code>ldd</code>	► <code>ldd</code> ► <code>dump -H executable</code>
Display open files	<code>lsof</code>	<code>lsof</code>
Display dynamic library calls	<code>ldd</code>	<code>dump</code>
Display process status	<code>ps</code>	<code>ps</code>

Task	Solaris	AIX 5L
Display process interdependencies in a tree format	pstree	proctree
Display, collect, or store system activity status	sar	sar
Trace system calls and signals	truss	truss
Display top CPU user for running processes and CPU and memory statistics	top	topas
Display virtual memory statistics	vmstat	vmstat

Displaying system information

Table A-21 shows the differences in basic system information between Solaris and AIX 5L OS.

Table A-21 Basic system information

System information task	Solaris	AIX 5L
System information	uname	uname
Processor information	<ul style="list-style-type: none"> ▶ prtdiag ▶ psrinfo 	<ul style="list-style-type: none"> lsdev lsattr
Memory size	<ul style="list-style-type: none"> ▶ prtdiag ▶ prtconf 	lsattr -E1 mem0
Mounted file system information	df	df
File usage	du	du
Show host name information	<ul style="list-style-type: none"> ▶ hostname ▶ uname -n 	<ul style="list-style-type: none"> hostname uname -n
Serial number	N/A	lsattr -E1 sys0 grep system
List process	<ul style="list-style-type: none"> ▶ prstat ▶ top ▶ ps 	<ul style="list-style-type: none"> ▶ nmon ▶ topas ▶ ps
Adapter location	<ul style="list-style-type: none"> ▶ prtdiag ▶ cfgadm ▶ cat /etc/path_to_inst 	<ul style="list-style-type: none"> ▶ lsdev ▶ lscfg ▶ lsslot

System information task	Solaris	AIX 5L
Network IP	<code>ifconfig</code>	<code>ifconfig</code>
Network route	<code>route</code>	<code>route</code>
Network connection features	<ul style="list-style-type: none"> ▶ <code>ndd</code> ▶ <code>kstat</code> 	<code>netstat -v</code>

Starting and stopping system services

Table A-22 shows a summary of how to manage system services on AIX 5L.

Table A-22 *Manage system services on AIX 5L*

Task	Command
List all subsystems	<code>lssrc -a</code>
List all subsystems of a specific group	<code>lssrc -g <i>group_name</i></code>
List one subsystem	<code>lssrc -s <i>subsystem_name</i></code>
Start all subsystems of a group	<code>startsrc -g <i>group_name</i></code>
Start one subsystem	<code>startsrc -s <i>subsystem_name</i></code>
Stop all subsystems of a group	<code>stopsrc -g <i>group_name</i></code>
Stop one subsystem	<code>stopsrc -s <i>subsystem_name</i></code>
Restart all subsystems of a specific group	<code>refresh -g <i>group_name</i></code>
Restart one subsystem	<code>refresh -g <i>subsystem_name</i></code>

Scheduling services

The following tables illustrate crontab commands and tasks.

Using crontab

The concepts about crontab on Solaris and AIX 5L are the same, but there are a few differences. These are displayed in Table A-23, Table A-24, and Table A-25.

Table A-23 shows the crontab command options.

Table A-23 Crontab command options

Crontab option	Solaris	AIX 5L
-e	Edit crontab	Edit crontab
-r	Remove crontab	Remove crontab
-l	List crontab	List crontab
-v	N/A	Crontab status

Table A-24 shows the options for starting and stopping crontab.

Table A-24 Starting and stopping crontab

Crontab task	Solaris	AIX 5L
Start	<code>/etc/init.d/cron start</code>	Automatically by <code>/etc/inittab</code>
Stop	<code>/etc/init.d/cron stop</code>	<ul style="list-style-type: none"> ▶ Remove from inittab with <code>rmitab cron</code> ▶ <code>kill crontab PID</code>
Restart	<ul style="list-style-type: none"> ▶ <code>kill -HUP PID</code> or ▶ <code>/etc/init.d/cron stop</code> and <code>/etc/init.d/cron start</code> 	<code>kill contab PID</code> (Be sure that cron is enabled on <code>/etc/inittab</code>)

Table A-25 shows the crontab control files.

Table A-25 Crontab control files

Task	Solaris	AIX 5L
Users allowed to use crontab	<code>/etc/cron.d/cron.allow</code>	<code>/var/adm/cron/cron.allow</code>
Users denied access to crontab	<code>/etc/cron.d/cron.deny</code>	<code>/var/adm/cron/cron.deny</code>
Spool area	<code>/var/spool/cron/crontabs</code>	<code>/var/spool/cron/crontabs</code>

Using the “at” files

Table A-26 shows the “at” files.

Table A-26 The “at” files

Description	File on Solaris	File on AIX 5L
Users allowed to use at	/usr/lib/cron/at.allow	/var/adm/cron/at.allow
Users not allowed to use at	/usr/lib/cron/at.deny	/var/adm/cron/at.deny
Spool area	/var/spool/cron/atjobs	/var/spool/cron/atjobs

Quotas

Table A-27 shows the quota commands.

Table A-27 Quota commands

Task	Solaris	AIX 5L
Display disk usage and quotas	quota	quota
Edit user and group quotas	edquota	edquota
Check file system quota consistency	quotacheck	quotacheck
Turn on file system quota	quotaon	quotaon
Turn off file system quota	quotaoff	quotaoff
Manage quota limit classes for journaled file system 2 (JFS2)	N/A	j2edlimit (available only for JFS2)

Table A-28 shows the quota configuration files.

Table A-28 Quota configuration files

Task	File on Solaris	File on AIX 5L
Parameters for each file system	/etc/vfstab	/etc/filesystems
Specifies user quotas	quota.user	quota.user
Specifies group quotas	quota.group	quota.group

Accounting

Table A-29 shows the accounting commands on Solaris and AIX 5L.

Table A-29 Accounting on Solaris and AIX 5L

Command	Specification
runacct	The runacct command is the main daily accounting shell procedure. Normally initiated by the cron daemon.
acctcom	Displays selected process accounting record summaries. The acctcom command then writes the records you request to standard output. This command is stored in the /usr/sbin/acct directory for access by all users.
dodisk	The dodisk command initiates disk-usage accounting by calling the diskusg command and the acctdisk command.
▶ acctdisk and ▶ acctusg (On Solaris, only acctdisk)	The acctdisk and acctusg commands are called by the dodisk command to perform disk usage accounting. Usually, this procedure is initiated when the cron daemon runs the dodisk command.
chargefee	Charges users for the computer resources they use. The chargefee command writes a record to the /var/adm/fee file.
acctmerg	Merges total accounting files into an intermediary file or a daily report
acctcms	Produces command usage summaries from accounting records
▶ acctprc1 ▶ acctprc2 ▶ accton (On Solaris, only accton)	Are called by the runacct command to perform process accounting shell procedures
lastcomm	Displays information about the last commands executed
who	Identifies the users currently logged in

AIX 5L management tools

Table A-30 shows the System Management Interface Tool (SMIT) symbols.

Table A-30 SMIT symbols

Symbols in SMIT dialog screen	Explanation
*	A required field
#	A numeric value is required for this field

Symbols in SMIT dialog screen	Explanation
/	A path name is required for this field
X	A hexadecimal value is required for this field
?	The value entered will not be displayed
+	A pop-up list or ring is available

Backup and restore

Table A-31 shows the backup and restore tasks on AIX 5L and Solaris.

Table A-31 Backup and restore tasks

Task	Solaris	AIX 5L
Local back up and restore of files and file systems	<ul style="list-style-type: none"> ▶ ufsdump/ufsrestore ▶ vxdump/vxrestore 	backup/restore
Remote back up and restore of files and file systems	<ul style="list-style-type: none"> ▶ ufsdump/ufsrestore ▶ vxdump/vxrestore 	rdump/rrestore
Create tape archives and add or extract files	tar	tar
Copy files into and out of archive storage and directories	cpio	cpio
Extract, write, and list members of archive files. Copy files and directory hierarchies.	pax	pax
Convert and copy a file	dd	dd
Copy the contents of a logical volume to a new logical volume	N/A	cp1v

Table A-32 shows the backup and restore devices.

Table A-32 Backup and restore devices

Special file name	Rewind on closing	Retention on opening	Bytes per inch
/dev/rmt*	yes	no	Density setting #1
/dev/rmt/*.1	no	no	Density setting #1

Special file name	Rewind on closing	Retention on opening	Bytes per inch
/dev/rmt/*.2	yes	yes	Density setting #1
/dev/rmt/*.3	no	yes	Density setting #1
/dev/rmt/*.4	yes	no	Density setting #2
/dev/rmt/*.5	no	no	Density setting #2
/dev/rmt/*.6	yes	yes	Density setting #2
/dev/rmt/*.7	no	yes	Density setting #2

Printer management and configuration

Table A-33 compares AIX 5L and Solaris with regard to printer management.

