AIX Version 6.1

Release Notes

IBM

AIX Version 6.1

Release Notes

Third Edition (May 2008)

Contents

Chapter 1. Read this before installation

Note: This software may contain errors that could result in critical business impact. It is highly recommended that you install the latest available fixes prior to using this software. Fixes can be obtained from IBM System p support at the following Web site:

> `http://www14.software.ibm.com/webapp/set2/sas/f/genunix3/aixfixes.html`

These Release Notes support AIX Version 6.1.

The AIX Version 6.1 Release Notes include information that helps you install AIX Version 6.1. To view the most current version of the Release Notes, go to the online Release Notes in the AIX® Information Center at the following Web site:

`http://publib14.boulder.ibm.com/infocenter/systems/aix/topic/com.ibm.aix.resources/61relnotes.htm`

Installation tips

The latest installation hints and tips are available from the IBM® Subscription Service for UNIX® servers at:

`http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd`

These tips might contain information that are critical for successful installation of this software.

Software License Agreements

There are instances where the Software Licence Agreements (SLA) might not be displayed correctly. In this event, the License Agreements can be viewed in all languages at the following Web site:

`http://www.ibm.com/software/sla/sladb.nsf`

Software Maintenance Agreement

In AIX Version 6.1, a separate Software Maintenance Agreement (SWMA) acceptance window displays during installation immediately after the license acceptance window. The response to the SWMA acceptance (accept or decline) is stored on the system, and either response allows the installation to proceed, unlike license acceptance which requires an accept to proceed.

The SWMA acceptance window is displayed during a New Overwrite or Preservation installation from base CD media.

For base CD media New Overwrite or Preservation installations, if a non-prompted installation is desired, the **ACCEPT_SWMA** field in the control_flow stanza of the **bosinst.data** file should be set to `yes` (to accept the SMWA terms) or `no` (to decline the SWMA terms). The **ACCEPT_SWMA** field is set to blank by default.

For NIM installations, if licenses have been accepted either from the choices made when initializing the installation, or using the **ACCEPT_LICENSES** field in a customized **bosinst.data** file, then this will constitute SWMA acceptance.

Service

Fixes and problem-solving databases

You can download AIX fixes and search technical databases (including ″APARS″ and ″Tips for AIX administrators″), from the following IBM eServer™ Support Web site:

`http://www14.software.ibm.com/webapp/set2/sas/f/genunix3/aixfixes.html`

1

Chapter 2. System requirements

Review the following information to determine the minimum and recommended system requirements needed to run AIX Version 6.1.

Required hardware

Only 64-bit Common Hardware Reference Platform (CHRP) machines running selected PowerPC® 970, POWER4™, POWER5™, and POWER6™ processors that implement the POWER™ architecture Platform Requirements (PAPR) are supported.

To see if you have a supported machine, log into the machine as the root user, and run the following command:

```
prtconf | grep 'Processor Type'
```

Note: RS64, POWER3™, and 604 processors, 32-bit kernel, 32-bit kernel extensions, and 32-bit device drivers are no longer supported.

Firmware

Some AIX systems might not boot from CD-ROM

Some AIX systems might not boot from CD-ROM because of firmware issues. To determine if your system will be affected by this problem, perform the following steps before you migrate or install a running AIX 4.3, AIX 5.1, or AIX 5.2 system:

1. At the command prompt, type the following:

   ```
   lscfg -vl cd*
   ```

2. Examine the data that is returned.

   If *Part Number* is 04N2964 and *ROS Level and ID* is less than or equal to `1_04` (for example, `1_02`, `1_01`, or `1_00`), contact your local service representative. Tell your service representative that your system requires the CD-ROM firmware upgrade that is described in RETAIN® TIP H1332.

   If the data returned does not match the data described in the preceding paragraph, your system is not affected by this problem.

Minimum firmware levels required for AIX 6.1

The following table shows minimum system firmware levels required before installing or upgrading your system to AIX 6.1.

Model Number	Product Name	Minimum Firmware Level
7028-6C4	pSeries® 630 Model 6C4	3R041029
7028-6E4	pSeries 630 Model 6E4	3R041029
7029-6C3	pSeries 615 Model 6C3	3F041029
7029-6E3	pSeries 615 Model 6E3	3F041029
7038-6M2	pSeries 650 Model 6M2	3K041029
7039-651	pSeries 655 Model 651	3J041029
7040-671	pSeries 670 Model 671	3H041029
7040-681	pSeries 690 Model 681	3H041029
9114-275	IntelliStation® POWER Model 275	3F041029

Firmware updates are available at the following Web site:

`http://www14.software.ibm.com/webapp/set2/firmware/gjsn`

If you experience problems booting your POWER4 system after updating AIX or firmware, to verify and correct the value of the real-base firmware variable, perform the following steps:

1. Go to the open firmware prompt when the system is booting by typing `8` when a beep is heard or the banner displays. If applicable, the HMC can also be used to set to boot to the SMS menu. From the SMS menu, type `0` and go to the open firmware prompt.

2. At the open firmware prompt, type:

   `printenv real-base`

   The following is a sample display:

   ```
   -------------- Partition: common -------- Signature: 0x70 ---------------
   real-base                2000000              c00000
   ```

   The value following real-base must be `c00000`. If any value other than `c00000` displays, run the following command:

   `setenv real-base c00000`

3. After updating the real-base variable, reboot your system using the power switch.

Firmware upgrade required to support an alternate boot device

The requirement of upgrading firmware when installing or booting AIX 6.1 in the scenarios described in this section applies only to the systems listed in the table included at the end of this section.

Installation

Some systems might encounter installation problems when you are installing AIX 6.1 on a system that is currently installed with a earlier version of AIX or when you are installing an earlier version of AIX on a system currently installed with AIX 6.1.

A firmware upgrade is required to support the following installation scenarios:

1. When an installation device is specified using the SMS menus or the Open Firmware command-line *and* the specified device is not the first available device in the AIX bootlist.

   Note: SMS menus differ, depending on the system. On some systems, the installation device is specified under the Multiboot menus. On other systems, the installation device is specified under the Select Boot Options menus.

2. When the F5 key is selected during boot, which is the fast path to install from the CD device, *and* the CD device is not the first available device in the AIX bootlist.

No firmware upgrade is required if no installation device is specified in the SMS menus or the Open Firmware prompt *or* if the specified installation device is the first available device in the AIX bootlist.

Memory requirements

AIX Version 6.1 minimum current memory requirements vary, based on the configuration.

A general rule for a minimum current memory requirement for AIX 6.1 is 512 MB. A smaller minimum current memory requirement of 256 MB may support a configuration with a very small number of devices and where the maximum memory setting is set to match the current memory of 256 MB.

AIX 6.1 requires the minimum current memory requirement to increase as the maximum memory configuration or the number of devices scales upward, or both. Larger maximum memory configurations or additional devices scale up the minimum current memory requirement. If the minimum memory requirement is not increased along with the maximum memory requirement, the partition hangs during the initial program load (IPL).

Host Ethernet Adapter memory requirements

Configurations containing a Host Ethernet Adapter (HEA) require more memory than the 512 MB minimum. Each logical HEA port that is configured requires approximately 612 MB of memory.

IBM Tivoli Directory Server memory requirements

IBM Tivoli® Directory Server Version 6.1 requires a minimum of 256 MB RAM for the Client and a minimum of 512 MB of RAM (1 GB or more is strongly recommended) for the Server. IBM Tivoli Directory Server (including the Client and the Server) requires about 160 MB of disk space.

IBM Tivoli Directory Server includes the DB2 Universal Database™ for AIX Version 9.1 Restricted Enterprise Server Edition. No previous versions of DB2® are supported. If you already have DB2 installed, you need approximately 45 MB of disk space to create the empty database and start the server. DB2 requires between 300 MB and 500 MB of disk space. Disk space required for data storage is dependent upon the number and size of database entries.

Your machine must be running on 64-bit hardware.

Your machine must be running a 64-bit kernel.

Paging space requirements

AIX Version 6.1 creates a 512 MB paging space (in the **/dev/hd6** directory) for all new and complete overwrite installations.

Disk requirements

AIX Version 6.1 requires a minimum of 2.2 GB of physical disk space for the same set of installed filesets due to increased library sizes and additional function.

Note: The following measurements provide information about disk usage when you install AIX Version 6.1 as compared to previous versions.

Base AIX Installation (Graphical System with CDE-Default)

Location	AIX 5L™ for POWER Version 5.1 Allocated (Used)	AIX 5L Version 5.2 Allocated (Used)	AIX 5L Version 5.3 Allocated (Used)	AIX Version 6.1 Allocated (Used)
/	8 MB (5.6 MB)	16 MB (10 MB)	20 MB (12 MB)	144 MB (97 MB)
/usr	385 MB (370 MB)	1040 MB (1034 MB)	1292 MB (1246 MB)	1520 MB (1463 MB)
/var	4 MB (1.4 MB)	16 MB (7 MB)	16 MB (12 MB)	16 MB (12 MB)
/tmp	20 MB (0.9 MB) (See note.)	32 MB (1.1 MB)	36 MB (1 MB)	64 MB (1 MB)
/admin	—	—	—	128 MB (1 MB)
/opt	4 MB (0.2 MB)	48 MB (26 MB)	96 MB (80 MB)	96 MB (80 MB)

Note: If the **/tmp** directory has less than 56 MB, it is increased to 56 MB during a migration installation so that the AIX Version 6.1 boot image is successfully created at the end of the migration.