Table A-33 Quick reference for printer management

Task	AIX 5L	Solaris
Run multiple tasks in a GUI environment	Choose one of the following: <ul style="list-style-type: none"> ▶ The smitty print fast path ▶ smitty ▶ The Web-based System Manager 	<ul style="list-style-type: none"> ▶ smc or ▶ printmgr
Add a printer	mkdev	lpadmin
Start a print queue	<ul style="list-style-type: none"> ▶ qadm (AIX 5L printing subsystem) or ▶ lpc (System V) 	<ul style="list-style-type: none"> ▶ accept and ▶ enable
Stop a print queue	<ul style="list-style-type: none"> ▶ qadm (AIX 5L printing subsystem) or ▶ lpc (System V) 	<ul style="list-style-type: none"> ▶ disable and ▶ reject
Display print queue status	lpstat	lpstat
Cancel a printing job	qcan	cancel

Task	AIX 5L	Solaris
Add a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> – mkque – mkquedev – mkvirprt ▶ System V: <ul style="list-style-type: none"> – lpadmin -p 	lpadmin
Change a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> – chque – chquedev – chvirprt ▶ System V: <ul style="list-style-type: none"> – lpadmin -p 	lpadmin
Remove a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> – rmque – rmquedev – rmvirprt ▶ System V: <ul style="list-style-type: none"> – lpadmin -x 	lpadmin -x
Display settings of a print queue	Choose one of the following: <ul style="list-style-type: none"> ▶ AIX 5L printing subsystem: <ul style="list-style-type: none"> – lsque – lsquedev – lsvirprt ▶ System V: <ul style="list-style-type: none"> – lpstat 	lpadmin

Disk and file system management

Table A-34 shows disk management in Solaris and AIX 5L.

Table A-34 Disk management

Task	Solaris	AIX 5L
Disk identification	<code>echo format</code>	<code>lsdev -Cc disk</code>
Vendor information	<code>format / inquire</code>	<code>lscfg -v1</code>
Disk analysis	<code>format / analyse</code>	<code>diag</code>

Table A-35 shows AIX 5L system area network (SAN) management by command line.

Table A-35 AIX 5L SAN management by command line

Command	Task
<code>lsparent -C -k iocb; lsparent -C -k qiocb</code>	List fibre channel (FC) adapters
<code>lsparent -C -k fcp</code>	List FC SCSI protocol adapters
<code>chdev</code>	Change adapter characteristics
<code>lsattr -E1 adapter name</code>	List adapter attributes

Table A-36 shows Volume Group Descriptor Area (VGDA) allocation.

Table A-36 VGDA allocation

Condition	VGDA allocation
Single physical volume (PV) in a volume group	Two VGDA's on one disk
Two PVs in a volume group	Two VGDA's on the first disk, one VGDA on the second disk
Three or more PVs in a volume group	One VGDA on each disk

Table A-37 shows the physical volume commands.

Table A-37 Physical volume commands

Command	Smit fast path	Description
lspv	smit lspv	Lists information about PVs
chpv	smit chpv	Changes the characteristics of a PV

Table A-38 shows the Logical Volume Manager (LVM) limitations.

Table A-38 LVM limitations

Volume group (VG) type	Maximum PVs	Maximum logical volume (LV)	Maximum physical partition (PP) per LV	Maximum PP size
Normal VG	32	256	32512	1 Gb
Big VG	128	512	130048	1 Gb
Scalable VG	1024	4096	2097152	128 Gb

Table A-39 provides the VG commands.

Table A-39 VG commands

Command	Smit fast path (menu management)	Task
lsvg	smit lsvg	Displays information about VGs
mkvg	smit mkvg	Creates a VG
chvg	smit chvg	Sets the characteristics of a VG
extendvg	smit extendvg	Adds a new disk on a VG
reducevg	smit reducevg	Removes a disk from a VG
varyonvg	smit varyonvg	Activates a VG
varyoffvg	smit varyoffvg	Deactivates a VG
exportvg	smit exportvg	Exports the definition of a VG from a set of physical volumes
importvg	smit importvg	Imports a new VG definition from a set of physical volumes

Table A-40 shows the LV commands.

Table A-40 LV commands

Command	Smit fast path	Description
lslv	smit lslv	Lists information about a logical volume
mlv	smit mlv	Creates a logical volume
chlv	smit chlv	Changes the characteristics of a logical volume
rmlv	smit rmlv	Deletes a logical volume
extendlv	smit extendlv	Extends a logical volume

Table A-41 shows the mirroring commands.

Table A-41 Mirroring commands

Command	Smit fast path	Task
mlvcopy	smit mlvcopy	Provides copies of data within the logical volume
rmlvcopy	smit rmlvcopy	Removes copies from a logical volume
mirrorvg	smit mirrorvg	Mirrors all the logical volumes that exist on a given volume group
unmirrorvg	smit unmirrorvg	Removes the mirrors that exist on volume groups or specified disks
syncvg	smit syncvg	Synchronizes logical volume copies that are not current

File systems

Table A-42 shows file system management in Solaris and AIX 5L.

Table A-42 File system management

File system management	Solaris	AIX 5L
Create a file system on disk	▶ newfs or ▶ mkfs	▶ mkfs or ▶ crfs
Check the file system space used	df -k	df -k
Check the file system i-nodes used	df -o i	df -k

File system management	Solaris	AIX 5L
Check file system for consistency	fsck	fsck
Check file system type	df -n	<ul style="list-style-type: none"> ▶ lsfs ▶ lslv ▶ lsvg
Check file with basic file system settings	cat /etc/vfstab	cat /etc/filesystems

Table A-43 shows the file system types.

Table A-43 File system types

File system types	Solaris	AIX 5L
Native file system	ufs	jfs and jfs2
CD-ROM file system	nsfs	cdrfs
DVD file system	udf	cdrfs
MSDOS file system	pcfs	cifs
Win95+ file system	pcfs	cifs
Network file system	nfs	nfs

Table A-44 shows NFS differences in Solaris and AIX 5L.

Table A-44 NFS differences

Task	Solaris	AIX 5L
Start NFS daemons	<ul style="list-style-type: none"> ▶ /etc/init.d/nfs.client start and ▶ /etc/init.d/nfs.server start 	startsrc -g nfs
Stop NFS daemons	<ul style="list-style-type: none"> ▶ /etc/init.d/nfs.client stop and ▶ /etc/init.d/nfs.server stop 	stopsrc -g nfs
Mount a resource on an NFS client	mount -F nfs server://resource /mntpoint	mount server://resource /mntpoint
Share a new file system	share -F nfsdirectory	exportfs -i directory

Task	Solaris	AIX 5L
Configure file of shared file systems	<code>/etc/dfs/dfstab</code>	<code>/etc/exports</code>
Files that contain NFS to be mounted on boot time	<code>/etc/vfstab</code>	<code>/etc/filesystems</code>
Command to share a directory or file system	<ul style="list-style-type: none"> ▶ <code>share</code> or ▶ <code>exportfs</code> 	<ul style="list-style-type: none"> ▶ <code>mknfsexp</code> or ▶ <code>exportfs</code>

Table A-45 shows AutoFS in Solaris and AIX 5L.

Table A-45 AutoFS

Task	Solaris	AIX 5L
Auto mount daemon	<code>automountd</code>	<code>automountd</code>
Default map file	<code>/etc/auto_master</code>	<code>/etc/auto_master</code>
Stop automount	<code>/etc/init.d/autofs stop</code>	<code>startsrc -s automountd</code>
Start automount	<code>/etc/init.d/autofs start</code>	<code>stopsrc -s automountd</code>

Table A-46 shows /proc management in Solaris and AIX 5L.

Table A-46 /proc management

Task	Solaris	AIX 5L
Process credentials	<code>pcred</code>	<code>proccred</code>
File descriptor information	<code>pfiles</code>	<code>procfiles</code>
Flag trace	<code>pflags</code>	<code>procflags</code>
Dynamic libraries loaded by process	<code>p1dd</code>	<code>procldd</code>
Address space map of processes	<code>pmap</code>	<code>procmap</code>
Start the stopped processes	<code>prun</code>	<code>procrun</code>
List signal actions	<code>psig</code>	<code>procsig</code>
Process stacks	<code>pstack</code>	<code>procstack</code>
Stop process on the PR_REQUESTED event	<code>pstop</code>	<code>procstop</code>
Print the process tree by ID or users	<code>ptree</code>	<code>proctree</code>

Task	Solaris	AIX 5L
Wait for all the specified processes to terminate	pwait	procwait
Current work directory of a process	pwdx	procwdx

Table A-47 shows swap management in Solaris and AIX 5L.

Table A-47 Swap management

Task	Solaris	AIX 5L
List total swap area and usage of swap area	swap -l	<ul style="list-style-type: none"> ▶ swap -l or ▶ lsp
Increase page space	swap -a	<ul style="list-style-type: none"> ▶ mkps ▶ chps -s
Reduce swap area	swap -r	<ul style="list-style-type: none"> ▶ chps -d ▶ rmpps
Activate page space	swap -a	<ul style="list-style-type: none"> ▶ swap -a ▶ swapon
Deactivate page space	swap -d	<ul style="list-style-type: none"> ▶ swap -d ▶ swapoff
Migrate page space between different disks	vxevac (available only if the page space area is under Veritas Volume Manager)	migratepv

Table A-48 shows AIX 5L JFS and JFS2 functions.

Table A-48 AIX 5L JFS and JFS2

Function	JFS	JFS2
Architectural maximum file system size	1 terabyte (TB)	4 petabyte (PB)
Architectural maximum file size	64 GB	4 PB
Number of i-nodes	Fixed, set at file system creation	Dynamic
i-node size	128 bytes	512 bytes
Fragment size	512	512
Block size	4096	4096

Function	JFS	JFS2
Directory organization	Linear	B-Tree
Compression	yes	no
Default ownership at creation	sys.sys	root.system
Set Group ID (SGID) of default file mode	SGID=on	SGID=off
Quotas	yes	yes

Table A-49 shows the directories (file system organization) on Solaris and AIX 5L.

Table A-49 File system organization

File system or directory	Solaris	AIX 5L
/	Root file system	Root file system
/etc	Configuration files	Configuration files
/dev	Special device files	Special device files
/var	Logs and spool area	Logs and spool area
/opt	Application and Solaris packages area	Application area
/tmp	Temporary files and swap area	Temporary files
/usr/bin	OS commands and shell scripts	OS commands and shell scripts
/bin	Symbolic link for /usr/bin	Symbolic link for /usr/bin
/sbin	Files used in initialization process	Files used on initialization process
/export/home	Home area	N/A
/home	N/A	Home area
/proc	Virtual file system for processes management	Virtual file system for processes management
/lib	Symbolic link for /usr/lib	Symbolic link for /usr/lib
/u	N/A	Symbolic link for /home

Physical disk and Logical Volume Manager

Table A-50 shows physical disk and LVM management in Solaris and LVM.

Table A-50 Physical disk and LVM management

Task	Solaris with physical disk partition	LVM on AIX 5L
Concat and stripe volume management	N/A	Available
Online file system management for size extend and reduce	N/A	Available
Mirror management	N/A	Available

Table A-51 shows Solaris VM and AIX 5L LVM.

Table A-51 Solaris VM and AIX 5L LVM

Volume management task	Solaris VM	AIX 5L LVM
Create a volume group	N/A	mkvg
Create a logical volume	metainit volumename raidtype devices...	mklv
Enable the volume or volume group	N/A	varyonvg
Disable the volume or volume group	N/A	varyoffvg
Export a volume group	N/A	exportvg
Delete the volume or volume group	metaclear	rm1v
Add a device to the volume or volume group	<ul style="list-style-type: none"> ▶ metattach or ▶ metainit 	extendvg
Delete a device from the volume or volume group	metadetach	reducevg
Create a soft partition or logical volume (no RAID)	metainit -p	mklv (see options on man pages)

Volume management task	Solaris VM	AIX 5L LVM
Create a soft partition or logical volume (RAID 0)	metainit with RAID 0 on devices first, then metainit -p to create the soft partition volume	mk1v (see options on man pages)
Create a soft partition or logical volume on a specific device	Same as above, but the second metainit -p will have the device name at the end of the command line	mk1v (see options on man pages)
Delete a soft partition or logical volume	metaclear	rm1v
Extend a volume or logical volume	metadetach Volname devicename	extendlv
Extend a file system after volume has been grown	growfs	chfs
Reduce a volume or logical volume	metadetach Volname devicename	chfs

Table A-52 shows Veritas and AIX 5L LVM terminology.

Table A-52 Veritas and LVM terminology

AIX 5L LVM	Veritas VM
Physical volumes	Disk media
Volume groups	Disk groups
Physical partitions	Subdisks
Logical partition	Plex
Logical volume	Volume
Logical volume mirrors	Logical partition copies

Table A-53 shows Veritas VM and LVM on AIX 5L.

Table A-53 Veritas VM and LVM on AIX 5L

Task	Veritas VM	LVM on AIX 5L
Administration tool	<ul style="list-style-type: none"> ▶ <code>vxdiskadm</code> or ▶ <code>vea</code> 	<ul style="list-style-type: none"> ▶ <code>smit lvm</code> or ▶ <code>wsm</code>
Check license	<code>vxlicrep</code>	No licence required
See disks	<code>vxdisk list</code>	<code>lspv</code>
Add a new disk	<code>vxdiskadd</code>	<code>extendvg</code>
Migrate a disk	<code>vxevac</code>	<code>migratepv</code>
Migrate a logical partition to another disk	N/A	<code>migratelp</code>
Start a volume	<code>vxvol start</code>	You put the <code>vg</code> on line with <code>varyonvg</code>
Stop a volume	<code>vxvol stop</code>	You put the <code>vg</code> offline with <code>varyoffvg</code>
List disk groups or volume groups	<code>vxvg list</code>	<code>lsvg</code>
Display information about disk group	<code>vxprint</code>	<code>lsvg</code>
Create a disk group	<code>vxvg init</code>	<code>mkvg</code>
Export a disk group or volume group	<code>vxvg deport</code>	<code>exportvg</code>
Import a disk group or volume group	<code>vxvg import</code>	<code>importvg</code>
Remove a disk from a disk group	<code>vxvg -g dname rmdisk</code>	<code>reducevg</code>
Add a disk to a disk group	<code>vxdiskadd</code>	<code>extendvg</code>
Display information about logical volume	<code>vxprint</code>	<code>lslv</code>
Create a logical volume	<code>vxassist make</code>	<code>mklv</code>
Extend a logical volume	<ul style="list-style-type: none"> ▶ <code>vxassist growto</code> or ▶ <code>vxassist growby</code> 	<code>extendlv</code>
Change logical volume settings	<code>vxedit set</code>	<code>chlv</code>

Task	Veritas VM	LVM on AIX 5L
Remove a logical volume	<ul style="list-style-type: none"> ▶ <code>vxassist remove</code> ▶ <code>vxedit rm</code> 	<code>rm1v</code>
Report statistics for volumes	<code>vxstat</code>	<code>lvmstat</code>
Extend a file system	<code>vxresize</code>	<code>chfs</code>
Shrink a file system	<code>vxresize</code>	<code>chfs</code>
Mirror a logical volume	<ul style="list-style-type: none"> ▶ <code>vxassist or</code> ▶ <code>vxmirror</code> 	<ul style="list-style-type: none"> ▶ <code>mk1vcopy or</code> ▶ <code>mirrorvg</code>

Troubleshooting

This section describes the troubleshooting options available for various problems that you might face.

Managing core files

Table A-54 describes core file administration in Solaris and AIX 5L.

Table A-54 Core file administration

Task	Solaris	AIX 5L
Modify core file settings, for example, name	<code>coreadm</code>	<code>chcore</code> (new w/AIX 5L V5.3)
Determine what process caused the core	<code>file core-filename</code>	<code>file core-filename</code>
Control the size of core file	<ul style="list-style-type: none"> ▶ <code>coreadm</code> ▶ <code>ulimit -c</code> ▶ <code>vi /etc/system</code> 	<ul style="list-style-type: none"> ▶ <code>chcore</code> ▶ <code>ulimit -c</code> ▶ <code>vi /etc/security/limits</code>
Force a running process to dump core (without stopping the process)	<code>gcore</code>	<code>gencore</code>
Gather core file and associated binaries and libraries	<code>explorer</code> (obtained from SunSolve)	<code>snapcore</code>

Task	Solaris	AIX 5L
Examine core file	<ul style="list-style-type: none"> ▶ pstack ▶ pmap ▶ pldd ▶ pflags ▶ pcred 	<ul style="list-style-type: none"> ▶ adb ▶ dbx
Debugger	<ul style="list-style-type: none"> ▶ adb ▶ gdb ▶ mdb 	<ul style="list-style-type: none"> ▶ adb ▶ dbx
Trace a process	truss	truss

Crash dumps

Table A-55 describes crash or system dump management.

Table A-55 Crash or system dump management

Topic	Solaris	AIX 5L
Crash dump utilities	<ul style="list-style-type: none"> ▶ dumpadm ▶ savecore 	<ul style="list-style-type: none"> ▶ sysdumpdev ▶ sysdumpstart
Crash configuration	view /etc/dumpadm.conf	sysdumpdev -l
Crash analyzing tools	mdb	pstat
Crash dump default store directory	/var/crash	/var/adm/ras
Generate a system dump	N/A	<ul style="list-style-type: none"> ▶ sysdumpstart ▶ smit dump
Save a crash dump that has already been generated	savecore	savecore
System dump file administration	dumpadm	sysdumpdev
Examine a system dump	mdb	/usr/lib/errdead kdb

Networking problems

Table A-56 shows troubleshooting for network problems.

Table A-56 *Troubleshooting: Network problems*

Task	Solaris	AIX 5L
Display interface settings	<code>ifconfig</code>	<code>ifconfig</code>
Display interface status and statistics	<code>netstat -i</code>	<code>netstat -i</code>
Configure interface	<code>ifconfig</code>	<code>ifconfig</code>
Check various network statistics	<code>netstat</code>	<code>netstat</code>
Check Domain Name System (DNS) resolver	<code>view /etc/resolv.conf</code>	<ul style="list-style-type: none"> ▶ <code>view /etc/resolv.conf</code> ▶ <code>smit namerslv</code>
Check name services configuration	<code>view /etc/nsswitch.conf</code>	<code>view /etc/netsvc.conf</code>
Display kernel network parameters	<ul style="list-style-type: none"> ▶ <code>ndd /dev/ip (\?)parameter</code> ▶ <code>ndd /dev/tcp (\?)parameter</code> 	<code>no -a</code>
Configure kernel network parameters	<code>ndd -set driver parameter</code>	<code>no -option Tunable</code>
Check for network link	<code>ndd driver link_status</code>	<code>netstat -v grep -i link</code>
Query DNS	<ul style="list-style-type: none"> ▶ <code>nslookup</code> ▶ <code>dig</code> 	<code>nslookup</code>
Check routing table	<code>netstat -r</code>	<code>netstat -a</code>
Check Address Resolution Protocol (ARP) entries	<code>arp -a</code>	<code>arp -a</code>
Test for connectivity	<code>ping</code>	<code>ping</code>
Check IP path	<code>traceroute</code>	<code>traceroute</code>
Capture network packets	<code>snoop</code>	<code>iptrace</code>

Using logs to troubleshoot

Table A-57 shows how to use logs to troubleshoot.