During a migration installation, if **/opt** exists only as a directory and has less than 3 MB of data, then a new **/dev/hd10opt** logical volume and **/opt** file system are created, and the data that existed in the **/opt** directory is moved to the new **/opt** file system.

If there is more than 3 MB of data in the **/opt** directory, then the new logical volume and file system are not created.

If any existing file system has a mount point in the **/opt** directory, or a mount point of **/opt** itself, the new logical volume and file system are not created.

Chapter 3. Installation, migration, upgrade, and configuration information

Installation

This section contains information about installing AIX 6.1 that supplements the information contained in *AIX Version 6.1 Installation and migration*. The installation guide is available online in the AIX Information Center and in printed hardcopy (SC23-6616-00).

To order these installation guides, contact your point of sale, or in the U.S., call IBM Customer Publication Support at 1-800-879-2755. Give the order number of the book you want to order.

To obtain AIX Version 6.1 installation hints and tips, visit the Subscription Service at the following Web site:

`http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd`

Installing AIX Version 6.1

The following methods can be used to install AIX Version 6.1:

- Complete overwrite installation
- Preservation installation
- Migration installation

Note: After you install or migrate a system to AIX Version 6.1, you can install a lower level of AIX by restoring a system backup or by performing a new and complete overwrite with base media. Preservation installations from AIX Version 6.1 to a lower level of AIX are not supported.

Note: The minimum size of the boot logical volume is 20 MB. If your current boot logical volume is less, the install process tries to increase it. However, partitions in a boot logical volume must be contiguous, and within the first 4 GB on the disk. If your system does not have free space that meets these requirements, a message will indicate there is not enough space to expand **hd5** (the boot logical volume).

To install AIX Version 6.1, boot your system from the product media, and follow the instructions in the *Installation and migration* in the AIX Information Center.

Disk format requirement

You cannot install AIX on an improperly formatted SCSI disk. AIX requires the disk to be formatted to a sector size supported by the attached SCSI controller. All AIX SCSI controllers support 512 byte sector SCSI disks. The 522 byte sector SCSI disks are only supported when they are attached to SCSI RAID controllers. If the disk has been formatted for SCSI RAID, but is not attached to a SCSI RAID controller, the disk might not configure. If the disk does configure, it might be unreadable in the AIX environment. In some instances, the certify function and the format function in AIX diagnostics can be used to reformat the disk for the attached SCSI controller.

Creating a bootable CD

It is recommended that you create a CD that can be used to boot and perform maintenance on your system that matches your current level of AIX.

To create a bootable CD, run the following commands (where *cdx* is an attached CD writer). The **bosinst.data** file must be set for a prompted install (`PROMPT = yes`).

```
cd /var/adm/ras
ls ./bosinst.data ./image.data | backup -ivqf/tmp/fakemksysb
mkcd -m /tmp/fakemksysb -d /dev/cdx
```

7

OR

```
mkcd -m /tmp/fakemksysb -S
```

will create a CD image that can be transferred to a system with a CD writer.

Note: The final **mkcd** command in the previous example makes an image that can be transferred to another system (AIX or non-AIX) for burning.

Base Operating System installation options

The information in this section supplements the ″Installation Options″ chapter of the *Installation and migration* in the AIX Information Center.

In the Base Operating System installation menus, if there are more than 50 disks on the system, the disks are ordinarily grouped by adapter. However, for some types of disks, the grouping is slightly different:

SCSI disks

Disks may be grouped by adapter or SCSI bus

IBM TotalStorage® DS4000™

Disks are grouped by disk array controller (DAC)

In each case, the user can select the adapter, SCSI bus, or DAC by name and see the associated disks. The physical location of the adapter, SCSI bus, or DAC is also displayed.

Installing AIX using the media device to install a partition with an HMC

The instructions for installing AIX using the media device to install a partition with an HMC have been changed to:

1. Activate the partition, as follows:

    a. Insert the *AIX Volume 1* CD or DVD into the media device of the managed system.

    b. Right-click on the partition to open the menu.

    c. Select **Activate**. The Activate Partition menu opens with a selection of partition profiles. Be sure the correct profile is highlighted.

    d. Select **Open a terminal window or console session** at the bottom of the menu to open a virtual terminal (vterm) window.

    e. Select **Advanced** to open the Advanced options menu.

    f. For the Boot mode, select **SMS**.

    g. Select **OK** to close the Advanced options menu.

    h. Select **OK**. A vterm window opens for the partition.

2. In the SMS menu on the vterm, do the following:

    a. Press Enter to select **5. Select Boot Options**.

```
PowerPC Firmware
Version SF220_001
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: 5
```

b. Press Enter to select **2. Select Boot Devices**.

c. Press Enter to select **1. Select 1st Boot Device**.

d. Press Enter to select **3. CD/DVD**.

e. Select the media type that corresponds to the media device and press Enter.

f. Select the device number that corresponds to the media device and press Enter. The media device is now the first device in the Current Boot Sequence list.

g. Press the ESC key until you return to the Configure Boot Device Order menu.

h. Press the x key to exit the SMS menu. Confirm that you want to exit SMS.

3. Boot from the *AIX Volume 1* CD or DVD, as follows:

a. Select console and press Enter.

b. Select language for BOS Installation menus, 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.

```
                    Welcome to Base Operating System
                    Installation and Maintenance

Type the number of your choice and press Enter.  Choice is indicated by >>>.

    1 Start Install Now with Default Settings

    2 Change/Show Installation Settings and Install

    3 Start Maintenance Mode for System Recovery

    88  Help ?
    99  Previous Menu
>>> Choice [1]: 2
```

4. Verify or Change BOS Installation Settings, as follows:

a. Type 1 in the **Choice** field to select the **System Settings** option.

b. Type 1 for New and Complete Overwrite in the **Choice** field and press Enter.

   Note: The installation methods available depend on whether your disk has a previous version of AIX installed.

c. When the Change Disk(s) screen displays, you can change the destination disk for the installation. If the default shown is correct, type 0 in the **Choice** field and press Enter. To change the destination disk, do the following:

   1) 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 disks. If you must deselect a disk, type its number a second time and press Enter.

   2) When 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 needed, change the primary language environment. Use the following steps to change the primary language used by this installation to select the language and cultural convention you want to use.

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

   1) Type 2 in the **Choice** field on the Installation and Settings screen to select the **Primary Language Environment Settings** option.

2) 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.

- To choose a predefined Primary Language Environment, type that number in the **Choice** field and press Enter.
- To configure your own primary language environment, do the following:

    a) Select **MORE CHOICES**.

    b) Select **Create Your Own Combination**.

    c) When the Set Primary Cultural Convention screen displays, type the number in the **Choice** field that corresponds to the cultural convention of your choice and press Enter.

    d) When the Set Primary Language screen displays, type the number in the **Choice** field that corresponds to your choice for the primary language and press Enter.

    e) When the Set Keyboard screen displays, type the number in the **Choice** field that corresponds to the keyboard attached to the system and press Enter.

  e. After you have made all of 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 installation is complete.

5. Complete the BOS Installation, as follows:

  a. Type `vt100` as the terminal type.

```
                           Set Terminal Type
 The terminal is not properly initialized.  Please enter a terminal type
 and press Enter.  Some terminal types are not supported in
 non-English languages.

     ibm3101          tvi912           vt330
     ibm3151          tvi920           vt340
     ibm3161          tvi925           wyse30
     ibm3162          tvi950           wyse50
     ibm3163          vs100            wyse60
     ibm3164          vt100            wyse100
     ibmpc            vt320            wyse350
     lft              sun


                       +----------------------Messages----------------------
                       | If the next screen is unreadable, press Break (Ctrl-c)
     88  Help ?        | to return to this screen.
     99  Exit          |
                       |
 >>> Choice []: vt100
```

  b. In the License Agreement menu, select **Accept License Agreements**.

  c. Select **yes** to ACCEPT 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**.

```
                           Installation Assistant

 Move cursor to desired item and press Enter.

   Set Date and Time
   Set root Password
   Configure Network Communications
   Install Software Applications
   Using SMIT (information only)


   F1=Help              F2=Refresh          F3=Cancel           F8=Image
   F9=Shell             F10=Exit            Enter=Do
```

f.   Set the correct date, time, and time zone. Press the F3 (or Esc+3) key to return to the Installation Assistant main menu.

g.   Select **Set root Password**. Set a root password for the partition.

h.   Select **Configure Network Communications**.

i.   Select **TCP/IP Startup**.

j.   Select from the Available Network Interfaces and press Enter.

k.   Enter the appropriate network information in the Minimum Configuration and Startup menu and press Enter. Use the F3 (or Esc+3) key to return to the Installation Assistant main menu.

l.   Exit the Installation Assistant by pressing F10 (or Esc+0).

m.   The vterm window displays a login prompt.

Secure by Default installation

A CD or DVD installation of AIX 6.1 with the Secure by Default (SbD) option prompts for the Expansion Pack CDs after the base operating system is installed. This step is necessary to install SSH and SSL packages for secure remote system accessibility. If this step is skipped, the system will not be network accessible because SbD erases binaries that use clear text passwords (for example, **telnet**, and **ftp**-similar binaries). If the SbD installation option is selected through NIM, the system administrator should ensure that the NIM **lpp_source** has the openssh and openssl images in place.