Table A-57 *Logging*

Task	Solaris	AIX 5L
Daemon for syslog	<code>/usr/sbin/syslogd</code>	<code>/usr/sbin/syslogd</code>

Task	Solaris	AIX 5L
Configuration file for syslog	<code>/etc/syslog.conf</code>	<code>/etc/syslog.conf</code>
Refresh syslogd after a change to configuration file	<code>kill -HUP syslogd-pid</code>	<code>refresh -p syslogd-pid</code>
Diagnostics messages for bootup problems	<code>/var/adm/messages</code> (if kern.debug messages are being logged)	<code>/var/adm/ras/bootlog</code>

File systems

Table A-58 shows troubleshooting for file systems.

Table A-58 Troubleshooting: File systems

Task	Solaris	AIX 5L
Display shared or exported file systems	<code>share</code>	<code>exportfs</code>
Display mounted file systems	<code>df</code>	<code>df</code>
Display detailed information about mounted file systems	<code>mount</code>	<code>mount</code>
Display NFS server's export list	<ul style="list-style-type: none"> ▶ <code>showmount -e hostname</code> ▶ <code>dfshares</code> 	<code>showmount -e hostname</code>
Display registered rpcbind/portmap processes	<code>rpcinfo -p hostname</code>	<code>rpcinfo -p hostname</code>
Display open files	<code>lsof</code> (freeware)	<code>lsof</code> (freeware)


System and user problems

Table A-59 shows troubleshooting for system and user problems.

Table A-59 Troubleshooting: System and user problems

Task	Solaris	AIX 5L
Trace system calls and signals	<code>truss</code>	<code>truss</code>
Print shared library dependencies	<ul style="list-style-type: none"> ▶ <code>ldd</code> ▶ <code>dump</code> 	<ul style="list-style-type: none"> ▶ <code>ldd</code> ▶ <code>dump</code>
Report interprocess communication (IPC) status	<code>ipcs</code>	

Task	Solaris	AIX 5L
Display and manage system resources available to a user or process	<ul style="list-style-type: none"> ▶ ulimit ▶ view /etc/system 	<ul style="list-style-type: none"> ▶ ulimit ▶ view /etc/security/limits
Identify which user or process is using a file or socket	fuser	fuser
Send signals to processes	<ul style="list-style-type: none"> ▶ kill ▶ pkill 	kill
List current processes	ps	ps
List current processes in an interactive and iterative format	top (on companion CD)	topas
Report system activity	sar	sar
Display virtual memory statistics	vmstat	vmstat
Display I/O statistics	iostat	iostat
Display system error log	dmesg	errpt
Perform memory test	Downloadable from Sun	rmss



Quick reference: Comparable commands and configuration files

This appendix contains the following tables:

- ▶ Table B-1 on page 500 shows the configuration file comparisons between Solaris and AIX 5L
- ▶ Table B-2 on page 501 shows the command equivalencies between the two operating systems

Configuration and other files

Table B-1 provides a quick reference to compare the names and the locations of some key configuration files in Solaris and AIX 5L.

Attention: AIX 5L configuration must be modified using commands unless the AIX 5L documentation specifies otherwise.

Table B-1 Configuration and other files

Solaris	AIX 5L	Comment
<ul style="list-style-type: none"> ▶ /etc/auto_master ▶ /etc/auto_home 	<ul style="list-style-type: none"> ▶ /etc/auto.master ▶ /etc/auto.home 	
/etc/default/login	/etc/security/login.cfg	
<ul style="list-style-type: none"> ▶ /etc/defaultdomain ▶ /var/yp/binding/domainname/ypservers 	N/A	Stored in Object Data Manager (ODM)
/etc/dfs/dfstab	/etc/exports	
<ul style="list-style-type: none"> ▶ /etc/ftpusers (Solaris 8) ▶ /etc/ftpd/ftpusers (Solaris 9) 	/etc/ftpusers	
/etc/ftpd/ftpass	/etc/ftpaccess.ctl	
/etc/inet/ (directory)	<ul style="list-style-type: none"> ▶ /etc/hosts ▶ /etc/services ▶ /etc/inetd.conf 	
/etc/inet/services	/etc/services	
/etc/inetd.conf	/etc/inetd.conf	
/etc/krb5/krb5.conf		.
/etc/mime.types	/etc/magic	
/etc/mnttab	N/A	Information stored in ODM
/etc/pam.conf	/etc/pam.conf	
/etc/printers.conf	/etc/qconfig	AIX 5L printing subsystem is quite different from the System V used in Solaris
/etc/syslog.conf	/etc/syslog.conf	Slightly different format

Solaris	AIX 5L	Comment
/etc/system	/etc/tunables (directory)	Do not edit directly. Use tuning commands.
/etc/vfstab	/etc/filesystems	Very different format
/usr/share/lib/zoneinfo/*	/usr/share/lib/zoneinfo/*	
<ul style="list-style-type: none"> ▶ /var/adm/messages ▶ /var/log/syslog 	dependant on /etc/syslog.conf	Also refer to errpt command
/var/spool/cron/crontabs/root	/var/spool/cron/crontabs/root	Use crontab command to edit

Table B-2 provides a quick reference of some comparable commands between Solaris and AIX 5L.

Table B-2 Comparable commands

Solaris	AIX 5L	Usage
/sbin/swapadd	mkps	Enable swap devices
admintool	smit	Admin graphical user interface (GUI)
appttrace	<ul style="list-style-type: none"> ▶ strace ▶ truss 	Application programming interface (API) tracing
arch -k	uname -m	List machine type
devfsadm	cfgmgr	Add device without reboot
df -k	df -k	File system allocation in units of kilobytes
<ul style="list-style-type: none"> ▶ getfacl ▶ setfacl 	<ul style="list-style-type: none"> ▶ aclget ▶ aclput 	Get and set access control list (ACL)
gzcat file tar -xvf -	gzcat file tar -xvf -	Unbundle compressed tape archive (TAR) file
lpsched	qdaemon	Printer daemon
modinfo	N/A	List loaded kernel modules
mountall	mount -a	Mount all entries in fstab/filesystems
mvdir	mv	Move a directory
nawk	nawk	Awk scripting language

Solaris	AIX 5L	Usage
patchadd	installp -a	Update package
<ul style="list-style-type: none"> ▶ patchrm ▶ pkgrm 	installp -u	Remove package
pkgadd	install_all_updates	Add package
pkgchk	lppchk -v	Verify package
<ul style="list-style-type: none"> ▶ pkginfo ▶ pkgparam 	lsipp -al	Query packages
<ul style="list-style-type: none"> ▶ prionctl -e ▶ nice 	nice	Start a process with a given priority
<ul style="list-style-type: none"> ▶ prionctl -s ▶ renice 	renice	Change the priority of a running process
prstat	topas	Report process statistics
prtdiag	alog	Error reporting tool
prvtoc	N/A	AIX 5L does not have a disk slice concept like Solaris
ps -ef	ps -ef	List all system processes
snoop	tcpdump	Network packets sniffer
tip	tip	Serial port access program
<ul style="list-style-type: none"> ▶ truss ▶ sotruss 	truss	Tracing
umountall	umount -a	Unmount entries in mtab
useradd	mkuserr	Add a user account
who -r	who -r	Show run level



AIX 5L Object Data Manager

This appendix describes the following characteristics about the AIX 5L Object Data Manager (ODM):

- ▶ “Overview” on page 504
- ▶ “Object Data Manager components” on page 504
- ▶ “Object Data Manager commands” on page 504
- ▶ “Changing the attribute values” on page 505
- ▶ “Location and contents of the Objects Data Manager repository” on page 506
- ▶ “Object Data Manager device configuration” on page 507

Overview

The ODM is a repository for information about the system. It contains device support, vital product data about the devices, and software support for the devices.

Object Data Manager components

There are three basic components of ODM:

- ▶ Object classes
The ODM consists of many database files, where each file is called an object class.
- ▶ Objects
Each object class consists of objects. Each object is one record in an object class.
- ▶ Descriptors
The descriptors describe the layout of the objects. They determine the name and the data type of the fields that are a part of the object class.

Object Data Manager commands

Following is a list of the commands that you can use to access the ODM:

- ▶ Create ODM classes using the **odmcreate** command. This command has the following syntax:

```
odmcreate descriptor_file.cre
```

The file `descriptor_file.cre` contains the class definition for the corresponding ODM class. Usually, these files have the suffix `.cre`.
- ▶ Delete an entire ODM class using the **odmdrop** command. This command has the following syntax:

```
odmdrop -o object_class_name
```

The name *object_class_name* is the name of the ODM class you want to remove. Be *very careful* with this command because it removes the complete class immediately.
- ▶ View the underlying layout of an object class using the **odmshow** command. The syntax is:

```
odmshow object_class_name
```

Table C-1 shows an extraction from ODM class PdAt, where four descriptors (uniquetype, attribute, deflt, and values) are shown.

Table C-1 Example of ODM class PdAt

Unique type	Attribute	Deflt	Value
tape/scsi/4mm4GB	block_size	1024	0-16777215,1
disk/scsi/1000mb	pvid	none	
tty/rs232/tty	login	disable	enable, disable

The system administrators usually work with objects. The **odmget** command queries objects in classes. Executing this command with only a class name as a parameter lists the complete class information in a stanza format. Use the **-q** flag to list only specific records. To add new objects, use **odmadd**. To delete objects, use **odmdelete**. To change the objects, use **odmchange**. These commands are explained in the next section.

All the ODM commands use the ODMDIR environment variable, which is set in the /etc/environment file. The default value of ODMDIR is /etc/objrepos.

Changing the attribute values

The ODM objects are stored in a binary format, which means that you must work with the ODM commands to query or change any objects.

Following is the procedure used in changing an object's attribute:

The **odmget** command shown in Example C-1 picks all the records from the PdAt class, where "uniquetype" is equal to "tape/scsi/8mm" and "attribute" is equal to "block_size". In this instance, only one record must be matched. The information is redirected into a file that can be changed using an editor. In this example, the default value for the block_size attribute is changed to 1024 from 512.

Example: C-1 Changing attributes

```
# odmget -q"uniquetype=tape/scsi/8mm and attribute=block_size" PdAt >
file
# vi file
PdAt:
    uniquetype = "tape/scsi/8mm"
    attribute = "block_size"
    deflt = "512"
    values = "0-245760,1"
    width = ""
```

```

        type = "R"
        generic = "DU"
        rep = "nr"
        nls_index = 6
# odmchange -o PdAt -q"uniquetype=tape/scsi/8mm and
attribute=block_size" file
# odmget -q "uniquetype=tape/scsi/8mm and attribute=block_size" PdAt

PdAt:
    uniquetype = "tape/scsi/8mm"
    attribute = "block_size"
    deflt = "512"
    values = "0-245760,1"
    width = ""
    type = "R"
    generic = "DU"
    rep = "nr"
    nls_index = 6

```

Note: Be cautious when changing the values in the ODM because incorrect ODM settings can have adverse effects on system operation.

Location and contents of the Objects Data Manager repository

The ODM contains two important types of device information. One is *predefined* device information, which describes all the supported devices. The other is *customized device* information, which describes all the devices that are actually attached to the system.

To support the diskless, dataless, and other workstations, the ODM object classes are held in three repositories. They are:

► /etc/objrepos

Contains the customized devices object classes and the four object classes used by the Software Vital Product Database (SWVPD) for the / (root) part of the installable software product. The root part of software contains files that must be installed on the target system. These files cannot be shared in an AIX 5L network. This directory also contains symbolic links to the predefined devices object classes, because the ODMDIR variable is set to /etc/objrepos.

- ▶ /usr/lib/objrepos
Contains the predefined devices object classes, SMIT menu object classes, and the four object classes used by SWVDP for the /usr part of the installable software product. The object classes in this repository can be shared across the network by /usr clients, and dataless and diskless workstations. The software installed in the /usr-part can be shared across a network by AIX 5L systems only.
- ▶ /usr/share/lib/objrepos
Contains the four object classes used by the SWVDP for the /usr/share part of the installable software product. The /usr/share part of a software product contains files that are not hardware dependent. They can be used on other UNIX systems also. An example is terminfo files that describe terminal capabilities. Because terminfo is used on many UNIX systems, terminfo files are part of the /usr/share part of a system product.

Object Data Manager device configuration

This topic explains the basics of device configuration in ODM. Support for the devices is implemented in ODM in different object classes. The predefined device class names start with *Pd* and the customized devices class names start with *Cu*.

The following sections describe the different predefined and customized object classes.

Predefined Devices (PdDv)

The predefined devices object class contains entries for all the devices supported by the system. A device that is not a part of this ODM class cannot be configured on an AIX 5L system.

Example C-2 shows the sample PdDv information. You can get this information by running the **odmget PdDv** command.

Example: C-2 Predefined devices (PdDv)

```
PdDv :  
    type = "150mb"  
    class = "tape"  
    subclass = "scsi"  
    prefix = "rmt"  
    devid = ""  
    base = 0  
    has_vpd = 1
```

```
detectable = 1
chgstatus = 0
bus_ext = 0
fru = 1
led = 2417
setno = 54
msgno = 1
catalog = "devices.cat"
DvDr = "tape"
Define = "/etc/methods/define"
Configure = "/etc/methods/cfgsctape"
Change = "/etc/methods/chggen"
Unconfigure = "/etc/methods/ucfgdevice"
Undefine = "/etc/methods/undefine"
Start = ""
Stop = ""
inventory_only = 0
uniquetype = "tape/scsi/150mb"
```

Following are the attributes you should know about:

- ▶ **Type**

This specifies the product name or model number, for example, 150 MB tape.
- ▶ **Class**

This specifies the functional class name. A functional class is a group of device instances sharing the same high-level function, for example, tape is a functional class name representing all the tape devices.
- ▶ **Subclass**

The device classes are grouped into subclasses. The subclass scsi specifies all the tape devices that might be attached to a Small Computer System Interface (SCSI) system.
- ▶ **Prefix**

This specifies the assigned prefix in the customized database that is used to derive the device instance name and the /dev name, for example, rmt is the prefix name assigned to the tape devices. Names of tape devices will then be rmt0, rmt1, or rmt2.
- ▶ **Base**

This specifies whether a device is a base device or not. A base device is any device that forms a part of a minimal base system. During the system boot, a minimal base system is configured to permit access to the root volume group and thus, to the root file system. This minimal base system can include, for

example, the standard I/O diskette adapter and an SCSI hard drive. The device shown in Example C-2 is not a base device.

▶ Detectable

This specifies whether the device instance is detectable or nondetectable. A device whose presence and type can be electronically determined after it is actually powered on and attached to the system is said to be detectable. A value of 1 means that the device is detectable, and a value of 0 means that it is not detectable. These values are defined in the `/usr/include/sys/cfgdb.h` file.

▶ Light-emitting diode

This indicates the hexadecimal value displayed on the light-emitting diode (LED) when the configure method executes. These values are stored in decimal. The value shown on the LEDs is hexadecimal.

▶ Catalog

This identifies the file name of the National Language Support (NLS) message catalog that contains all the messages pertaining to this device.

▶ `setno` and `msgno`

Each device has a specific description, for example, 150 MB tape drive, which is shown when the device attributes are listed using the `lsdev` command. These two descriptors are used to show the message.

▶ `DvDr`

This identifies the base name of the device driver associated with all the device instances belonging to the device type, for example, `tape`. Device drivers are usually stored in the `/usr/lib/drivers` directory.

▶ Define

This names the Define method associated with the device type. All the Define method names start with the `def` prefix. This program is called when a device is brought into a defined state.

▶ Configure

This names the Configure method associated with the device type. All the Configure method names start with the `cfg` prefix. This program is called when a device is brought into the available state.

▶ Change

This names the Change method associated with the device type. All the Change method names start with the `chg` prefix. This program is called when a device is changed through the `chdev` command.

- ▶ Unconfigure

This names the Unconfigure method associated with the device type. All the Unconfigure method names start with the `ucfg` prefix. This program is called when a device is unconfigured by `rmdef`.
- ▶ Undefine

This names the Undefine method associated with the device type. All the Undefine method names start with the `und` prefix. This program is called when a device is undefined by `rmdef`.
- ▶ Start and Stop

Only logical devices support a stopped state. A stopped state means that the device driver is loaded, but no application can access the device. These attributes name the methods to start or stop a device.
- ▶ uniquetype

A key that is referenced by the other object classes. Objects use this descriptor as a pointer back to the device description in PdDv. The key is a concatenation of the class, subclass, and type values.

Predefined Attributes (PdAt)

The Predefined Attribute (PdAt) object class contains an entry for each existing attribute or each device represented in the Predefined Devices (PdDv) object class. An attribute is any device-dependent information such as interrupt levels, bus I/O address ranges, baud rates, parity settings, or block sizes. The extract of PdAt in Example C-3 shows three attributes (block size, physical volume identifier, and terminal name).

Example: C-3 Predefined attributes (PdAt)

```
PdAt:
    uniquetype = "tape/scsi/1200mb-c"
    attribute = "block_size"
    deflt = "512"
    values = "1024,512,0"
    ...
```

```
PdAt:
    uniquetype = "disk/scsi/1000mb"
    attribute = "pvid"
    deflt = "none"
    ...
```

```
PdAt:
    uniquetype = "tty/rs232/tty"
```

```
attribute = "term"
deflt = "dumb"
values = ""
...
```

Following are the key fields shown in Example C-3:

- ▶ **uniquetype**
This descriptor is used as a pointer back to the device defined in the PdDv object class.
- ▶ **attribute**
This identifies the name of the device attribute. This is the name that can be passed to the **mkdev** and the **chdev** configuration commands.
- ▶ **deflt**
This identifies the default values for an attribute. Nondefault values are stored in Customized Attribute (CuAt).
- ▶ **values**
This identifies the possible values that can be associated with the attribute name, for example, allowed values for the `block_size` attribute range from 0 - 245760, with an increment of 1.

Customized Devices

The Customized Devices (CuDv) object class contains the entries for all the device instances defined in the system. As the name implies, a defined device object is an object that a define method has created in the CuDv object class. A defined device object might or might not have a corresponding actual device attached to the system.

A CuDv object contains attributes and connections that are specific to a device. Each device, distinguished by a unique logical name, is represented by an object in the CuDv object class. The customized database is updated twice, during system boot and at runtime, in order to define new devices, remove undefined devices, or update the information for a device whose attributes have been changed.

Example C-4 shows a part of the CuDv object.