AIX Toolbox Media and NIM lpp_sources

When a Network Install Manager `lpp_source` is used for base system installs, do not copy the contents of the *AIX Toolbox for Linux*® *Applications* CD into the `lpp_source`. This results in multiple copies of **cdrecord** and **mkisofs** software installing during base installation. Neither **cdrecord** or **mkisofs** installs if multiple copies are present.

Graphics software bundle requires additional CDs

Due to space constraints on the AIX base product media CDs, the graphics software bundle is now included on the *Volume 2* and *Volume 3* CDs. For installations using CD media, you are prompted for the *Volume 2* and *Volume 3* CDs if you install with the defaults for an overwrite or preservation installation (`Graphics Software = yes`).

If you create a Network Installation Management (NIM) `lpp_source` with CD media, you will not be prompted for the *Volume 2* CD to add the graphics software to the `lpp_source`. To add the graphics software after creating the `lpp_source`:

1.   Type the **smitty nim_update_add** command. The **Add Software to an lpp_source** menu is displayed.

2.   Select the **Graphics** bundle for **INSTALLP BUNDLE containing packages to add**. Change the answer for `Process multiple volumes?` to `yes`, if necessary

Note: When creating an `lpp_source` from a prior release of AIX, and copying the **Graphics.bnd** software to the `lpp_source`, restore the **Graphics.bnd** appropriate to the release you are creating the resources to, and make it into a NIM resource. You can get the bundle from the **bos** image in the `lpp_source`:

```
# cd /tmp # restore -xvqf <lpp_source_path>/bos ./usr/sys/inst.data/sys_bundles/Graphics.bnd
```

This command restores in **/tmp/usr/sys/inst.data/sys_bundles**. Copy it to the location of your choice, and create a new NIM bundle resource, `smitty nim_mkres`.

Network Installation Management

Network Installation Management (NIM) includes a readme file that is installed with the NIM Master **bos.sysmgt.nim.master** fileset. The path name of the file is **/usr/lpp/bos.sysmgt/nim/README**. The readme file contains additional information about the AIX Version 6.1 NIM product and includes the following topics:

- Restrictions on SPOT Creation for Releases Prior to 5.3 (New LPP_SOURCE Directory Structure)
- Web-based System Manager NIM May Have Problems Installing SW on Client Machines
- Restrictions on Customize Operation for RPM Packages
- Steps Necessary For Adding GNOME -or- KDE Desktop Support

When Live Partition Mobility (LPM) is used to migrate a machine (that is, move a machine from one physical server to another) and the machine is defined as a NIM client, the NIM administrator must update the cupid attribute for the NIM client to reflect the new hardware value after the LPM migration completes. To update the cupid attribute, do the following:

1. On the NIM client, acquire the new cupid ID by running the following command:

   ```
   uname -a
   ```

2. On the NIM master, run the following command:

   ```
   nim -o change -a cupid+<cupid> <client>
   ```

CSM Server

Before you install the CSM Server, you must read the *Software Planning and Installation Guide* for specific procedural steps to use when you are installing CSM. Installation of this product is not possible if you do not use the documented procedures in this book.

CSM Server requires four open-source rpm filesets that must be installed prior to installing the CSM Server software and its dependent packages, the CSM Distributed Command Execution Manager (DCEM) GUI and the CSM DCEM Web-based System Manager application. The required rpm filesets are:

- tcl
- tk
- expect
- conserver

As the root user, do the following to install the rpm filesets and the CSM Server:

1. Install the above rpm filesets using SMIT Install Software (type **smitty install_latest** at the AIX command line).
   a. Press F4, and select **/dev/cd0** (CD Drive) as the **INPUT device / directory for software**.
   b. Press F4, and select (by pressing F7 for each package) **tcl-8.3.3**, **tk-8.3.3**, **expect-5.32**, and **conserver-7.2.4** as the **SOFTWARE to install** values, or press F4 and select all the software packages you want.
   c. To accept the software license agreements, press the Tab key to change `no` to `yes` as the **ACCEPT new license agreements** value, and then press Enter.
   d. Press Enter again to confirm that you want to continue the installation process.
   e. Review the installation results, and press F3 to return to the installation panel, or press F10 to return to the AIX command line.

2. Install the CSM Server and its dependent software using SMIT Install Software (type **smitty install_latest** at the AIX command line).
   a. Press F4, and select (by pressing F7 for each package) **csm.server**, **csm.gui.dcem**, and **csm.gui.websm** as the **SOFTWARE to install** values, or press F4 and select all the software packages you want.

b. To accept the software license agreements, press the Tab key to change `no` to `yes` as the **ACCEPT new license agreements** value, and then press Enter.

c. Press Enter again to confirm that you want to continue the installation process.

d. Review the installation results, and press F3 to return to the installation panel, or press F10 to return to the AIX command line.

IBM Tivoli Directory Server

You can install and use IBM Tivoli Directory Server only in association with your licensed use of AIX operating system functions. You must purchase a full-use license through Passport Advantage® for any other use of the IBM Tivoli Directory Server such as authentication and AIX user registry. The Passport Advantage package includes a White Pages application. The Passport Advantage license entitles you to use and to receive support for the IBM Tivoli Directory Server Proxy server and the White Pages application.

Other installation information

Installation packaging formats

AIX Version 6.1 supports the following installation-packaging formats:

- installp, AIX system installation command and packaging format
- RPM, a Linux installation command and packaging format
- ISMP, InstallShield Multi-Platform packaging format

With the **geninstall** command, you can list and install packages from media that contains installation images packaged in any of the listed formats. The **geninstall** and **gencopy** commands recognize the non-installp installation formats and either call the appropriate installers or copy the images, respectively.

The AIX Version 6.1 product media contains installp packages and RPM packages that are installed during a BOS installation. The installp packages are located in the following path, where *mount_point* is the mount point:

`/mount_point/installp/ppc`

The RPM packages are located in the following path, where *mount_point* is the mount point:

`/mount_point/RPMS/ppc`

If you have media that contains ISMP packages for AIX 6.1, the ISMP packages are located in the following path, where *mount_point* is the mount point:

`/mount_point/ismp/ppc`

The **installp**, **bffcreate**, **geninstall**, **gencopy** and **nim** commands recognize this media structure.

For more information about software packaging, see the Software Product Packaging Concepts section in the *Installation and migration* in the AIX Information Center.

Troubleshooting problems with installation from mksysb backup

Check that you have sufficient free blocks in the file systems to write temporary files. Check that each file system has at least 500 blocks free when the **mksysb** backup image is made. The system needs work space in each file system when installing from a **mksysb** backup image.

Note: Depending on the type of data or files in the file system, you might need additional blocks free. For example, if the file system has a lot of small files, an extra 4 KB is automatically allocated to allow for metadata expansion.

Migration

Maximum size of boot image increased

For AIX Version 6.1, the maximum size of the boot image has changed from the previous value used for AIX 5.2 (and earlier releases) value of 11,984 KB (12 MB minus 16 KB) to 31,984 KB (32 MB minus 16 KB). The size of the boot logical volume has increased from 16 MB to 20 MB. If your current boot logical volume is 16 MB or less, the install process tries to increase it. However, partitions in a boot logical volume must be contiguous, and within the first 4 GB on the disk. If your system does not have free space that meets these requirements, a message will indicate there is not enough space to expand **hd5** (the boot logical volume).

System migrated to AIX 5.3 (or later) might experience double boot

When booting AIX Version 5.3 (or later) on a system that has previously been running an earlier release of AIX, you may notice that the system automatically reboots and restarts the boot process. This is how the firmware processes changed information in the boot image.

This reboot also occurs if the process is reversed. A system previously running AIX 5.3 (or later) that is booting a release of AIX prior to 5.3 goes through the same process. This ″double boot″ occurs only once; if the stored value does not change, then the second boot does not occur.

If you install AIX 5.3 (or later) and continue to use only that version, this double boot occurs once, and it occurs only if your system was running a pre-AIX 5.3 release before you boot AIX 5.3 (or later). Systems that are preinstalled with AIX 5.3 (or later) and use only that version do not experience the ″double boot.″

Replacements for the vmtune and schedtune commands

When you migrate a system from a previous version of AIX to AIX Version 5.2, AIX Version 5.3, or AIX Version 6.1, it is automatically set to run in compatibility mode (pre520tune mode). Compatibility scripts that replace the **vmtune** and **schedtune** commands are included with AIX 5.2, which means that the previous behavior of the tuning commands is preserved to a large extent after a migration.

However, when you migrate to AIX 5.3, the pre520tune compatibility mode applies only to settings that were configured with the **no** and **nfso** commands because the **vmtune** and **schedtune** commands are no longer included. The compatibility mode is meant to be a temporary help in the migration to the new tuning framework and should normally not be used with releases after AIX 5.2.

KDE desktop

If the CDE and KDE desktops are both installed on a system migrated from AIX 5.x to AIX 6.1, the KDE desktop might not start from the CDE login. To fix this problem, remove the following CDE startup information from the **/etc/inittab** file:

```
dt:2:wait:/etc/rc.dt
```

Note: You must have root user authority to remove this CDE startup information.

Do not delete the following KDE entry from the **/etc/inittab** file:

```
kdm:2:once:/opt/freeware/kde/bin/kdm
```

Performance monitoring API

The Performance Monitoring API is contained in the **bos.pmapi** fileset. A beta version of the same code was made available to selected customers, and also through alphaWorks®, under the name *pmtoolkit.*

When you are migrating from any level of AIX with any level of the beta fileset installed, you must uninstall the **pmtoolkit** fileset and reboot the machine before you install the **bos.pmapi** fileset. If you do not, the machine will fail to boot when you attempt to load the **pmtoolkit** fileset's kernel extension.