Example: C-4 Customized devices

```
CuDv:
  name = "cd0"
  status = 1
  chgstatus = 2
```

```
ddins = "scdisk"
location = "10-60-00-4,0"
parent = "scsi0"
connwhere = "4,0"
PdDvLn = "cdrom/scsi/scsd"
```

CuDv:

```
name = "hdisk0"
status = 1
chgstatus = 2
ddins = "scdisk"
location = "20-60-00-8,0"
parent = "scsi1"
connwhere = "8,0"
PdDvLn = "disk/scsi/scsd"
```

They key descriptors in CuDv are:

▶ name

A CuDv object for a device instance is assigned a unique logical name to distinguish the instance from other device instances. Example C-4 shows two devices, a CD-ROM device (cd0) and a hard disk (hdisk0).

▶ status

This identifies the current status of the device instance. The possible values are:

- Status =0: Defined
- Status =1: Available
- Status =2: Stopped

▶ chgstatus

This flag tells you whether the device instance has been altered since the last system boot. The diagnostics facility uses this flag to validate system configuration. The flag can take the following values:

- chgstatus =0: New device
- chgstatus =1: Do not Care
- chgstatus =2: Same
- chgstatus =3: Device is missing

▶ l

This descriptor typically contains the same value as the Device Driver Name descriptor in the PdDv object class. It specifies the device driver that is loaded into the kernel.

- ▶ location
This identifies the location code of the device.
- ▶ parent
This identifies the logical name of the parent device instance.

Customized Attributes

The CuAt object class contains customized device-specific attribute information. Devices represented in the CuDv object class have attributes found in the PdAt object class and the CuAt object class. There is an entry in the CuAt object class for attributes that take customized values. Attributes taking the default value are found in the PdAt object class. Each entry describes the current value of the attribute.

These objects out of the CuAt object class show two attributes that take customized values. The attribute login has been changed to enable. The attribute pvid shows the physical volume identifier that has been assigned to the hdisk0 disk.

Additional device object classes

Following are the additional device object classes:

- ▶ PdCn
The Predefined Connection (PdCn) object class contains connection information for adapters, which are sometimes called intermediate devices. This object class also includes predefined dependency information. For each connection location, there are one or more objects describing the subclasses of devices that can be connected.
- ▶ CuDep
The Customized Dependency (CuDep) object class describes the device instances that depend on other device instances. This object class describes the dependence links between the logical devices exclusively. Physical dependencies of one device on another device are recorded in the CuDv object class.
- ▶ CuDvDr
The Customized Device Driver (CuDvDr) object class is used to create the entries in the /dev directory. These special files are used from the applications to access a device driver that is a part of an AIX 5L kernel.
- ▶ CuVPD
The Customized Vital Product Data (CuVPD) object class contains vital product data (manufacturer of device, engineering level, part number, and so

on) that is useful for technical support. When an error occurs with a specific device, the vital product data is shown in the error log.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this IBM Redbook.

IBM Redbooks

For information about ordering these publications, see “How to get IBM Redbooks” on page 516. Note that some of the documents referenced here might be available in softcopy only.

- ▶ *A Practical Guide for Resource Monitoring and Control (RMC)*, SG24-6615
- ▶ *AIX 5L Differences Guide Version 5.2*, SG24-5765
- ▶ *AIX 5L Practical Performance Tools and Tuning Guide*, SG24-6478
- ▶ *An HACMP Cookbook*, SG24-4553
- ▶ *Cluster Systems Management Cookbook for pSeries*, SG24-6859
- ▶ *IBM AIX 5L Reference for HP-UX System Administrators*, SG24-6767
- ▶ *IBM BladeCenter JS21: The POWER of Blade Innovation*, SG24-7273
- ▶ *IBM Certification Study Guide eServer p5 and pSeries Administration and Support for AIX 5L Version 5.3*, SG24-7199
- ▶ *IBM eServer Certification Study Guide - AIX 5L Installation and System Recovery*, SG24-6183
- ▶ *IBM eServer Certification Study Guide - pSeries AIX System Administration*, SG24-6191
- ▶ *IBM Tivoli Storage Manager: Bare Machine Recovery for AIX with SYSBACK*, REDP-3705
- ▶ *Solaris to Linux Migration: A Guide for System Administrators*, SG24-7186

Other publications

These publications are also relevant as further information sources:

- ▶ Article on NIM Installation and Configuration
<http://www.samag.com/articles/2005/0510/>

Online resources

These Web sites and URLs are also relevant as further information sources:

- ▶ AIX Installation in a Partitioned Environment
http://publib16.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixins/aix1parins/mastertoc.htm#mtoc
- ▶ Cluster servers
<http://www-03.ibm.com/servers/eserver/clusters>
- ▶ Hardware Management Console for pSeries Installation and Operations Guide
http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/hardware_docs/pdf/380590.pdf
- ▶ IBM Systems Hardware Information Center
<http://publib.boulder.ibm.com/infocenter/eserver/v1r3s/index.jsp>
- ▶ Solaris 9 System Administration Guide
<http://docs.sun.com/app/docs/doc/817-6958>

How to get IBM Redbooks

You can search for, view, or download IBM Redbooks, IBM Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy IBM Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

Symbols

.com 136
.diag 136
.ucode 136
/ 401
/dev 158
/dev/dsk 158
/dev/hd6 23
/dev/hdisk 159
/devices 158
/etc/.dynamic_routing 199
/etc/auto.master 115
/etc/auto/maps 115
/etc/auto_master 115
/etc/clsntp.conf 210
/etc/cron.d/cron.allow 255
/etc/cron.d/cron.deny 255
/etc/default/inetd 202, 469
/etc/default/nfs 470
/etc/defaultdomain 189, 466
/etc/defaultrouter 189, 201, 466, 468
/etc/dfs/dfstab 114, 470
/etc/dhcpsd.ar 203
/etc/dhcpsd.cr 203
/etc/environment 22, 342–343
/etc/exports 113–114, 470
/etc/filesystems 109
/etc/group 348
/etc/hostname 189, 466
/etc/hostname.interface 184, 198
/etc/hosts 22
/etc/inet* 189, 466
/etc/inet/hosts 198
/etc/inet/ipnodes 198
/etc/inet/netmasks 198
/etc/inet/services 185
/etc/inetd.conf 202–203, 254, 469
/etc/inetinit 199
/etc/init.d/cron 255
/etc/init.d/dhcp stop or start 204, 470
/etc/init.d/inetsvc 469
/etc/init.d/inetsvc stop 202, 469
/etc/init.d/nfs.client 114
/etc/init.d/nfs.client start 470
/etc/init.d/nfs.client stop 470
/etc/init.d/nfs.server 114
/etc/init.d/nfs.server start 470
/etc/init.d/nfs.server stop 470
/etc/inittab 24, 226, 255
/etc/named.conf 204
/etc/netmasks 184, 189, 466
/etc/netsvc.conf 189, 467
/etc/nodename 189, 466
/etc/nsswitch.conf 189, 467
/etc/passwd 332, 344–346
/etc/path_to_inst 240
/etc/profile 342, 344
/etc/rc*.d/ 250
/etc/rc.d 24
/etc/rc.shutdown 24
/etc/resolv.conf 189, 467
/etc/security/envIRON 342
/etc/security/group 349
/etc/security/limits 356
/etc/security/passwd 344–346
/etc/services 202–203, 254, 469
/etc/shadow 344
/etc/skel/local.cshrc 341
/etc/skel/local.login 341
/etc/skel/local.profile 341
/etc/syslog.conf 17
/etc/system 4
/etc/utmp 330
/etc/vfstab 109
/sbin/init 225
/usr/lib/cron/at.allow 256
/usr/lib/cron/at.deny 256
/usr/samples/tcpip/addrS.awk 205
/usr/samples/tcpip/hosts.awk 205
/usr/samples/tcpip/named.boot 204
/usr/samples/tcpip/named.data 205
/usr/sbin/crfs 110
/usr/sbin/in.daemon 202, 469
/usr/sbin/inetd -s 202, 469
/usr/websm/pc_client/ 272
/var/adm/cron/at.allow 256
/var/adm/cron/at.deny 256

/var/adm/cron/cron.allow 255
/var/adm/cron/cron.deny 255
/var/adm/messages 15
/var/spool/cron/atjobs 256
/var/spool/cron/crontabs 255
/var/tmp/snmpd.log 211

Numerics

32-bit 32
64-bit RISC 33
888 24

A

acctcms 260
acctcom 259
acctdisk 259
acctmerg 260
accton 260
acctprc1 260
acctprc2 260
acctusg 259
adapter 287
add
 local print queue 284
 print queue 318, 483
 printer 318, 482
 serial terminal (TTY) in AIX 5L 169
 users 325
Admin 7
admin
 tool 7, 262
 wizard 7
AIX 5L
 error log 15
 print subsystem 281
alternate destination disk 56
alternate disk installation 56
alternate disk rootvg cloning 58
alternate mksysb install 62, 64
American Standard Code for Information Inter-
change, *See* ASCII
APAR 148
Apple 30
applied state 141
architecture 31
 types 31
ASCII 11
Authorized Program Analysis Report, *See* APAR

automatic tunnel 192
automounter 114
available print queue 295

B

bandwidth 246
basic system installation 48
BGP 200
block device 159
boot 214
 default boot 214
 emergency boot 214
 interactive boot 215
 interactive start of services 215
 list 221, 224
 reconfiguration boot 215
 recovery boot 215
 single user 215
 troubleshooting 430
 verbose boot 215
Border Gateway Protocol, *See* BGP
bundle 139
business applications 33

C

CA Unicenter 15
cancel printing job 305, 318, 482
Canon 30
Capacity on Demand 37
central administration 68
cfgadm 240
cfgmgr 92, 158, 166
change
 print queue 319, 483
 user 331
character device 284
chargefee 259
check status 299
chfn 345
chfs 129, 132
chgroup 352
chitab 22
chlv 105, 132
chpath 179
chps 119
chsec 325, 348
chuser 325, 339, 345, 356
cifs 111

- CIM 261
 - query language 261
 - XML 261
- classical system 31
- client/server environment 69
- clone 60
- CMOS-6S 31
- command
 - alog 223
 - chdev 509
 - lp 294–295
 - lpfilter 281
 - lpforms 281
 - lpget 281
 - lsdev 161, 509
 - mksysb 56
 - odmadd 16, 505
 - odmchange 505
 - odmcreate 504
 - odmdelete 505
 - odmdrop 504
 - odmget 505, 507
 - odmshow 504
 - oslevel 61, 140, 147
 - oslevel -r 147
 - passwd 323
 - rmdef 510
- commit state 141
- committing software 144
- Common Information Model Object Manager 262
- compression 417
- configured tunnels 192
- core files 433
- cplv 413
- crash dump 23, 436
- crontab 254
- customize
 - attributes 513
 - devices 511
 - install 68

D

- Data Encryption Standard, *See* DES
- daystar 30
- DDNS 203
- route add 201, 468
- default print subsystem 310
- default queue 295

- Defense Communications Network Local-Network Protocol 200
- delete print queue 291
- DES 140
- descriptor 504
- DEV_WAIT 304
- device driver 287
- DHCP 202
 - client 203
 - Linux 203
 - server 203
 - Solaris 203
 - /etc/inet/dhcpsvc.conf 203
 - dhcpconfig, dhcpconfig 203
 - dhcprm, dhcprm 203
 - dhtadm, dhtadm 203
 - in.dhcpd 203
 - pntadm, pntadm 203
- dhcraction 189, 203, 467, 469
- dhcpconfig 189, 203, 467, 469
- dhcpinfo 189, 204, 467, 469
- dhcprm 189, 203–204, 467, 469–470
- dhcprd 189, 203, 467, 469
- dhcps 203
- dhcpsconf 189, 203, 467, 469
- dhcpsd 204, 469
- dhcptab 203
- dhtadm 189, 203, 467, 469
- diag 167
- dial-in administration 282
- disable 293
 - print queue 293
- disk
 - disk partitioning 92
 - groups 130
 - media 130
- diskless 69
- display
 - print queue status 318, 482
 - settings of print queue 319, 483
- Distributed Management Task Force, *See* DMTF
- DLPAR 39, 243–244
- DMTF 261
- DNS 204
- dodisk 259
- domain 243
- Domain Name System, *See* DNS
- Dynamic Domain Name System, *See* DDNS
- Dynamic Host Configuration Protocol, *See* DHCP

dynamic LPAR, *See* DLPAR
dynamic reconfiguration 165, 243
dynamic routing 198
 AIX 200

E

easy NIM client configuration 72
EGP 200
EMC powerpath 175
enable
 print queue 293
ESS 176
Etherchannel 195
exclude 407
exportfs directory 470
Exterior Gateway Protocol, *See* EGP

F

failover 177
 solution 195
file set
 AIX 5L 135
 naming convention 135
file system 375
File Transfer Protocol, *See* FTP
FirePower 30
firmware 220
fix 147
 database 148
flarcreate 400
floating point computation 32
frequencies 32
FTP 201

G

gated 200–201, 468
grace period 257
graphics 32
grep 16
group 322, 347
 add 323, 325, 349
 command 348
 del 323
 delete 353
 modify 323, 351

H

HACMP 24
hard limits 256
hardware location codes in AIX 5L 161
Hardware Management Console, *See* HMC
hdisk 159
header/trailer page options 296
High Availability Cluster Multi-Processing, *See* HACMP
High Sierra File System, *See* HSFS
Hitachi 176
HMC 21, 37, 273, 275
holding and releasing a printing job 307
home directory 322
host name 240
hosted installation 37
hot-pluggable 165
HP OpenView ITO 15
HSFS 110

I

I/O feature cards 30
IBM Tivoli Distributed Monitoring 15
IBM TotalStorage Enterprise Storage Server, *See* ESS
ICMP 200
identifier 226
IETF 262
Industry Standard Architecture, *See* ISA
inet 185, 190
inet6 190
inetd 201
 /etc/default/inetd 201, 391
 /etc/inetd.conf 201
 /etc/services 201
 ENABLE_CONNECTION_LOGGING 201
 ENABLE_TCPWRAPPERS 201, 391
Infoprint Manager 281
init 226
init 5 165
initialization files 322
inittab 21
install software 142
installp 149
instfix 148
Integrated Virtualization Manager 38
interface backup adapter 196
Intermediate System to Intermediate System 200

- Internet Control Message Protocol, *See* ICMP
- Internet Engineering Task Force, *See* IETF
- interprocess 22
- iostat 448, 498
- IP routing 198
 - Linux 199
 - Solaris 198
 - /etc/defaultrouter 198
 - /etc/gateways 198
 - /etc/notrouter 198
 - /usr/sbin/in.rdisc 198
 - ndpd 199
 - RDISC 198
 - RIP 198
 - ripngd 199
- ipaddr 201, 468
- ipreport 190, 467
- iptrace 190, 467
- IPv4 184, 190, 198
 - Linux
 - /etc/hosts 188
 - /etc/protocols 188
 - /etc/resolv.conf 188
 - /etc/services 188
 - Solaris
 - /etc/bootparams 185
 - /etc/defaultdomain 185
 - /etc/defaultrouter 185
 - /etc/ethers 185
 - /etc/inet/hosts 185
 - /etc/inet/protocols 185
 - /etc/inet/services 185
 - /etc/netmasks 184
 - /etc/nodename 184
 - /etc/nsswitch.conf 185
 - /etc/resolv.conf 185
- IPv4 tunnels 192
- IPv6 190–192, 198
 - Linux 191
 - Solaris 191
 - /etc/hostname6.interface 191
 - /etc/inet/ipnodes 191
- IPv6 in AIX 5L 191
- IPv6 in Solaris 191
- ISA 30
- ISA slots 30

J

- j2edlimit 257
- Java 1.3 14
- jfs2 111
- job processing 296
- journaling 123

K

- kernel parameters 23
- kill -HUP inetd process 202, 469
- kill in.daemon-pid 202, 469

L

- large file systems 123
- LDAP 206
- LED 21, 222
- Licensed program product, *See* LPP
- light-emitting diode, *See* LED
- Lightweight Directory Access Protocol, *See* LDAP
- limit classes 256
- Linux 14
- list
 - hardware vital product data 164
 - user 323, 335
- load balance 175, 195
 - by IP address 197
 - by MAC 196
 - by round robin 196
- local print queue 284
- logical disk device
 - Solaris 158
- Logical Partition, *See* LPAR
- Logical Volume 105, 130
 - mirrors 130
- logical volume manager, *See* LVM
- login 325, 345
- logs 438
- LPAR 21, 37, 105, 130, 243–244
 - copies 130
- LPP 135, 139
- lpq 302
- lpr 294
- lprm 305
- lpset 280
- lpshut 280
- lpstat 293, 302
- lpssystem 281
- lpusers 281

ls 5
lsattr 164, 177, 240
lscfg 160, 164, 240
lsdev 163, 240
lsitab 22
lslv 105, 132
lspath 159
lsps 119, 160
lspv 61, 131
lsslot 167, 169, 240
lssrc 250
lssrc -ls dhcpcd 204, 469
lssrc -s named 205
lssrc -t subservername 202, 469
lsuser 325, 337, 345, 356
lsvg 132, 160
LVM 96
lvmstat 132

M

mail service 209
maintenance level 140, 147
Management Information Base 262
Management Information Base, *See* MIB
master 68
MCA 31
MCA-based RS/6000 222
mdb utility 433, 436
message queue 22
messages/diagnostics 296
metaclear 129
metadetch 129
metainit 128–129
metattach 129
MIB 262
micropartitioning 38
microprocessor 30, 32
Microsoft Multipath I/O, *See* MPIO
migratelp 131
migratepv 119, 131
mirroring 107
mirrorvg 107–108, 132
mixed IPv4 and IPv6 192
mk 407
mkcd 404
mkdev 158, 168–169
mkfs 109, 159
mkgroup 350

mkitab 22, 230
mklv 105, 128–129, 132
mklvcopy 107, 132
mknfs 112
mknfsexp 114
mkpath 179
mkps 120
mkque 289
mkqudev 290
mksysb 62, 401
mksysb image 62
mkuser 324, 326, 342, 345, 356
mkvg 128, 132
mlv 129
monolithic installation 36
motif 11–12, 266
Motorola 30
mount 159
move job between queues 308
MPIO 176
mt 418
multimedia 32
Multipath 93
multipathing 175

N

name resolution 69
namerslv 189, 467
nnd 189, 240, 467
nnd /dev/ip 189, 467
nnd /dev/tcp 189, 467
nnd -set driver parameter 189, 467
ndpd 199, 201, 468
ndpd-router 201, 468
netstat 189, 240, 467
netstat -i 189, 467
netstat -r 189, 467
netstat -v interface 189, 467
network file system, *See* NFS
Network Information Service, *See* NIS
Network Router Discovery (RDISC) 198
network troubleshooting 445
newfs 109, 159
newgrp 348
news 344
NFS 69, 111, 231
nfsconfigure 470
NFSv4 111