Verify that the **pmtoolkit** fileset is installed by typing the following at the command line:

```
lslpp -l pmtoolkit
```

- If you get the following output:

  ```
  lslpp: 0504-132  Fileset pmtoolkit not installed
  ```

  you can safely install the **bos.pmapi** fileset.

- If you get the following output:

  ```
  Fileset                     Level  State      Description
  ----------------------------------------------------------------------
  Path: /usr/lib/objrepos
    pmtoolkit                 1.3.1.6  COMMITTED  Performance Monitor Toolkit
                                                  1.3.1
  ```

  complete the following steps:

  1. Run the following command:

     ```
     installp -u pmtoolkit
     ```

  2. Reboot the machine. After the machine reboots, you can safely install the **bos.pmapi** fileset.

SNMPv3

After you migrate to AIX 6.1 from pre-AIX 5.2 systems, the non-encrypted version of SNMPv3 will run by default. If you have your own community, trap, or smux entries in your **/etc/snmpd.conf** file, those must be manually migrated to the **/etc/snmpdv3.conf** file. For instructions on how to migrate this information, see ″Network Management″ in *Networks and communication management* in the AIX Information Center.

Kerberos

All of the secure remote commands use the Kerberos Version 5 library and the GSSAPI library provided by IBM Network Authentication Service Version 1.4 that is located on the *AIX Version 6.1 Expansion Pack* CD. However, you must install the **krb5.client.rte** fileset.

If you are migrating to AIX 6.1 and have Kerberos Version 5 installed, the installation scripts will prompt you to install the **krb5.client.rte** fileset. The secure remote commands support Kerberos clients and servers from both Native Kerberos 5 and DCE.

For more information, see ″Understanding the Secure Rcmds″ in *Managing Communications and Networks* in the AIX Information Center.

Multipath I/O (MPIO)

In AIX Version 6.1, the DS4K products are configured as Multipath I/O (MPIO) devices by default.

A DS4K product using the FCPARRAY driver may be migrated to the MPIO driver by using the following instructions, or all DS4K devices may be migrated by uninstalling the **devices.fcp.disk.array.rte** package and then running the **cfgmgr** command or rebooting.

The DS3K products are always configured as MPIO devices. There is no FCPARRAY support for these devices. The MPIO support for these devices removes the limitation of connecting only one adapter to each DS3/4K controller port.

Instructions to convert DS4000 disks from FCPARRAY to MPIO

The MPIO driver has been enhanced to support most DS4000 models. The MPIO driver allows more than two paths to be configured to the device, and this simplifies zoning and improves performance. For the DS4000 to operate correctly in an MPIO configuration, the following steps must be performed.

The following AIX releases and minimum service packs can be used to convert DS4000 disks from FCPARRAY to MPIO:

- AIX 5.2 with the 5200-10 Technology Level and the 5200-10-04 Service Pack
- AIX 5.3 with the 5300-06 Technology Level and the 5300-06-05 Service Pack
- AIX 5.3 with the 5300-07 Technology Level and the 5300-07-02 Service Pack
- AIX 6.1 with the 6100-00 Technology Level and the 6100-00-02 Service Pack

The following DS4000 models are supported by AIX MPIO:

- 1722-600 = DS4300 = FAStT 600
- 1742-900 = DS4500 = FAStT 900
- 1814 = DS4700/DS4200
- 1815 = DS4800

To convert DS4000 disks from FCPARRAY to MPIO, do the following:

1. Change the NVSRAM settings on DS4000 storage used in the SAN (or direct attach) by doing the following:

   Note: If this step was previously performed, go to step 2. However, if DS4000 firmware was updated, this step must be performed again.

   a. From the main Enterprise Management screen, highlight the subsystem you want to change.

   b. From the Tools menu, select `Execute Script` to open a Script Editor window.

   c. Enter the following:

   ```
   set controller [a] HostNVSRAMBYTE [0x06,0x27] = 0;
   set controller [b] HostNVSRAMBYTE [0x06,0x27] = 0;
   ```

   d. From the Tools menu, use the Script Editor to select `Verify & Execute`.

   e. Wait for the script to complete.

   Attention: Do not cancel the script operation.

   When the script completes, exit the Storage Manager.

2. Install the MPIO_DS3_4K APAR/iFIX that is appropriate for the AIX release on the server, and then reboot the AIX server.

3. Determine the DS4000 model or models that you are using on your AIX host by running the following commands, where *X* is the hdisk number for the DS4000 Array Disk type:

   ```
   lsdev —Cc disk | grep DS4K
   lscfg —vl hdiskX
   ```

   For example:

   ```
   # lsdev -Cc disk
   hdisk2 Available 0C-08-02 DS4K Disk Array Device

   # lscfg -vl hdisk2
   hdisk2 U787A.001.DPM0WY4-P1-C5-T1-W200800A0B81326B7L3000000000000 1742-900 (900) Disk Array Device

       Manufacturer................IBM
       Machine Type and Model......1742-900
       ROS Level and ID............30393134
       Serial Number...............
       Device Specific.(Z0)........0000053245004032
       Device Specific.(Z1)........
   ```

4. Use the following table and the Machine Type and Model output from step 3 on page 16 to determine your DS4000 Array Disk type.

Table 1. DS4000 Array Disk Cross Reference

Machine Type-Model	Array Disk	Storage Server
1722-600	DS4300	FAStT 600
1742-900	DS4500	FAStT 900
1814	DS4700/DS4200	
1815	DS4800	

5. Check the AIX systems driver support and state by running the following command:

```
# 'manage_disk_drivers'
```

The output from this command displays the DS4000 devices that are supported by MPIO and RDAC, and indicates if they are currently configured for MPIO or RDAC enablement.

For example:

```
# manage_disk_drivers
 1: DS4300: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
 2: DS4500: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
 3: DS4700/DS4200: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
 4: DS4800: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
```

Note: If the AIX system has more than one type of DS4XXX models attached, run the **manage_disk_drivers** command for each model type.

In the example in step 3 on page 16, hdisk2 is a DS4500. In the example in step 5, DS4500 is currently enabled for RDAC/fcparray.

To change the driver that manages the DS4000, run the following commands in order, where *X* in the first command is the number of the array disk stanza from the output of the **manage_disk_drivers** command. For example: for DS4700, enter `# manage_disk_drivers – c 3`; for DS4800, enter `# manage_disk_drivers – c 4`, etc.

```
# manage_disk_drivers – c X
```

To verify the change, answer `Y` when prompted.

```
# bosboot –a
# shutdown –Fr
```

6. After the server reboots, all of the hdisk devices that were converted will be configured under the MPIO driver. All of the hdisks that are connected to DS4000 should be displayed as `MPIO Other DS4K Array Device` as indicated by the **lsdev –Cc disk** output.

7. To verify that hdisks are mapped to the appropriate LUNs on DS4000, run the **mpio_get_config –A** command. This command is similar to the **fget_config** command for the RDAC driver. The **mpio_get_config** command is for informational purposes only; you cannot change the LUN ownership using this command.

Instructions to convert DS4000 disk driver from MPIO to FCPARRAY

The following AIX releases and minimum service packs can be used to convert the DS4000 driver from MPIO to FCPARRAY:

- AIX 5.2 with the 5200-10 Technology Level and the 5200-10-04 Service Pack
- AIX 5.3 with the 5300-06 Technology Level and the 5300-06-05 Service Pack
- AIX 5.3 with the 5300-07 Technology Level and the 5300-07-02 Service Pack
- AIX 6.1 with the 6100-00 Technology Level and the 6100-00-02 Service Pack

To convert the DS4000 driver from MPIO to FCPARRAY, do the following:

1. Install the MPIO_DS3_4K APAR/iFIX that is appropriate for the AIX release on the server.

2. Change the NVSRAM settings on DS4000 storage used in the SAN (or direct attach) by doing the following:

   Note: If this step was previously performed, go to step 3. However, if DS4000 firmware was updated, this step must be performed again.

   a. From the main Enterprise Management screen, highlight the subsystem you want to change.

   b. From the Tools menu, select `Execute Script` to open a Script Editor window.

   c. Enter the following:

   ```
   set controller [a] HostNVSRAMBYTE [0x06,0x27] = 0;
   set controller [b] HostNVSRAMBYTE [0x06,0x27] = 0;
   ```

   d. From the Tools menu, use the Script Editor to select `Verify & Execute`.

   e. Wait for the script to complete.

      Attention: Do not cancel the script operation.

      When the script completes, exit the Storage Manager.

3. To migrate from MPIO to RDAC, there must be no more than two connections between the server and the storage (one per controller). Verify that this requirement is met by verifying that there is a separate zone for each HBA and controller pair. Refer to the RDAC documentation for valid configuration details.

4. After the installation completes successfully, reboot the system.

5. Determine the DS4000 model or models that you are using on your AIX host by running the following command where *X* is the hdisk number for the DS4000 Array Disk type:

   ```
   lsdev –Cc disk | grep DS4K
   lscfg –vl hdiskX
   ```

   For example:

   ```
   # lsdev -Cc disk
   hdisk2 Available 0C-08-02 DS4K Disk Array Device

   # lscfg -vl hdisk2
   hdisk2 U787A.001.DPM0WY4-P1-C5-T1-W200800A0B81326B7L3000000000000 1742-900 (900) Disk Array Device

       Manufacturer................IBM
       Machine Type and Model......1742-900
       ROS Level and ID............30393134
       Serial Number...............
       Device Specific.(Z0)........0000053245004032
       Device Specific.(Z1)........
   ```

6. Use the following table and the Machine Type and Model output from step 5 to determine your DS4000 Array Disk type.

Table 2. DS4000 Array Disk Cross Reference

Machine Type-Model	Array Disk	Storage Server
1722-600	DS4300	FAStT 600
1742-900	DS4500	FAStT 900
1814	DS4700/DS4200	
1815	DS4800	

7. Check the AIX systems driver support and state by running the following command:

   ```
   # 'manage_disk_drivers'
   ```

   The output from this command displays the DS4000 devices that are supported by MPIO and RDAC, and indicates if they are currently configured for MPIO or RDAC enablement.

   For example:

```
# manage_disk_drivers
 1: DS4300: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
 2: DS4500: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
 3: DS4700/DS4200: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
 4: DS4800: currently RDAC/fcparray; supported: RDAC/fcparray, MPIO
```

Note: If the AIX system has more than one type of DS4XXX models attached, run the **manage_disk_drivers** command for each model type.

In the example in step 5 on page 18, hdisk2 is a DS4500. In the example in step 7 on page 18, DS4500 is currently enabled for RDAC/fcparray.

To change the driver that manages the DS4000, run the following commands in order, where *X* in the first command is the number of the array disk stanza from the output of the **manage_disk_drivers** command. For example: for DS4700, you would enter `# manage_disk_drivers – c 3`; for DS4800, you would enter `# manage_disk_drivers – c 4`, etc.

`# manage_disk_drivers – c X`

To verify the change, answer `Y` when prompted

```
# bosboot –a
# shutdown –Fr
```

8. After the server reboots, all of the hdisk devices that were converted will be configured under the RDAC driver.

IBM Blade Center Issues

To ensure that the storage devices are properly configured on the IBM Blade Center, change the **init_link** setting on the Fibre Channel adapter from `arbitrated loop` to `point to point`.

Enter the following commands to change the **init_link** setting on the Fibre Channel adapter:

```
chdev -l fcsX -ainit_link=pt2pt –P
bosboot -aD
cfgmgr
```

Chapter 4. Limitations and restrictions

This section lists restrictions and limitations applying to AIX Version 6.1.

Workload Partitions not supported on thin servers

Workload Partitions (WPARs) are not supported on thin servers (diskless and dataless systems that are not capable of booting and running without the assistance of servers on a network).

WPAR parameters must be in English ASCII text

WPAR input parameters must be in English ASCII text. This includes the following WPAR variables:
- WPAR name
- WPAR password
- WPAR paths
- WPAR application
- WPAR hostname

Installing applications in a WPAR environment

The WPAR documentation describes how to install applications in a WPAR environment using various applications such as Apache, DB2 and WAS. These examples are not intended to imply that they are the supported versions or configurations of these applications.

System software cannot be directly managed in a non-shared /usr Workload Partition

If a WPAR is configured to have writeable, non-shared **/usr** and **/opt** filesystems, the AIX system software within that WPAR cannot be directly managed from within the WPAR. Operations that are prevented on system software include **apply**, **commit**, **deinstall**, and **reject**. If it is necessary to modify system software within a non-shared WPAR, use the **/usr/sbin/swvpdmgr -w** *<fileset_names>* command to allow those filesets to be directly managed within the Workload Partition.

SNMPv3

In AIX Version 6.1, due to the security concern that the ″public″ community name configured in the **/etc/snmpdv3.conf** file is able to query a lot of Management Information Base (MIB) information on the system, the default behavior has been changed to restrict the ″public″ community name to view this information.

AIO has been removed from the ODM

For each Asynchronous I/O (AIO) function there is a Legacy and a POSIX definition. In AIX Version 6.1, both POSIX and Legacy extensions are loaded at boot time. Do not run the `mkdev -l [aio0 | posix_aio0]` command to load the extension because it will fail on AIX Version 6.1. AIO attributes have been removed from the Object Data Manager (ODM) and can no longer be queried with the **lsattr** command or changed with the **chdev** command. All of the tunables have been removed from the ODM and are managed by the **ioo** command.

Using a USB optical device with VIOS

When you switch USB optical devices away from a Virtual I/O Server platform, then switch them back, the client partitions cannot use the optical devices until you delete the virtual optical devices, as well as the real optical devices. Run the **cfgmgr** command to make the optical devices available.

Performing an internal or external snapshot of a JFS2 filesystem

The **snapshot** command fails in the following instances:

- The **snapshot** command fails with a `Not owner` error if you are trying to create an internal snapshot and the filesystem already has an external snapshot and vice versa. In this instance, the **fscntl** system call returns -1 and the **errno** parameter has the EPERM value.

- The **snapshot** command fails with a `Not owner` error if trying to create an internal or an external snapshot and the filesystem is HSM enabled. In this instance, the **fscntl** system call returns -1 and the **errno** parameter has a EPERM value.

- The **chfs** command fails with a `A system call received a parameter that is not valid` error if trying to enable HSM for a filesystem that has an internal or an external snapshot. In this instance, the **finfo** system call returns -1 and the **errno** parameter has a EINVAL value.

- The **snapshot** command fails with a `No space left on device` error when trying to create an internal snapshot and the snapshot limit is exceeded. In this instance, the **fscntl** system call returns -1 and the **errno** parameter has a ENOSPC value.

Web-based System Manager

Remote client management

An HTTP Server must be installed and configured using one of the following configuration methods:
- Installing the IBM HTTP Server 2.0.47.1 on an AIX machine
- Installing any other HTTP Server on an AIX machine

This is necessary to support remote client management using Web-based System Manager. Proper configuration of an HTTP Server allows an AIX machine to serve the remote client download pages, Java™ Web Start, applet pages, and online extended helps.

When installing the IBM HTTP Server 2.0.47.1 on an AIX machine:
- Use the **wsm_remote** Software Bundle (**smitty install_bundle**) to install the IBM HTTP Server.
- Upon successful installation of the software, the bundle's post-installation processing script consolidates the steps needed to configure and initiate remote access and file serving capabilities for Web-based System Manager.
- This software installation bundle prompts you to insert the AIX Expansion Pack media to install the IBM HTTP Server.
- If you obtained the IBM HTTP Server, Version 2.0.47.1 from the following IBM HTTP Server product Web site:

  `http://www.ibm.com/software/webservers/httpservers/`

  then the **wsm_remote** Software Bundle allows you to install IHS from the hard disk by specifying the directory path name that contains your copy of the software installation images. To install IHS on AIX using the **wsm_remote** Software Bundle, manually complete the setup as follows:
  1. The installation directory path name must be in the format `./ismp/ppc/package_name`. For example, downloaded installation images can be copied to the **/usr/sys/inst.images/ismp/ppc/IHS2** directory. In this example, the installation source name is **/usr/sys/inst.images**, and the package name is **IHS2**.

2. The response file named **silent.res** must be linked to the name **IHS2.response** for AIX to detect automatic responses during a silent installation, such as specifying the **-P ihs.installLocation=/usr/ HTTPServer** preferred AIX installation location and a language other than the default en (English) language.

When installing any other HTTP Server on an AIX machine, complete the following:

1. Install the Web server.
2. Upon successful installation of the software, configure the Web server using the **smitty web_based_system_manager** SMIT fast path command.
3. Provide the required information in the panels. A configuration script runs and consolidates the steps needed to configure and initiate remote access and file-serving capabilities for Web-based System Manager.

After updating the **sysmgt.websm** filesets, **wsmserver** in the **/etc/services** file and in the **/etc/inittab** file is updated. If modifications were previously made to these entries, the files might need to be re-edited after updating.

Host Ethernet Adapter limitation

AIX Dynamic Logical Partitioning (DLPAR) of Integrated Virtual Ethernet (IVE), also known as Host Ethernet Adapter (HEA), is not supported in AIX 5.3 with the 5300-06 Technology Level and AIX 5.2 with the 5200-10 Technology Level. Support for this feature is enabled in AIX 5.3 with the 5300-07 Technology Level and AIX 6.1 with the 6100-00 Technology Level and later releases.

Chapter 5. AIX Information Center

The AIX Information Center is provided on the Web at http://publib14.boulder.ibm.com/infocenter/systems/ aix. The information center with translations will be available on DVD in orders processed after 9 December 2007. The AIX Information Center can be installed from or be viewed directly from the DVD on any AIX or Microsoft® Windows® systems that are capable of reading a DVD.

If you require a translated version of the documentation and cannot access the Web site or use a DVD, then you might be able to download a copy of the DVD contents from the ″Entitled Software Service″ site under the terms of your AIX Software Maintenance Agreement if electronic download is offered in your country.

Information about using the electronic software delivery site is provided by going to the Web site at https://www-05.ibm.com/servers/eserver/ess/ProtectedServlet.wss and clicking **Help**. The electronic install image is provided in a **tar.gz** format. After downloading the compressed tar image, decompress, unpack, and run **install_aix** to start the installation wizard.

The AIX Information Center DVD media is shipped with all orders for AIX Version 6.1 media manufactured after 9 December 2007, including orders specifying delivery of CD-ROMs. If you order AIX Version 6.1 before 9 December 2007 and require the DVD, you must reorder the AIX Version 6.1 installation media under the terms of an active AIX Software Maintenance Agreement. After IBM provides an installable version of the AIX Information Center on CD-ROM media, if you require the AIX Information Center on CD-ROM, you can obtain a free set of the CD-ROMs by reordering the AIX Version 6.1 installation media under the terms of an active AIX Software Maintenance Agreement and specifying CD-ROM (feature code 3410) as the delivery media.

Note: It is recommended that you restart your system after the AIX Information Center is installed. On AIX systems, exit the installation wizard after the installation of the documentation for each language. On AIX systems, to set the default browser, type the following command:

```
chwebconfig -b <browser location>
```

Appendix A. What's new

New and enhanced functionality in AIX Version 6.1

AIX Version 6.1 delivers support for the System p™ POWER6 based offerings.

Virtualization

AIX Version 6.1 includes significant new capabilities for virtualization including:

- **Workload Partitions**

  Workload partitions (WPARs) provide a virtualized operating system environment within a single instance of the AIX operating system. WPARs secure and isolate the environment for the processes and signals that are used by enterprise applications. WPARs complement other AIX virtualization technologies. WPARs can improve efficiency by reducing the number of system images to maintain, providing easy setup and management, and high system utilization through server consolidation. There are two type of WPARs supported:

  - System WPARs are autonomous virtual system environments with their own private file systems, users and groups, resource controls, login, network space, and administrative domain. A system WPAR shares the kernel with the global AIX environment in which it runs, and can share or have its own copies of the system **/usr** and **/opt** file systems.

  - Application WPARs provide an environment for isolation of applications and their resources. The WPAR application inherits all resources and execution environments from the global environment.

- **Application Mobility**

  Application Mobility is a new capability that allows a client to relocate a running WPAR from one system to another, without requiring the workload running in the WPAR to be restarted. Application Mobility is intended for use within a data center and requires the use of the new Licensed Program Product, the IBM AIX Workload Partitions Managers (WPAR Manager). Both System and Application WPARs can be relocated with the WPAR manager.

Enterprise Storage Management

AIX Version 6.1 includes new improvements to Enterprise Storage Management. These enhancements include:

- **NFS Support for Workload Partitions**

  When mounting NFS file systems from within a system, WPAR performs the same as a regular NFS mount (Versions 2, 3, and 4 supported). Statistics (nfsstat) and tunables (nfso) commands from within a WPAR are specific to that WPAR. NFS mounts from within a mobile WPAR are relocated with the WPAR.

- **JFS2 Integrated Snapshots**

  JFS2 has provided support for snapshots in external logical volumes since AIX Version 5.2. In AIX Version 6.1, snapshots are created in the same storage device as the file system. This new feature allows:

  - Ease of management by removing management of separate logical volumes for snapshots. The snapshot resides in the same host storage object as the primary file system. These snapshots are referred to as internal snapshots to contrast with the snapshots in separate logical volumes, which are now referred to as external snapshots.

  - The number of snapshot generations per file system has been increased to 64. This increase provides better support for real world environments where snapshots are taken at weekly, daily and hourly intervals compared to the external snapshot limit of 15.

  - The new integrated snapshot facility provides superior ease of use. Since the snapshot is in the primary file system, earlier versions of files can be accessed by non-privileged users without requiring a separate mount of the snapshot. This new facility also allows NFS client access to snapshot data for exported file systems.

27

Security

AIX Version 6.1 includes significant new enhancements to its security features. These enhancements include:

- **Role Based Access Control**

  Role Based Access Control (RBAC) is designed to improve security and manageability by allowing administrators to delegate system administrative duties to non-root users. RBAC in AIX has been enhanced to provide very fine granular authorizations that identify the privileged operation that they control. These authorizations can be used to create the required roles necessary and assign those roles to the users required to manage the system.

- **Trusted AIX**

  Trusted AIX extends the security capabilities of AIX by supplying integrated multi-level security. Trusted AIX is implemented as an installation option that provides the highest levels of label-based security to meet critical government and private industry security requirements.

- **Encrypting Filesystem**

  The IBM Journaled Filesystem Extended (JFS2) provides for greater data security with the addition of a new capability to encrypt the data in a file system. Clients can select from a number of different encryption algorithms. The encrypted data can be based up in encrypted format, reducing the risk of data being compromised if backup media is lost or stolen. The JFS2 encrypting file system can also prevent the compromise of data even to root-level users.

- **Trusted Execution**

  Trusted Execution provides an advanced mechanism for checking and maintaining system integrity. A signature (SHA256/RSA) database for important system files is created automatically as part of the regular AIX installation. The Trusted Execution tool can be used to check the integrity of the system against the database. An administrator can define policies such as monitoring the loads of files listed in the database and not allowing execution/loads if hashes do not match.

- **Secure by Default**

  The AIX Version 6.1 installation offers a new option, Secure by Default, that installs only the minimal number of services to provide the maximum amount of security. The Secure by Default option works particularly well when used in conjunction with the AIX Security Expert to only enable the system resources required for the system's intended purpose.

System Management

AIX Version 6.1 includes new improvements to the manageability of the AIX operating system. These enhancements include:

- NFSv4 support for the Network Installation Manager (NIM)
- Graphical Installation

  The AIX Graphical Installer provides a simplified, easy-to-use version of the AIX installer. Users are presented with a graphical user interface to start a system installation instead of the existing text-based installation menu. The Graphical installer is limited to users that boot DVD media on a system that does not have an existing operating system on its disks. If the installation code finds a root volume group on a disk, the traditional BOS menus are presented.

- New graphical systems console, the IBM Systems Director Console for AIX

  The Systems Director Console for AIX provides a responsive Web access to common systems management tools such as the Systems Management Interface Tool (SMIT) and offers integration into the IBM Systems Director.

dscrctl Command
Purpose

Allows the system administrator to read the current settings for the hardware streams mechanism and to set a system wide value for the Data Stream Control Register (DSCR). The Data Streams Control Register is privileged. It can be read or written only by the operating system.

For more information on the Data Stream Control facilities, refer to the POWER Instruction Set Architecture V2.05 publicly available from http://www.power.org.

Syntax

To query the characteristics of the hardware streams on the system:
```
dscrctl -q
```

To set the operating system default prefetch depth on the system temporarily (i.e, for the current session) or permanently (i.e after each reboot):
```
dscrctl [-n] [-b] -s <dscr_value>
```

To cancel a permanent setting of the operating system default prefetch depth at boot time:
```
dscrctl -c
```

Description

The **dscrctl -q** subcommand queries and displays the number of hardware streams, and the platform and operating system default prefetch depth. Any user can run this subcommand.

The **dscrctl -s** subcommand sets the operating system default prefetch depth. It requires root authority to run. This default can be changed either for the current session (-n), at boot time (-b) or both (-n -b).

The **dscrctl -c** option cancels the setting of the operating system default prefetch depth at boot time. This option removes the **dscrctl** command from the **/etc/inittab** file and thus takes effect after the next reboot.

Flags

-q   Query: Display the number of hardware streams supported by the platform and the values of the firmware and operating system default prefetch depth.

-c   Cancel: Cancels a permanent setting of the system default prefetch depth at boot time by removing the **dscrctl** command from the **/.etc/inittab** file.

-n   Now: Used in conjunction with the -s flag, changes the runtime value of the operating system default prefetch depth. The change is not persistent across boot.

-b   Boot: Used in conjunction with the -s flag, makes change persistent across boots by adding a **dscrctl** command to the **/etc/inittab** file.

-s *dscr_value*
     Set: Defines the value for the new operating system default prefetch depth. The value is treated as a decimal number unless it starts with `0x` in which case it is treated as hexadecimal.

Examples

1. Set the value of the operating system default prefetch depth to 13 for the current session:
    ```
    # dscrctl -n -s 13
    ```
2. Display the current settings for the hardware streams mechanism:
    ```
    # dscrctl -q
    Current DSCR settings:
     number_of_streams = 16
     platform_default_pd = 0x5 (DPFD_DEEP)
     os_default_pd = 0xd (DSCR_SSE | DPFD_DEEP)
    #
    ```

/etc/inittab

RAS features and customization

AIX Version 6.1 introduces new RAS (Reliability, Availability, and Serviceability) features and improves functionality. Features that can potentially cause measurable performance impact are installed and enabled at a level that is intended to optimize RAS versus performance trade-offs. The features can be separately enabled or disabled to match the memory consumption and performance needs of a given installation. This can be done from the Problem Determination menu in SMIT (fastpath: **smitty problem**). Key features that can be enabled, disabled, and otherwise customized from this menu include the following:

- **System Dump**

  Beginning with AIX Version 6.1 with the 6100-01 Technology Level, an iSCSI device can be configured as a dump device for firmware-assisted system dumps if the dump logical volume is on the iSCSI boot disk.

  A more reliable system dump, called a firmware-assisted or fw-assisted system dump, is introduced. It minimizes the role of the failing AIX instance in collecting serviceability data. Firmware-assisted system dump is only enabled on POWER6 partitions with at least 4 GB of memory. When enabled, the system dump reserves a scratch area of partition memory, the size of which depends on several factors, including maximum partition memory. In general, the scratch area is between 128 MB and 256 MB in size. Firmware-assisted system dump is only enabled if the adapter firmware associated with the dump device has the necessary support.

  Most devices are supported, but may require an adapter firmware update. Firmware-assisted system dump includes a non-default mode that supports a full memory dump. When this mode is enabled, the size of the dump device might need to be increased to reflect the larger size of the dump. The default firmware-assisted system dump mode is for a selective memory dump whose contents and size are similar to the traditional AIX system dump.

  Beginning with AIX Version 6.1, all types of system dumps are compressed. The ability to disable dump compression is removed.

- **Advanced First Failure Data Capture features**

  The Advanced First Failure Data Capture features include default-on memory traces and run-time error-checking capabilities. The default memory consumption associated with these features is similar to what is used in AIX 5.3. Additional run-time error checking and tracing are added to selected AIX subsystems.

- **Kernel Recovery**

  AIX Version 6.1 introduces a recovery framework that allows AIX to continue running after selected errors that would have caused a partition outage in AIX 5.3. When enabled, this framework introduces a new 4 KB stack per thread, as well as a new 64 KB stack per processor.

- **Component and Live Dump**

  AIX Version 6.1 introduces a live dump capability that allows a selective dump of kernel memory to occur without requiring a partition reboot or application outage. By default, the live dump capability reserves 64 MB or 1/64 of the partition's real memory, whichever is less. By default, live dumps are written to the **/var/adm/ras/livedump** directory. These and other attributes can be customized.

- **ProbeVue**

  AIX Version 6.1 introduces a programmable dynamic trace capability called ProbeVue. ProbeVue provides several tunables to customize its memory usage and performance characteristics. Consult the **/usr/lpp/bos.sysmgt/probevue.README.txt** readme file for the latest information on ProbeVue usage and restrictions.

- **Kernel Storage Protection Keys**

  AIX Version 6.1 introduces support for POWER6 Virtual Storage Protection Keys by the AIX kernel and kernel extensions. Storage keys protect against erroneous accesses and memory overlays by segmenting portions of the address space. The performance impact of storage keys depends on the

workload, based on factors such as how much time is spent in kernel mode and the frequency of addressability changes while in kernel mode. When enabled, kernel storage keys require an additional 4 KB stack per thread, as well as an additional 44 KB stack per processor.

JFS2 sync tunables

JFS2 sync tunables provide ways to limit the number of pages that are written to a file during sync operations. When there is heavy random I/O activity to a large file during a sync operation, all reads and writes from user programs to that file are blocked. When there are a large number of "dirty pages" in the file, the time required to complete the writes to disk can be lengthy.

Note: These tunables should only be used if application response is noticeably delayed when a sync occurs. The optimum setting for these tunables is dependent on memory size and I/O bandwidth. If tuning is required, start with a neutral setting of 256 for both tunables.

The following are definitions for JFS2 sync tunables:

j2_syncPageCount
Limits the number of modified pages that are scheduled to be written by a sync operation in one pass for a file. When this tunable is set, the file system will write the specified number of pages without blocking I/O to the rest of the file. The sync call will iterate on the write operation until all modified pages have been written.

j2_syncPageLimit
Overrides **j2_syncPageCount** when a threshold is reached to ensure that the sync completes.

JFS2 sync tunables are manipulated with the **ioo** command, and they can also be managed with smit or wsm.

Hints for sync tunable settings:

```
j2_syncPageCount
 Default: 0
 Range: 0-65536
 Type: Dynamic
 Unit: 4KB pages
```

When you are running an application that uses file system caching and does large numbers of random writes, you might need to adjust this setting to avoid lengthy application delays during sync operations. The recommended values are in the range of 256 to 1024. The default value of zero gives the normal sync behavior of writing all "dirty pages" in a single call. Small values for this tunable result in longer sync times and shorter delays in application response time. Larger values have the opposite effects.

```
j2_syncPageLimit
 Default: 16
 Range: 1-65536
 Type: Dynamic
 Unit: Numeric
```

Set this tunable when **j2_syncPageCount** is set, and increase it if the effect of the **j2_syncPageCount** change does not reduce application response times. The recommended values are in the range of 1 to 8000. The **j2_syncPageLimit** setting has no effect if the **j2_syncPageCount** setting is 0.

Additional information

The devices.artic960 fileset

The **devices.artic960** fileset provides support for the IBM ARTIC960Hx 4-Port Selectable PCI Adapter (FC 2947). This includes EEH support and 64-bit support for the FC 2947 adapter. If an additional fileset is installed to access the IBM ARTIC960 FC 2947 adapter, full EEH and 64-bit support depends on the ability of the additional fileset to support EEH and 64-bit.

Included with the **devices.artic960** fileset are the following filesets:

- **devices.artic960.rte**, IBM ARTIC960 Runtime Support
- **devices.artic960.ucode**, IBM ARTIC960 Adapter Software
- **devices.artic960.diag**, IBM ARTIC960 Adapter Diagnostics

When a PCI I/O error occurs on an IBM PCI ARTIC960 adapter, the adapter slot becomes frozen and the IBM ARTIC960 adapter can be reset. Following an EEH error, the adapter software needs to be downloaded to the adapter again.

To determine if an EEH error occurred on an IBM ARTIC960 adapter, inspection of the error log is necessary. A temporary EEH error on an IBM ARTIC960 adapter is logged as a temporary EEH error followed by I/O errors specific to the IBM ARTIC960 adapter. Recovery from a temporary EEH error is accomplished by removing and making the IBM ARTIC960 device driver using the **rmdev** and **mkdev** command. This process loads the necessary adapter software onto the adapter.

If the error log shows a permanent EEH error, it is necessary to use the hot plug manager to remove and make the adapter again.

The **devices.artic960** fileset does not support interprocess communication through mailboxes on AIX Version 6.1.

The devices.pci.14108c00 fileset

The **devices.pci.14108c00** fileset provides support for SDLC and bi-synchronous protocols on the IBM ARTIC960Hx 4-Port Selectable PCI Adapter (FC 2947). When combined with the installation of the **devices.artic960** fileset, Enhanced Error Handling (EEH) support is provided. Either 32-bit or 64-bit kernel mode is supported. 32-bit applications are supported.

Error log labels for Fibre Channel adapters have changed in AIX 6.1

The error log templates are in the **devices.common.IBM.fc.rte** fileset. The **devices.pci.df1000f7.com** driver fileset that references the error log templates has changed. The following changes were made in the error logs:

- Errors previously logged using the `FCS_ERR`n template label (where n is between 0 and 10, inclusive) are now logged using the `FCA_ERR`n template label (where n is between 0 and 15, inclusive).
- Errors previously logged using the `FSCSI_ERR`n template label (where n is between 0 and 10, inclusive) are now logged under the `FCP_ERR`n template label (where n is between 0 and 15, inclusive).

The new templates also provide 1024 bytes of detailed date where as the previous templates had only 228 bytes.

AIXLink/X.25 LPP

AIXLink/X.25 LPP Version 2.1 is supported on AIX Version 6.1.

Appendix B. Listing of filesets on the AIX media

AIX for POWER Version 6.1 CD set

The AIX for POWER Version 6.1 CD set consists of eight CDs with the following software groupings. During normal software installation with the CD device (such as **/dev/cd0**), you are prompted for the CD volume. Corresponding language filesets (messages and locales) are also installed by default, to match the environment of your system.

- **Volume 1:** Contains the minimal Base Operating System (BOS) software installed on every system, as well as all devices and both kernels, and the English message catalogs. To install a system with only ″Volume 1″ from the BOS menu, set Desktop to NONE, change the default for Graphics bundle to No, and change the default for System Management Client bundle to No.
- **Volume 2:** Contains software to install the Graphics bundle, and to set the Desktop to CDE. System management software, X11 software and Java software are on this CD and on Volume 3.
- **Volume 3:** Contains system management software, printer software, as well as additional CSM, RSCT, Fortran, and Java software.
- **Volume 4:** Contains pieces of Open_GL, PEX_PHIGS, LDAP, and DB2 software that comes with AIX.
- **Volume 5:** Contains software for installing AIX in other languages. Messages, help text, and locales for German, French, Italian and Japanese are included.
- **Volume 6:** Contains software for installing AIX in other languages. Messages, help text, and locales for Catalan, Czech, Spanish, Hungarian, Polish, Brazilian Portuguese, Russian, and Slovakian are included.
- **Volume 7:** Contains software for installing AIX in other languages. Messages, help text, and locales for Korean, Simplified Chinese, and Traditional Chinese are included.
- **Volume 8:** Contains software to support bidirectional and complex text languages, including Arabic, Hebrew, Thai, Vietnamese, Hindi, Tamil, Telugu, Gujarati, Marathi, Kannada, Malayalam, Welch, Maltese, Azerbaijani-Latin, Urdu (India), and Urdu (Pakistan). Chinese language support for Hong Kong and Singapore is also included.

Appendix C. CAPP/LSPP EAL4+ updates

This appendix serves as a supplement to *AIX Version 6.1 Security* and provides information relevant to configuring and using a system according to the requirements for the CAPP/LSPP EAL4+ Common Criteria evaluation of AIX Version 6.1 with the 6100-00-02 Service Pack. To make this appendix consistent with *AIX Version 6.1 Security*, the headings used are identical unless otherwise noted. The information here supersedes information in *AIX Version 6.1 Security*.

For more information about CAPP/EAL4+, see *AIX Version 6.1 Security* and AIX information.

Notes:

1. The following sections in *AIX Version 6.1 Security* are not applicable:
   - Running a CAPP/EAL4+ distributed system
   - Shared files in the distributed system
   - Setting up the distributed system (Master)
   - Setting up the distributed system (all systems)
2. The kernel security flags in Table 33 of *AIX Version 6.1 Security* omitted the kernel flag for ROOT. ROOT is DISABLED in operational mode, and ENABLED in configuration mode.

Administrators who have questions about configuration changes should refer to the *Security Target* (ST), Chapter 6, for information about the evaluated mechanisms and their settings.

In CAPP installation, the administrator is root. In LSPP installation, the administrator is a user with any authorization that gives privileges to that user.

When root sets a password, the system does not check it for password quality rules. Therefore, the administrator must use the password quality rules when setting passwords for other users.

Any statements in *AIX Security* that refer to AIX 5.3 are not applicable for this installation. Use PRPQ number P91209 and feature code 5869 to get AIX 6100–00–01 and a copy of the release notes. After AIX 6100–00–01 is installed in CAPP/EAL4+ or LSPP mode, you must upgrade to AIX 6100–00–02 (service pack 2).

Attention:

- Do not change the kernel security flags that are configured for the CAPP/LSPP system operational mode.
- Only single-level printing is supported in the evaluated configuration.
- Do not use accessauths = ALLOW_ALL on shell scripts in the **/etc/security/privcmds** file.

Installing a CAPP/EAL4+ system

From the Install Menu, select:

```
New & Complete Overwrite

Security Model
 Trusted AIX = no
    -  More Options
```

Under `More Options`, select `yes` for the `CAPP/EAL4+` option, and if you are using WPAR, select `no` for the `TCB` option. If you are using a customized **bosinst.data** file for a nonprompted installation, the `TCB` option can be set to `yes`.

Disable remote root login for a CAPP installation. To disable remote root login, run the following command after installation: `/usr/bin/chuser rlogin=false subgroups=SUADMIN root`. Add administrative users to the SUADMIN group so they can **su** to root.

After AIX 6100–00–01 is installed in CAPP/EAL4+ or LSPP mode, you must upgrade to AIX 6100–00–02 (service pack 2). Follow the steps in "Installing AIX 6100–00–02 (service pack 2)" to upgrade to AIX 6100–00–02.

Installing a LSPP/EAL4+ system

From the Install Menu, select:

```
New & Complete Overwrite

Security Model
 Trusted AIX = yes
    - More Options
```

Under `More Options`, select `yes` for the `LSPP/EAL4+` option.

After AIX 6100–00–01 is installed in CAPP/EAL4+ or LSPP mode, you must upgrade to AIX 6100–00–02 (service pack 2). Follow the steps in "Installing AIX 6100–00–02 (service pack 2)" to upgrade to AIX 6100–00–02.

Installing AIX 6100–00–02 (service pack 2)

Use Download Director to securely download the filesets needed to upgrade to AIX 6100–00–02.

1. Go to the Fix Central Web site at http://www-912.ibm.com/eserver/support/fixes/.
2. Select the following options:
    - In the **Product family** drop-down list, select **System p**
    - In the **Product** drop-down list, select **AIX**
    - In the **Version** drop-down list, select **6.1**
    - In the **Fix type** drop-down list, select **Fix packs**
    - Click **Continue**
    - In the **Select a Technology Level** drop-down list, select **All 6.1**
    - Click **Go**
3. In the **Fix packs** list, select **6100-00-02-0750**. For additional information about the service pack, click on the Package details and Installation tips tabs.
4. Click **Continue**.
5. In the Package download screen, select **Download using Download Director** and then click **Continue**.
6. The Download Director Java applet will start. Click **Download Now**. Grant access for downloading the packages to the system by responding to the popup dialog boxes in your browser.
7. Install the filesets in a directory on the system that is being upgraded. For example, **/usr/sys/sp2**.
8. Generate a **.toc** file by running the **inutoc** command. For example, `# inutoc /usr/sys/sp2`.
9. After the **.toc** file is generated, run the following command to invoke smitty to install the updates:

    `# smitty update_all`
10. Remove the **writesrv** daemon from /etc/inittab

    `# rmitab writesrv`
11. Remove the **snmp** daemons by commenting out he following lines from /etc/rc.tcpip:

    ```
    /usr/sbin/aixmibd
    /usr/sbin/hostmibd
    /usr/sbin/snmpmibd
    ```

Reboot the system to complete the upgrade, and then verify that the system has been upgraded by running the following command:

```
# oslevel -r or oslevel -s
```

If the system was successfully upgraded, `6100–00–02` is displayed.

Changing the audit filesystem

The /audit filesystem is a jfs filesystem. It must be changed to a jfs2 filesystem. In addition, CAPP systems require additional commands. To complete these changes, do the following:

1. For LSPP systems, go to step 3. For CAPP systems only, enter the following commands:

```
audit shutdown
lsvg -l rootvg
```

2. If the TYPE field contains question mark (?) symbols, enter the following command:

```
synclvodm -v rootvg
```

3. Remove the jfs filesystem and create a jfs2 filesystem by entering the following commands:

```
umount/audit
rmfs /audit
crfs -v jfs2 -m /audit -g rootvg -A yes -p rw -a size=100M
```

Updating the Trusted Signature Database (TSD)

Because the CAPP/LSPP configuration changes system mode bits, TSD integrity errors will occur. During system reboot, several options are presented. Select the **Ignore All** option.

Update the TSD by entering the following command:

```
trustchk -u ALL mode
```

Notes and tips for LSSP systems

- After the system is installed, as isso, set the automatic reboot option to false by entering the following command:

```
chdev -l sys0 -a autorestart=false
```

- If TSD continues to generate intlabel errors, clear the errors as isso with PV_ROOT privilege by entering the following commands:

```
cp /etc/security/tsd/tsd.dat /etc/security/tsd/tsd.dat.org

trustchk -q /usr/sbin/format /usr/sbin/fdformat /usr/sbin/mount /usr/sbin/unmount \
/usr/sbin/umount /usr/sbin/tsm /usr/sbin/getty /usr/sbin/login /usr/sbin/mkvg \
/usr/sbin/extendvg /usr/bin/w /usr/bin/uptime >/tmp/list.dat

grep -p SLTL /tmp/list.dat |sed 's/SLTL/SHTL/' >/tmp/new.dat

trustchk -w -a -f /tmp/new.dat

trustchk -y ALL
```

- If any error messages related to audit are displayed on the console, as isso, restart the audit system by entering the following commands:

```
# audit shutdown
# audit start
```

- After three failed login attempts, the isso/so login is blocked by the network; however, the administrator can continue to access these accounts on the local console.
- The output of commands executed by cron/at are not forwarded to the user's mail spool.

- World-writeable directories which have label ranges (for example: **/tmp**) are not partitioned. To prevent the possibility of information flowing between labels, the administrator must partition these directories immediately after the initial configuration.

Network interface

On Trusted AIX, the default network interface has a label range with minSL=impl_lo and maxSL=ts_all. For LSSP/EAL4+ systems, there is no label range, and the default rule is automatically changed to impl_lo when the LSPP/EAL4+ install option is selected. To change the default rule, as isso, use the **netrule** command. For example:

```
/usr/sbin/netrule i+u default +impl_lo +impl_lo +impl_lo
```

Updating WPAR

After creating the WPAR on a CAPP system, run the following command in the WPAR to make it EAL4+ compliant:

```
/usr/lib/security/CC_EVALify.sh
```

When clogin is executed for the first time on a LSPP system, the firstboot scripts run (including CC_EVALify.sh). Since these scripts cause clogin to run longer than usual, when clogin calls TSM to login, the WPAR is still in configuration mode, so the login is denied. Wait approximately 10 minutes for the WPAR to complete the configuration before attempting another clogin.

For newly created WPAR systems, the default user options must be set to meet the evaluation requirements: these include root in CAPP mode or isso/sa/so in LSPP mode. These users have either no password or "weak" passwords, and their passwords must be updated before allowing untrusted users access to either the global environment or the respective WPAR.

The evaluation password requirement is that the probability of correctly guessing a password must be at least one in 1,000,000, and the probability of correctly guessing a password during repeated attempts within one minute must be at least one in 100,000.

To comply with the requirement, change the following user parameters in **/etc/security/user**:

```
default:
 maxage        = 8
 maxexpired    = 1
 minother      = 2
 minlen        = 8
 maxrepeats    = 2
 loginretries  = 3
 histexpire    = 52
 histsize      = 20
```

Updating EFS

EFS was evaluated as a cryptographic file system. The evaluation does not cover the aspects of root guard mode versus full access to root.

After EFS is enabled, set the security attributes for the efsmgr and egskeymgr commands by running the following command:

```
setsecattr -c accessauths=ALLOW_ALL
innateprivs=PV_DEV_QUERY,PV_DEV_CONFIG,PV_AU_ADD,PV_DAC_R,PV_DAC_W,PV_DAC_X /usr/sbin/efsmgr

setsecattr -c accessauths=ALLOW_ALL
innateprivs=PV_DEV_QUERY,PV_DEV_CONFIG,PV_AU_ADD,PV_DAC_R,PV_DAC_W,PV_DAC_X /usr/sbin/efskeymgr

setkst -t cmd
```

Appendix D. 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Dept. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

39

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

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.

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.

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.

Trademarks

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

AIX

AIX 5L

alphaWorks

DB2

DB2 Universal Database

DS4000

eServer

IBM

ibm.com®

IntelliStation

Passport Advantage

POWER

POWER3

POWER4

POWER5

POWER6

PowerPC

pSeries

RETAIN

System p

Tivoli

TotalStorage

Java and all Java-based trademarks and logos are registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

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

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

IBM

Printed in U.S.A.