NIM 407
nim_attr 69
nim_objec 69
nim_pdattr 69
NIS 206, 231
NIS and NIS+ 206
NIS+ 206
NLSPATH 343
nmon 240
no -a 189, 467
no -o Tunable=NewValue 189, 467
nonbootable 21
nonprompted installation 68
normal boot list 221
normal mode 220

O

object classes 504
Object Data Manager, *See* ODM
objects 504
ODM 4, 15, 97, 504
 database 69
Open Shortest Path First, *See* OSPF
OpenPROM 214
operational monitoring 15
operator panel 21
OPR_WAIT 304
OSPF 200
output screen 12, 267

P

package 134–135
 management 135
paging 118
paper/page options 296
parallel printers 283
Partition Load Manager 245
password 322
 files 344
patch 146
 cluster 150
 manage 262
 manager 151
patchadd 146
PatchPro Expert 152
PatchPro Interactive 152
patchrm 146
PCFS 110

PCI bus 30
PCI RS/6000 221
pcred 116
Pd 507
PdCn 513
PdDv 507
Pegasus CIM Server 262
performance 375, 475
Peripheral Component Interconnect 30
pfiles 116
pflags 116
physical partition 130
physical volume 101, 130
ping 190, 467
pioneer 30
pkgadd 134
pkgchk 134
pkginfo 134
pkgparam 134
pkgrm 134
pldd 116
plex 130
pmap 116
pntadm 189, 203, 467, 469
pop-up 11, 266
portmap 111
post 21
PostScript filters 282
POWER 30
Power Computing 30
POWER2 31
POWER3 31
POWER3 II 32
POWER4 33
PowerPath 176
PowerPC 30, 32, 221
predefined
 devices 507
Predefined Attributes 510
print
 device 284
 duplex 298
 formatted file 298
 job number 300
 job owner
 name 300
 landscape 298
 text files to PostScript 298
printer

- drivers 286
- mode 288
- model 286
- pitch 298
- type 283
- prioritize printing job 305
- proccred 116
- processes 376, 475
- procfiles 116
- procflags 116
- procldd 116
- procmap 116
- procrun 117
- procsig 117
- procstack 117
- procstop 117
- proctree 117
- procwai 117
- procwdx 117
- prstat 240
- prtconf 160, 240
- prtdiag 160, 240
- prvtoc 159
- prun 117
- ps 240, 447
- ps -ef | grep 'in.' 202, 469
- psig 117
- psrinfo 240
- pstack 117
- pstop 117
- ptree 117
- pwait 117
- pwck 353
- pwdadm 332, 345
- pwdx 117

Q

- qadm 293
- qcan 305
- qchk 293, 299, 302
- qchk -L 306
- qhld 307
- qmov 309
- qpri 305–306
- qprt 281, 294–295
- qprt -R 306
- qstatus 299
- queue 289

- device 291
- QUEUED 307
- quorum 99
- quota 256–257
- quota.group 257
- quota.user 257
- quotacheck 257
- quotaoff 257
- quotaon 257

R

- radius 30
- raw device 159
- RDAC 176
- RDISC 198
- rdump 414
- Redbooks Web site 516
 - Contact us xviii
- reducevg 129
- redundant 175
- Redundant Disk Array Controller ,See RDAC
- refresh 203, 251
- refresh -s inetd 203
- reinstall currently installed software 142
- release 147
- Reliable Scalable Cluster Technology 243, 248
- remote server 313
- remove
 - print queue 319, 483
 - user 328
- replica 128
- resource monitoring and control 24
- Resource Monitoring and Control, See RMC
- respawn 226
- restvg 410
- RIP 198
- RIP protocol 200
- ripngd 199, 201, 468
- Rlogin 201
- RMC 24, 270
- rmdev 158, 166, 170, 173
- rmgroup 353
- rmitab 22, 255
- rmlv 106, 129, 132
- rmlvcopy 108
- rmpath 179
- rmps 122
- rmuser 325, 328, 342, 345, 356

root password recovery 443
round_robin 177
route 184, 189, 199, 467
routed 200–201, 468
Routing Information Protocol, *See* RIP
rpcbind 111
rpcinfo 111
rpm 134
rrestore 415
RS/6000 SP 31
RS64 32
RS64-II 32
RSCT 243
run level 226
run multiple tasks in a GUI environment 318, 482
runacct 259

S

-s dhcpsd 204, 470
SAN 174
SAP/R3 281
sar 448, 498
savecore 436
savevg 410
scalability 68
SCSI 101
semaphore 22
send mail 209
serial printer 283
service boot list 221
Service Location Protocol 261
share
 memory 22
shared
 processing 38
showrev 146
shut down 165, 231
single interface 14
site initialization file 341
Small Computer System Interface, *See* SCSI
SMIT 4–5, 7–9, 167, 263
 ctinet6 194
 dialog screen 10
 Ether channel 196
 fast path 263
 log 264
smit inetd 202, 469
smit inetdconf 202, 469
smit mkinetvi 197
smit performance 189, 467
smit route 199
 204, 470
SMIT System Management Interface Tool, *See* SMIT
smitty alt_install 57
smitty chgenet 170
smitty chgroup 352
smitty chuser 340
smitty lsuser 338
smitty mkggroup 350
smitty mkuser 327
smitty passwd 333
smitty qcan 294, 305
smitty qchk 300
smitty qhld 307
smitty qpri 307
smitty qstart 293
smitty qstatus 299
smitty reject 149
smitty rmpq 291
smitty rmuser 329
smitty route 189, 467
smitty spooler 310
smitty telinit 230
smitty users 334
smitty rmgroup 353
snapshots 123
SNMP 210, 262
SNMP Simple Network Management Protocol, *See* SNMP
snoop 190, 447, 467, 496
soft limit 256
software
 installation image 68
 updates
 AIX 140
Software Vital Product Database 506
Solaris Management Center 7
Solaris Management Console 263
Solaris Resource Manager 243–244
spooler 313
SSA 101
start print queue 293
startsrc 113, 232, 251
startsrc -s named 205
startsrc -t subservername 202, 469
 204, 470
startsvc -g nfs 470

- startup modes 219
- static routing 198
- statistics 359
- stderr 12
- stdout 12
- stop print queue 293, 318, 482
- stopsrc 251
- stopsrc -t subservername 202, 469
- stopsvc -g nfs 470
- Storage Area Network (SAN) 93
- subdisks 130
- subserver 231
- Sun IP multipath 195
- Sun storedge traffic manager 176
- Sun trunking 195
- Sun Volume Manager 128
- SunSolve 151
- swap 118
- swapoff 119
- swapon 119
- Symmetrix 176
- syncvg 108
- Sysback 415
- sysdef 160
- sysdumpdev 24
- syslog 15
- syslog.conf 17
- system
 - bus 30
 - configuration 220
 - dump 23
- System Management Service 220
 - menu 220
- System Resource Controller 202
- System ROS 221
- System V 22
 - print subsystem 282
- sys-unconfig 184

T

- tapechk 417
- TCP/IP 69, 231
- tcpdump 190, 467
- tcpip 204, 470
- tctl 418
- telinit 229–230
- Telnet 201
- text

- formatting 296
 - print 296
- time zone 343
- time zone information 343
- topas 240
- touch 165
- trace 223
- traceroute 190, 467
- Trivial File Transfer Protocol 201
- truss 448, 497
- tunneling 192

U

- ufsdump 400
- ulimit 355
- uname 240
- UNIX file system 110
- unmirrorvg 108
- unshare directory 470
- unshareall 470
- user name 322
- useradd 323, 325, 327
- user-defined function 110
- userdel 323, 328
- usermod 323, 339

V

- varyoffvg 129, 131
- varyonvg 129, 131
- verification 61
- Veritas Dynamic Multi-Pathing 175
- Veritas Volume Manager 130
- virtual
 - I/O
 - server 38
 - printer 289
- virtual I/O 39
- Virtual IP address 197
- virtualization 244
- vmstat 448, 498
- volume 130
- volume group 102, 130
- Volume Group Descriptor Area 97
- vxassist 132
- vxdg 132
 - vxdg depor 132
 - vxdg deport 132
 - vxdg import 132

vxdisk list 131
vxdiskadd 131–132
vxdiskadm 131
vxedit 132
vxevac 119, 131
vxfs 110
vxlicrep 131
vxmirror 132
vxprint 132
vxresize 132
vxstat 132
vxvol 131

W

Web-based Enterprise Management 262
Web-based System Manager 4, 14, 282
WebSM and HMC coexisting 276
Windows 14
Work Load Manager 243, 246
470



Redbooks

Sun Solaris to IBM AIX 5L Migration: A Guide for System Administrators

(1.0" spine)
0.875" <-> 1.498"
460 <-> 788 pages



Sun Solaris to IBM AIX 5L Migration: A Guide for System Administrators



Task-based grouping of OS differences between the two environments

A comprehensive and quick transition guide

A reference for experienced system administrators

The aim of this IBM Redbook is to provide a technical reference for IT system administrators in organizations that are considering a migration from Sun Solaris to IBM AIX 5L-based systems. This book presents a system administrator view of the technical differences that exist and the methods that are necessary to complete a successful migration to AIX 5L-based systems.

This book is designed primarily as a reference for experienced Sun Solaris 8 or 9 system administrators who will be working with AIX 5L. This book is not an AIX 5L administration how-to book for system administrators who are beginners, but rather a guide for experienced administrators who have to translate a given Solaris system administration task to AIX 5L.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks