AIX 7.2 Technology Level 5 Service Pack 3

Common Criteria Administration Guidance

Version 1.3

Version History

Revision	Date	Changes
1.2	3/4/22	Submit for BSI review
1.3	4/4/22	Address the comments from BSI

Table of Contents

1 Overview

This document provides instructions to configure and operate AIX 7.2 Technology Level 5 (TL5) Service Pack 3 (SP3) in the Common Criteria evaluated configuration to meet the NIAP Protection Profile for General Purpose Operating Systems version 4.2.1 (a.k.a. OSPP) and Extended Package for Secure Shell v1.0. The evaluated components are known as the Target of Evaluation (TOE). AIX guidance documents used for the evaluation are bundled and located in the aix72_ref.tar file. Section 5 "References" provides the location and hash value of this file.

Most of the installation steps, security configuration steps, and system operation steps documented in this guide require an administrative role. For the exception cases where a non-administrative user is allowed to perform the operations, the role will be called out explicitly in the respective sections.

Commands referenced in this guide along with command parameters are described in detail in the AIX 7.2 Commands reference. In case of any discrepancies, this document supersedes other AIX configuration and guidance documents.

Hardware and Firmware Requirements (Operational Environment)

- IBM POWER System E950 with POWER9 SMT8 core processor
- System firmware FW950
- PowerVM Virtual I/O System (VIOS) version 3.1.1

Software Requirements (TOE)

- AIX 7.2 TL5 SP3 Operating System (a.k.a. AIX 7.2.5.3)
- OpenSSH Client Software
- OpenSSH Server Software
- openssl-fips-20.16.102.2103
- Ifixes:
    - CCEMGR_fix
    - CCECCSUMA1_fix
    - InstTU_fix
    - TD0325_fix
    - efs_fix
    - lscore_fix
    - mount_fix
    - openssh_fix14
    - audit_fix
    - kernel_fix3
    - java_feb2022_fix

Additional Requirement (Operational Environment)

The following must exist on another system to perform remote administrator and remote user access.

- Remote SSH v2 client (for remote access)
- Remote system (to host the SSH v2 client)

1.1 Objectives for the Operational Environment

The evaluated configuration defines the following operational environment objectives. The operational environment must follow these objectives in order for the TOE to function securely.

- **OE.PLATFORM**—The OS relies on being installed on trusted hardware.
- **OE.PROPER_USER**—The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
- **OE.PROPER_ADMIN**—The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

1.2 Major Security Features

The TOE supports the following major security features.

- Auditing
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

A number of AIX security features (e.g., Trusted Execution, AIXPert, Trusted AIX) are excluded from the evaluated configuration.

1.3 Roles

The evaluated configuration employs the following roles.

Administrator—All-powerful users with the ability to manage the security aspects of the TOE as well as manage other users.

User—Non-administrative users that can manage the security of the objects (e.g., files, directories) that they own, but cannot affect the general security of the TOE.

For AIX, an administrator is known as the root user (a.k.a. superuser). Root user capability is enabled by default in the TOE. All non-administrative users of AIX are known as users (a.k.a. ordinary user).

Because the TOE is installed as a PowerVM/VIOS client, the PowerVM/VIOS **padmin** role is required to install the TOE.

1.4 Document Layout

Section 2 describes how to obtain AIX 7.2 TL5 SP3 from the IBM website and how to install it on an existing PowerVM/VIOS v3.1.1 system. Section 3 and section 4 describe additional packages and steps required to place the TOE into its evaluated configuration. All steps in all sections must be followed in the provided order to obtain the initial evaluated configuration.

2 Install AIX from a Media Repository/Virtual Media Library

This is a step-by-step command line procedure for using a virtual media repository to install an AIX partition for the evaluated configuration.

Create a virtual DVD on VIOS

Once the installation image has been obtained from the IBM website, all PowerVM/VIOS steps must be performed as **padmin** user on the PowerVM/VIOS system using the Hardware Management Console (HMC).

Step 1: Obtain the AIX base ISO image.
Before ordering AIX install image online, you should request your IBM License Entitlement. The following are the step-by-step instructions on how to request IBM License Entitlement through IBM Passport Advantage Online (PAO) website.

a) Go to: https://www.ibm.com/software/passportadvantage/

b) Enter your IBMid and password and click continue.
Note: If you do not yet have an IBMid and password, click 'Create an IBMid' and fill in the required fields and submit.
You will be notified when your IBM ID an PW are activated and you can return to the PAO website to log and complete your access request.

c) Complete a “Self-nomination” form.

Think of the Self-nomination form as an application for access. It will be forwarded to your Site Primary (or Secondary) Contact who will accept or deny your request based in large part upon the information you provide. **Remember, your Primary (or Secondary) Contact, NOT IBM, determines who can access your PAO Site.**

- **Enter the Site number you wish to access**
  If you do not know your Site number, reach out to your Sales organization for a copy of a recent Proof-of-Entitlement (PoE), invoice, or sales order. All these documents should include your PAO Site number.
- **Provide a Business Justification** explaining why you need PAO Site access.
  For example:
  “I need to purchase software”
  “I need to renew S&S”
  “I need to download software”
  “I need to generate reports or view proof of entitlements”

Your business justification helps your Site Primary Contact assign you the right role(s) and grant you the application privileges you need.

Roles	Applications	Privileges
• All roles • Primary Contact (only one per Site) • Secondary Contact (up to 4) • User (unlimited)	• All applications • Software download and media access / Purchase and renewal • Reporting (Software and service online access privileges) • Entitlement inventory and deployments • Contact update • Account-related documents	• All privileges • None • View • Update • Software download only • Software download and media access only • Software download, media access, quotes, product catalogs and license renewal

d) Click SUBMIT.

Your request for access will be forwarded to your PAO Primary Contact (sometime referred to as your Site admin) for processing and approval.

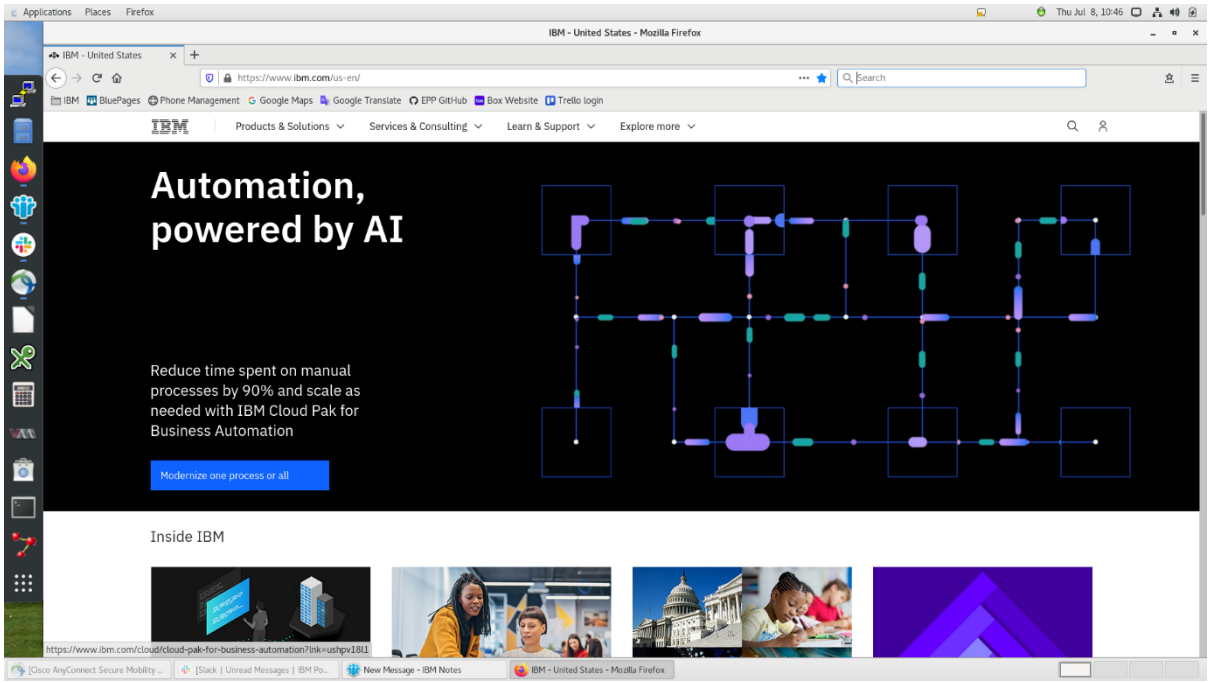
You will be notified when your request has been approved.

The customers who have entitlement to AIX product and have an active SW maintenance agreement can order AIX 7.2.5.3 ISO image and get the image files through the Entitled Systems Support (ESS) site:
https://www.ibm.com/servers/eserver/ess/index.wss?lnk=msdDO-enss-usen

Here are the steps to take to obtain AIX base ISO image.

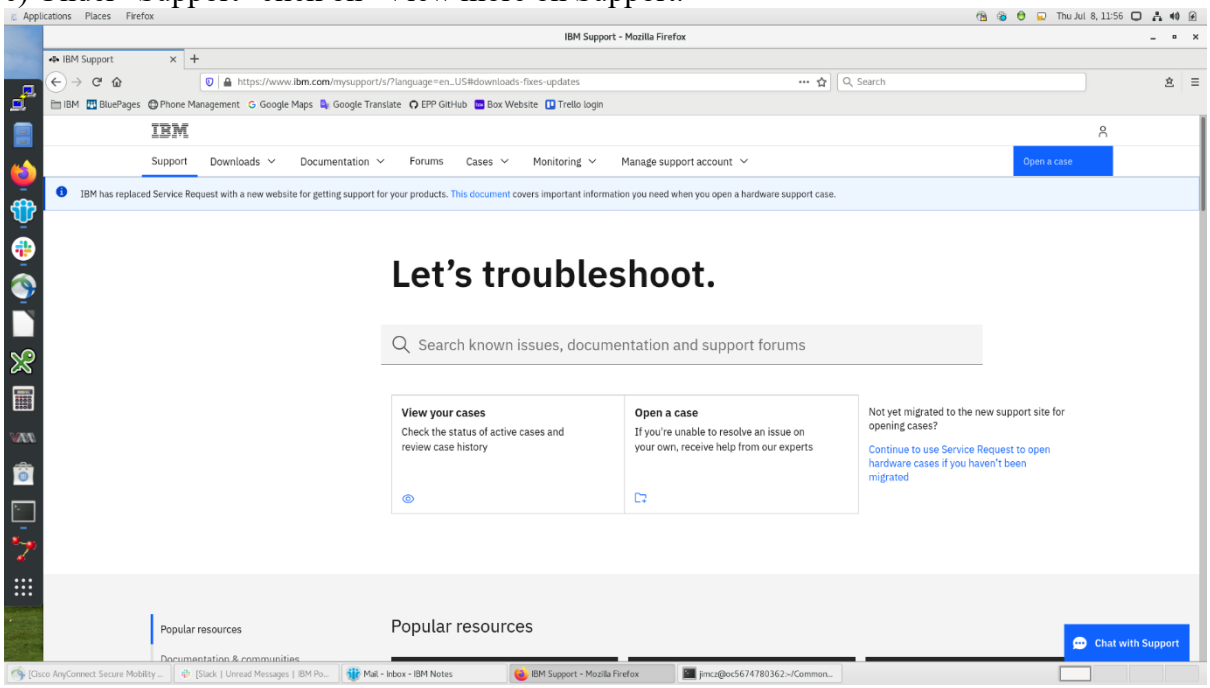
1. Go to the IBM site and navigate to the ESS site.

a) Go to https://www.ibm.com

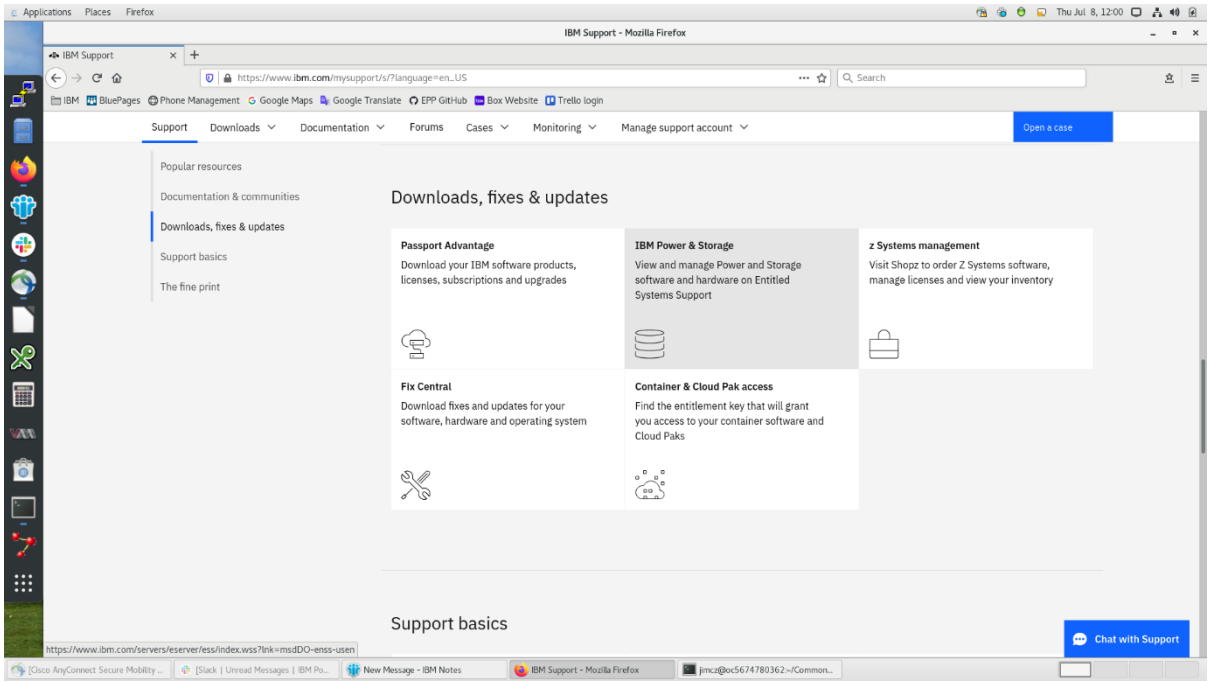


b) Click on "Learn & Support" pull down menu.

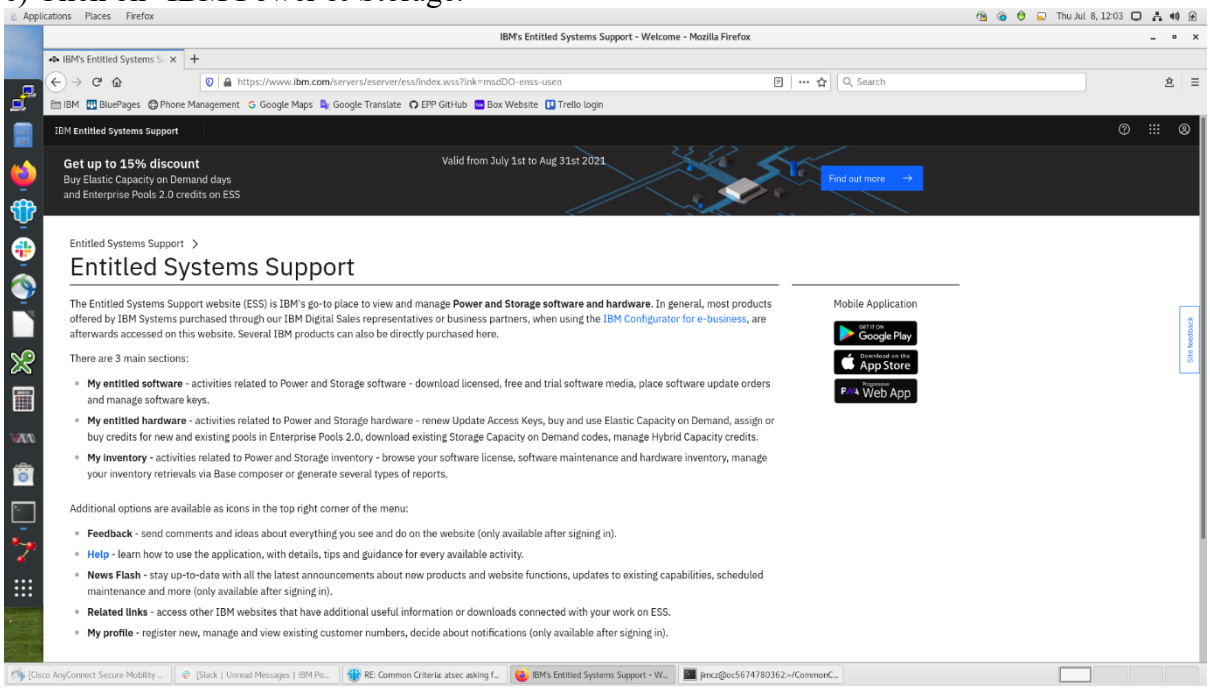
c) Under "Support" click on "View more on Support."



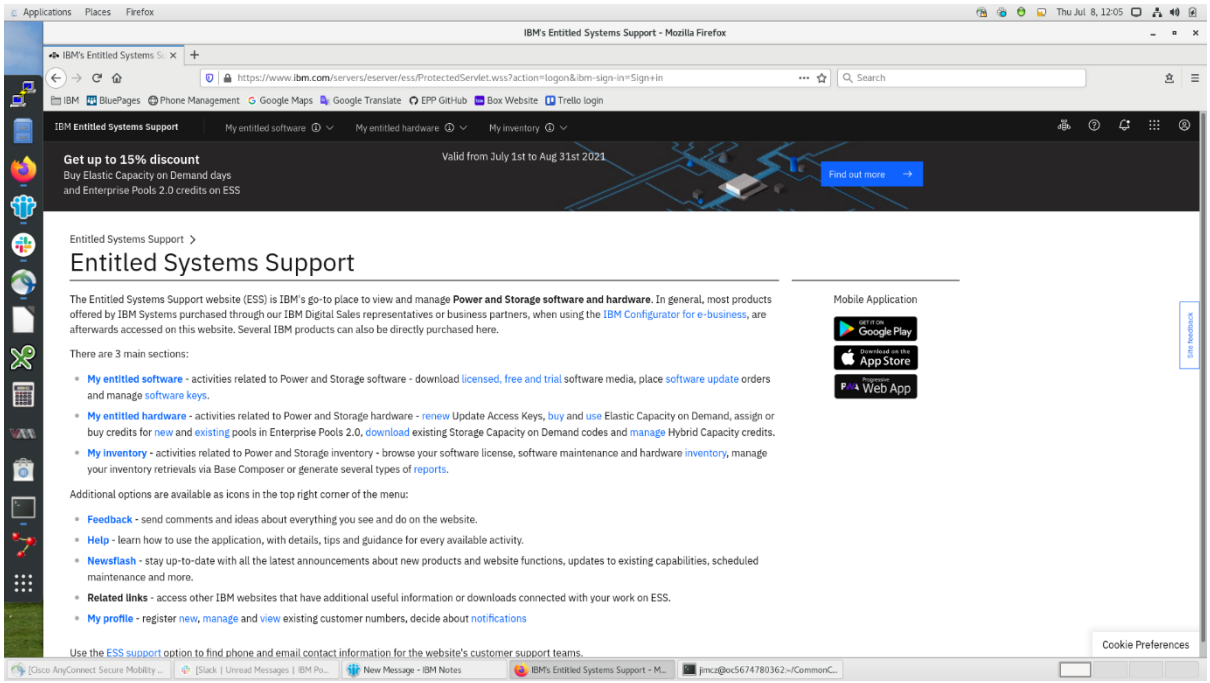
d) Scroll down to the "Downloads, Fixes & Updates" section.



e) Click on "IBM Power & Storage."

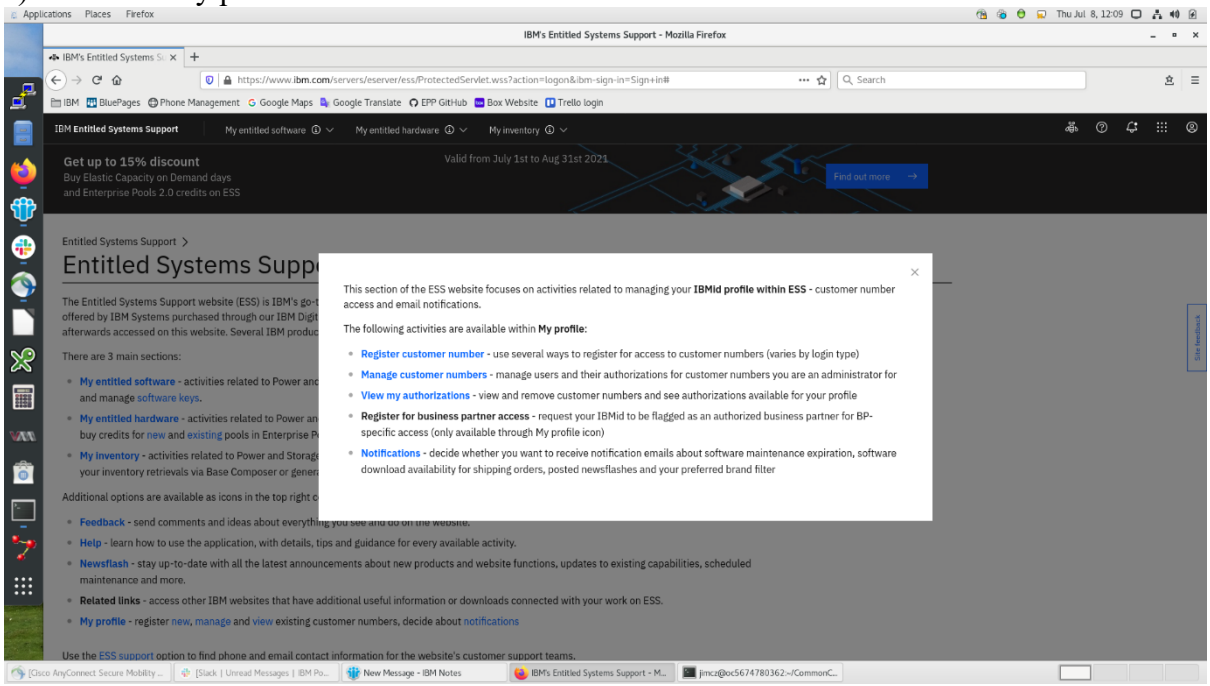


f) Scroll down and click on "Sign in" to sign in with your IBM Web ID.

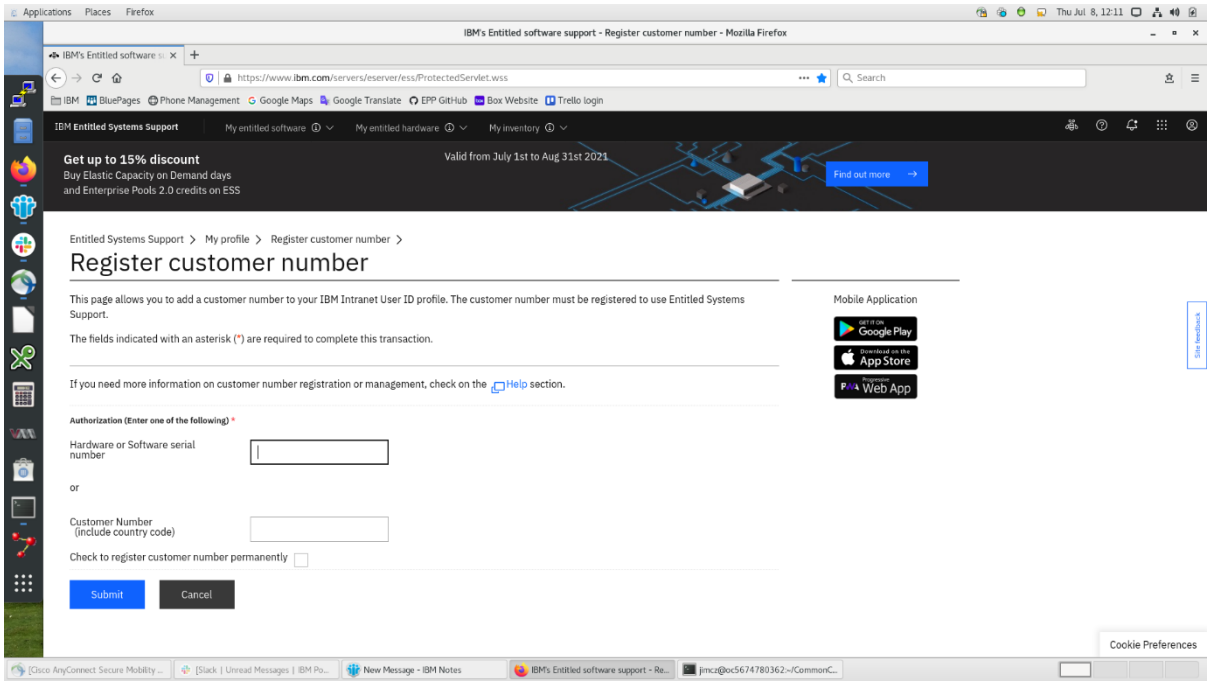


2. If you have never been on the site before you must "attach" yourself to your IBM Customer Number.

a) Click on "My profile."

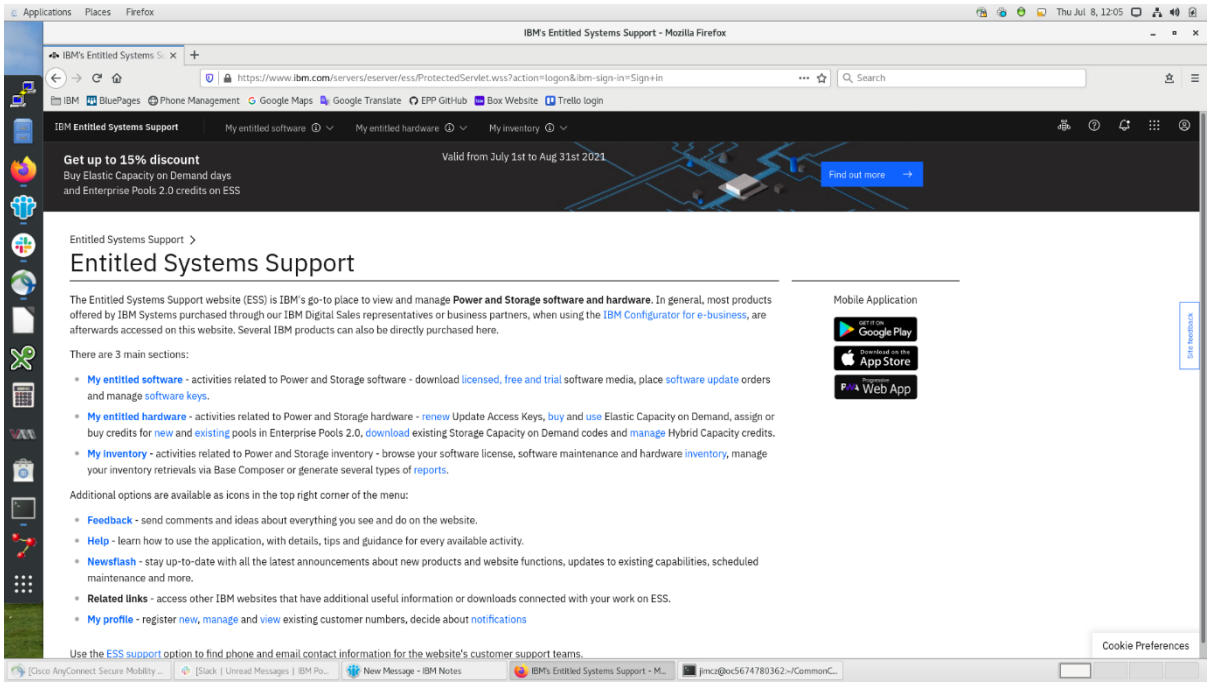


b) Click on "Register customer number."

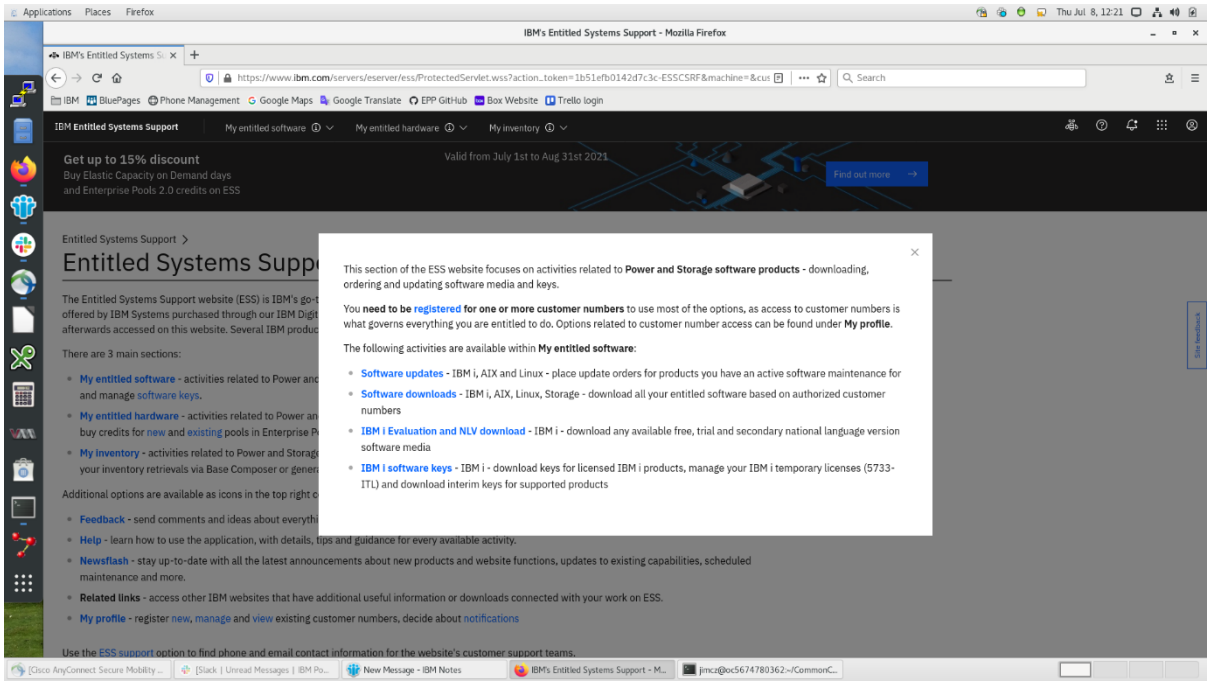


c) You may enter the country code/customer number combination or the HW/SW serial number of an IBM product purchased using that customer number. If you are the first to register for the customer, you will become the "primary" contact for that customer number and you have to approve future requests to attach Web IDs to that customer number. If you are not the first, your request to attach the customer number will be sent to the current primary contact for that customer number. You can go no further until your IBM Web ID is associated with one or more customer numbers.

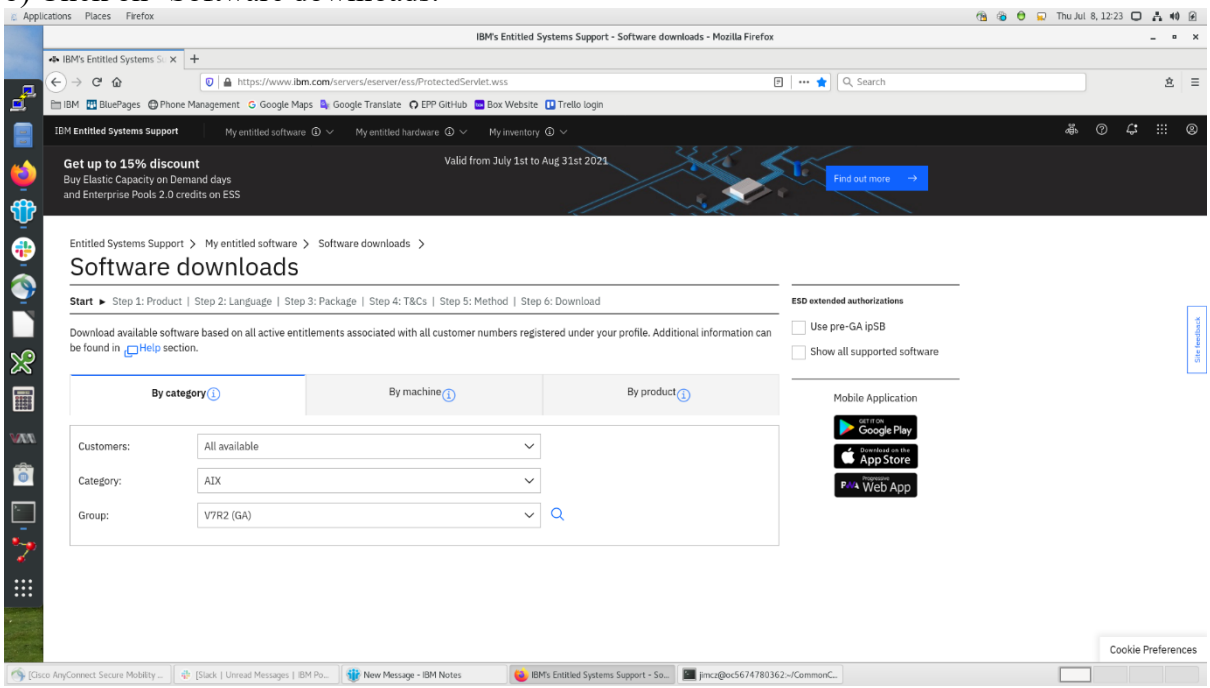
3. Start the software download.



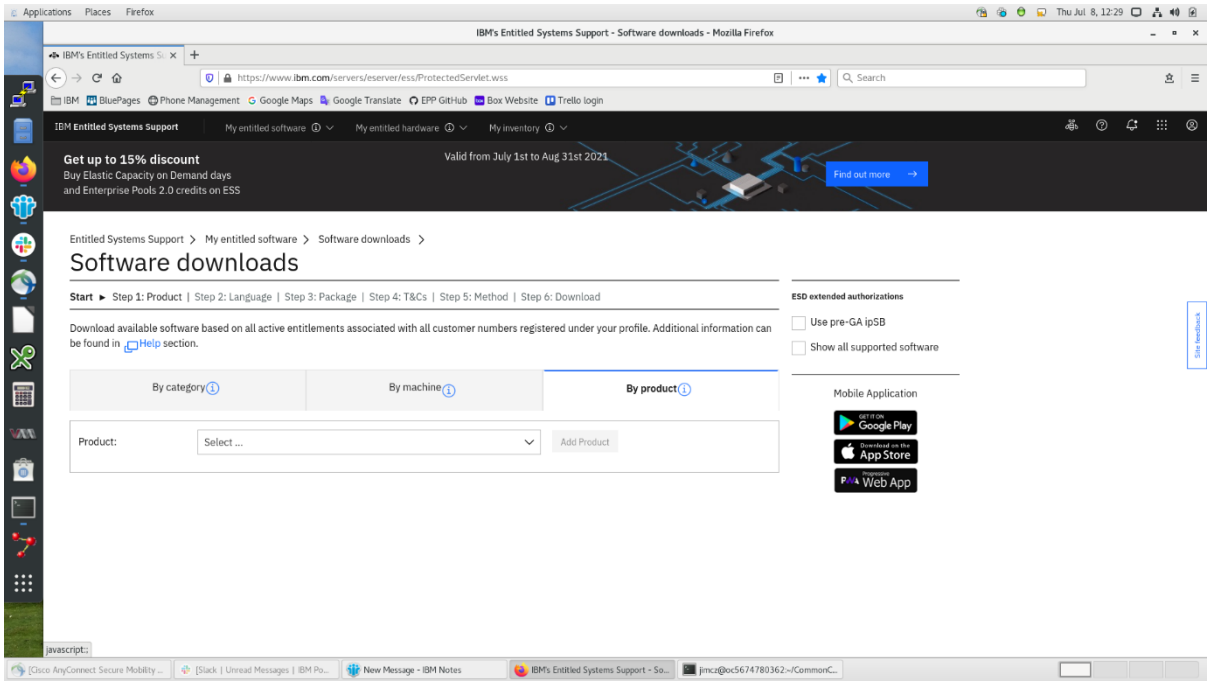
a) Click on "My entitled software."



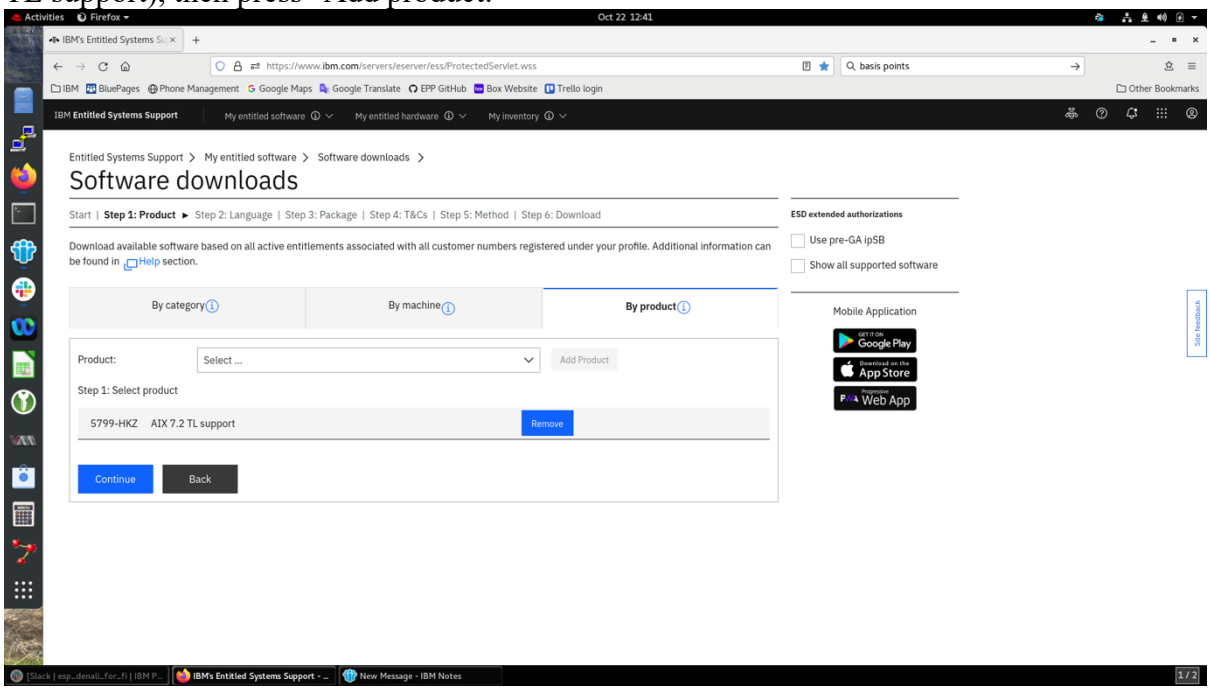
b) Click on "Software downloads."



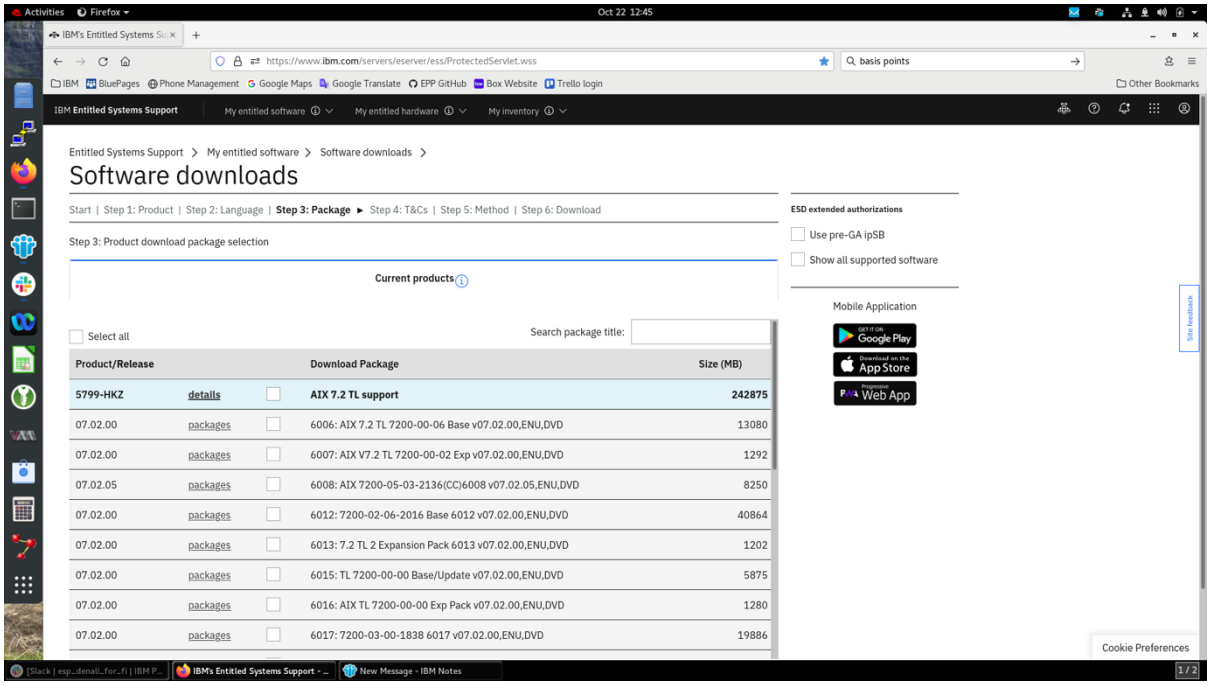
c) Click on the "By product" tab.



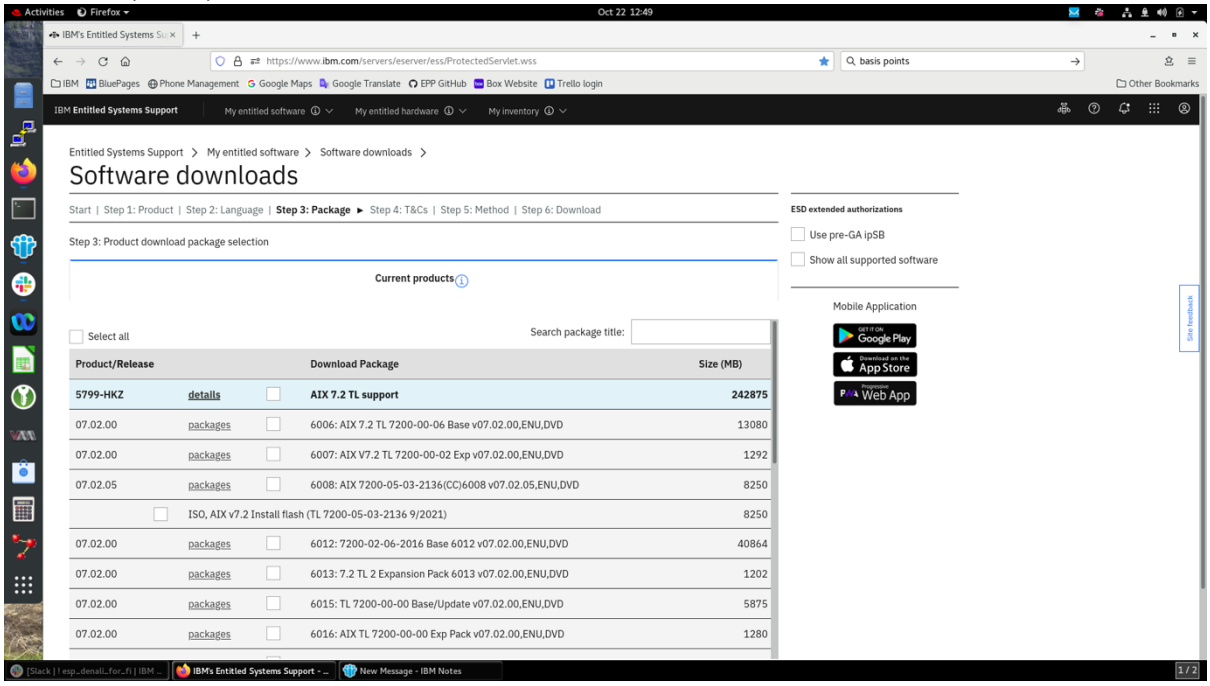
d) Find one of your software products in the selection box, in this case 5799-HKZ (AIX 7.2 TL support), then press "Add product."



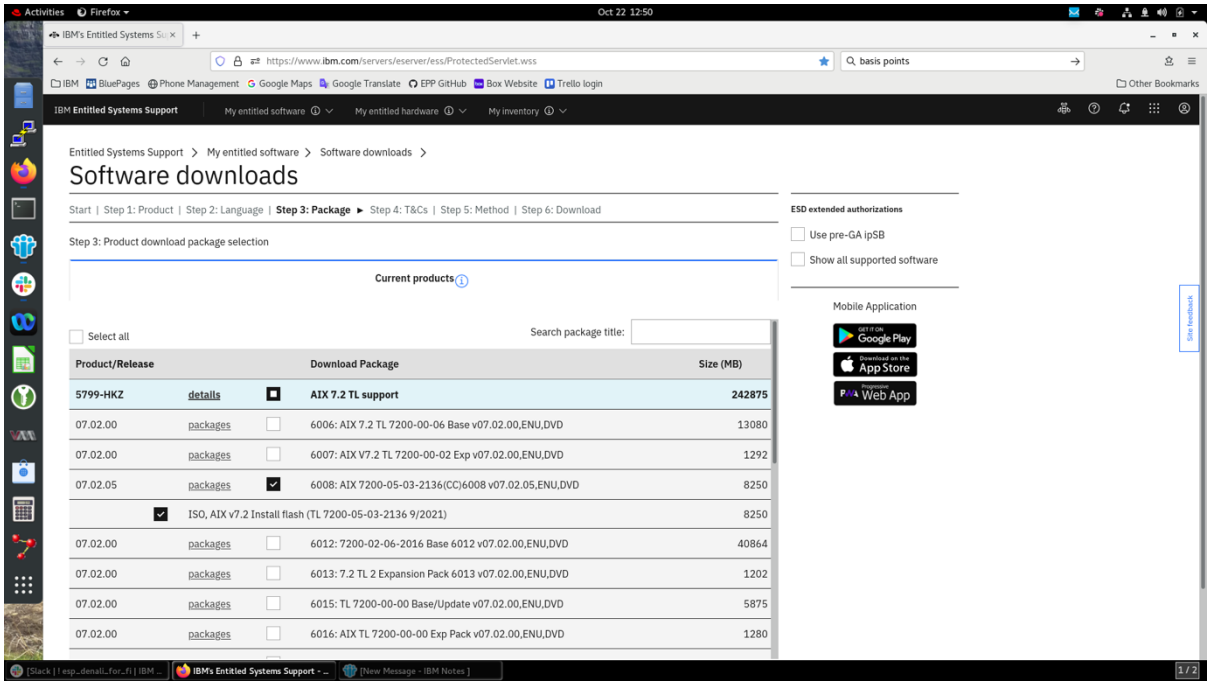
e) Click on the "Continue" button. You will get a list of your selected product and the delivery features under that product.



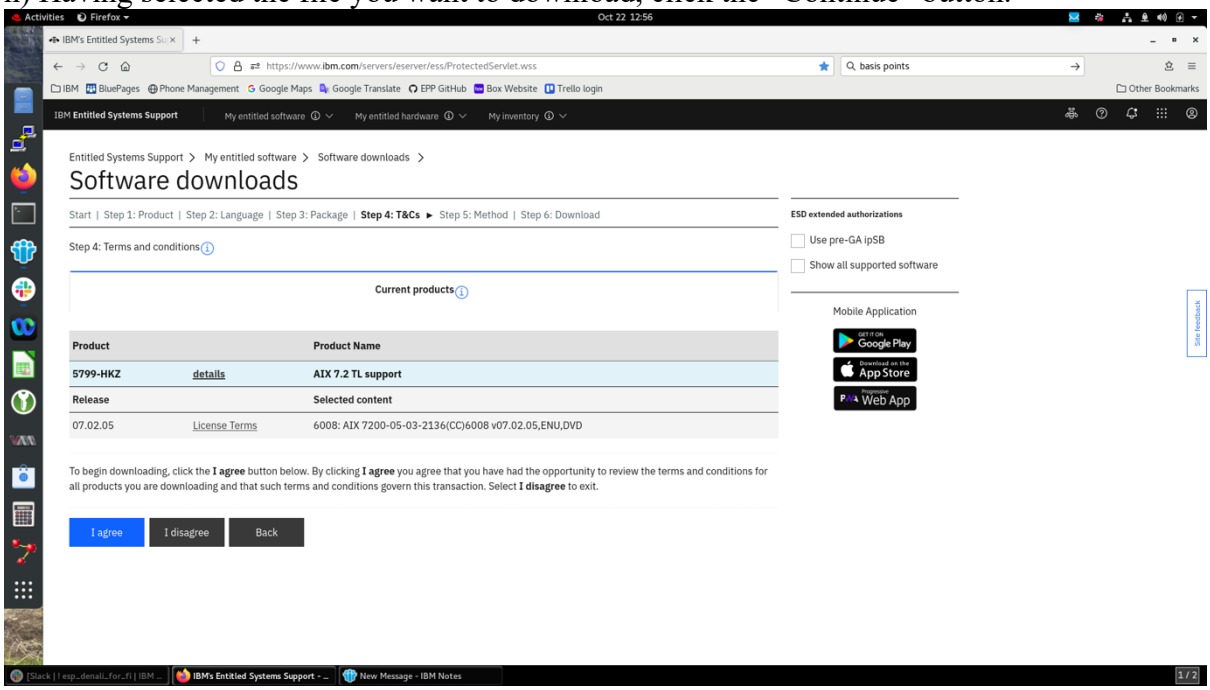
f) Click on the “packages” button next to “6008: AIX 7200-05-03-2136(CC)6008 v07.02.05,ENU,DVD”.



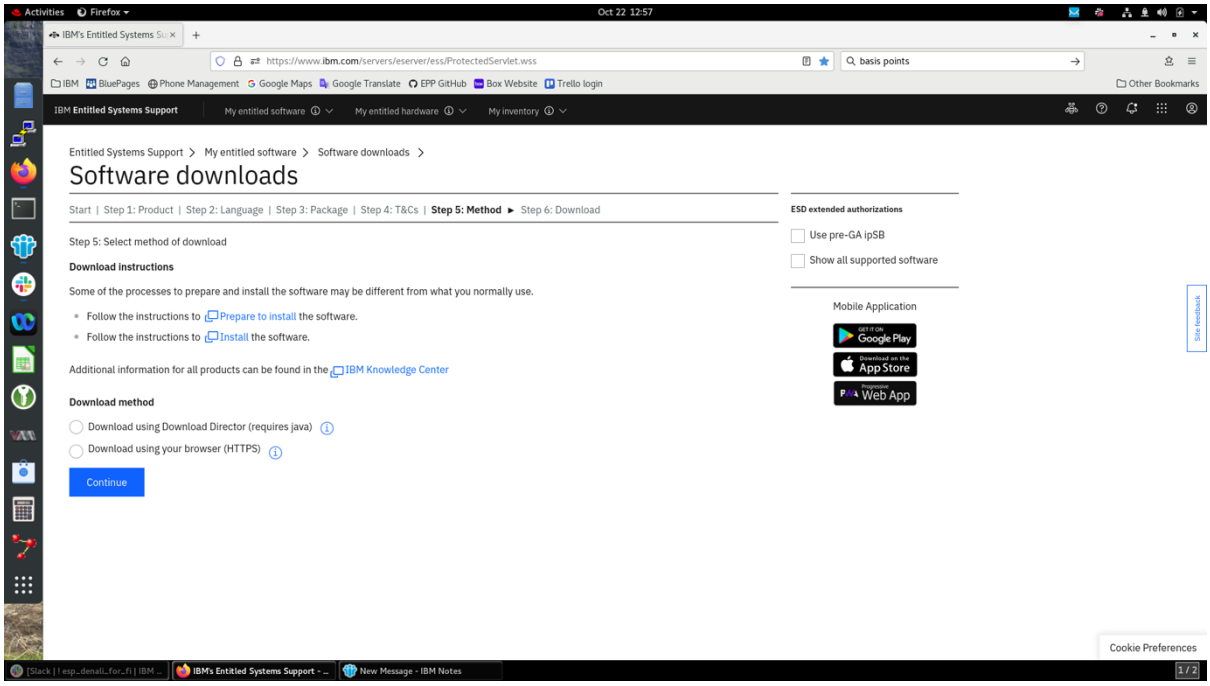
g) Click the check box next to the “ISO, AIX v7.2 Install flash (TL 7200-05-03-2136 9/2021)”



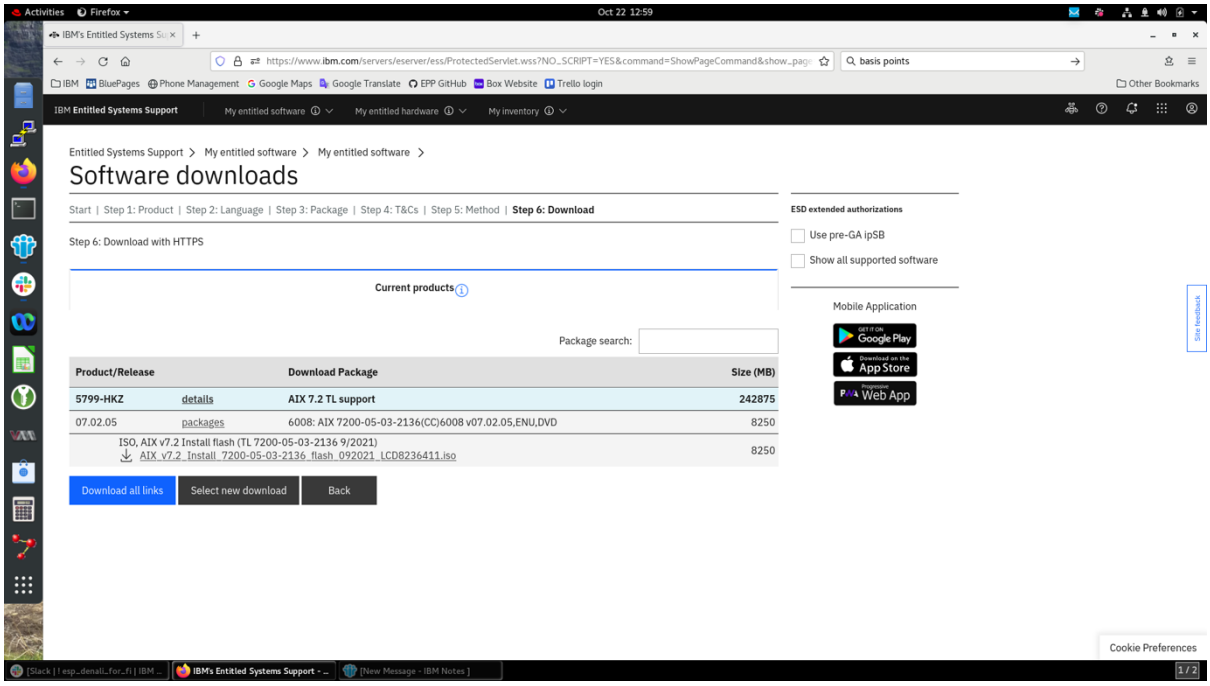
h) Having selected the file you want to download, click the “Continue” button.



i) Click on the "I agree" button to accept the licenses.



j) Choose your download method, either Download Director or HTTPS, and click the "Continue" button.



k) Click on the "AIX_v7.2_Install_7200-05-03-2136_flash_092021_LCD8236411.iso" link to begin the down load of the file.

Step 2: Save AIX base ISO image on the VIOS server

In the example below, the AIX 7.2.5.3 ISO file is saved in the **/home/padmin/72X_media/** directory on the VIOS server.

 # ls -al /home/padmin/72X_media/

Output:

total 16114648
drwxr-xr-x 2 padmin staff 256 Sep 08 10:52 .
drwxr-x--- 11 padmin system 4096 Oct 04 16:21 ..
-rw-r--r-- 1 padmin staff 43 Sep 08 10:51 AIX_v7.2_Install_7200-05-03-2136_flash_092021_LCD8236411.cksum
-rw-r--r-- 1 padmin staff 8250687488 Sep 08 11:07 AIX_v7.2_Install_7200-05-03-2136_flash_092021_LCD8236411.iso

Validate the checksum of the file. Use the following command to generate the checksum of the file.

 # cat /home/padmin/72X_media/AIX_v7.2_Install_7200-05-03-2136_flash_092021_LCD8236411.iso | openssl dgst -sha256

The output from this command must exactly match the following expected checksum.

(stdin)= d63c2844baec2f1a21d2caed6925c85a87f14abdd22c54324cf63f714197131f

If the checksums do not match, try downloading the image again. If the problem persists, contact your IBM representative.

Step 3: Create/Modify the media repository on the VIOS server

1. Create the repository in **rootvg** if it does not exist. If the repository already exists, see the next instruction in this step.

 # lsrep

Output:

The DVD repository has not been created yet.

 # mkrep -sp rootvg -size 4G

Output:

Virtual Media Repository Created
Repository created within "VMibrary" logic volume

2. Make sure that **rootvg** has enough free space in the physical partition to create the virtual media disk using lsrep. Add size to the repository with the **chrep** command.

 # chrep -size 9G

 # lsrep

Output:

Size(mb)	*Free(mb)*	*Parent Pool*	*Parent Size*	*Parent Free*
13257	*13257*	*rootvg*	*139776*	*46592*

Step 4: Create the virtual media disk on the VIOS server

Copy the **.iso** file to the VMLibrary repository. If the command fails, more space in the repository may be needed using the **chrep** command.

 # mkvopt -name AIX_72_5_3_ESD -file /home/padmin/72X_media/AIX_v7.2_Install_7200-05-03-2136_flash_092021_LCD8236411.iso -ro

Step 5: Verify the virtual media disk is part of the repository on the VIOS server

 # lsrep

Output:

```
Size(mb) Free(mb) Parent Pool       Parent Size      Parent Free
   13258     5389 rootvg              139776            46592

Name                                File Size Optical       Access
AIX_72_5_3_ESD                         7869 none        ro
```

Step 6: Create the file backed optical device and map it to the vhost name that corresponds to your LPAR

If the LPAR already contains a running AIX OS, log in as root on the target LPAR. Check the partition ID listed before the LPAR name using the **uname** command. (The ID is not necessarily the one from this example.)

 # uname -L

Output:

10 lpar-name

Or, if the LPAR is new, run the following command from HMC, replacing **<server name>** and <**lpar name>** with the values appropriate for your system.

 # lssyscfg -r lpar -m <server name> --filter "lpar_names=<lpar name>" -F lpar_id

Remember the **lpar-name** for use later and convert the partition ID into a 2-digit hexadecimal value (e.g., 10 -> 0a).
Return to VIOS and find the vhost adapter that corresponds to the partition ID by running **lsmap -all | grep vhost | grep 0x000000*XX***, replacing *XX* with the hexadecimal partition ID.

 # lsmap -all | grep vhost | grep 0x0000000a

Output:

```
vhost0          U9040.MR9.132931X-V1-C3                0x0000000a
```

Make note of the vhost adapter value displayed by the **lsmap** command because it will be used in the following steps.
Create the optical device and map it to the vhost adapter found under the previous command substituting your vhost in place of **vhost0** below.

 # mkvdev -fbo -vadapter vhost0 -dev vAIX_72_5_3_ESD

Output:

vAIX_72_5_3_ESD Available

Step 7: Assign the virtual media disk (image) to the optical device using the **loadopt** command on the VIOS server

Make note of the LUN corresponding to your optical device for reference in Step 8 in the next section. Also, substitute your vhost in place of **vhost0** below in the **lsmap** command..

 # loadopt -vtd vAIX_72_5_3_ESD -disk AIX_72_5_3_ESD

 # lsmap -vadapter vhost0

Output:

```
SVSA            Physloc                                      Client Partition ID
--------------- -------------------------------------------- ------------------
vhost0          U9040.MR9.132931X-V1-C3                      0x0000000a

VTD                   vAIX_72_5_3_ESD
Status                Available
LUN                   0x8500000000000000
Backing device        /var/vio/VMLibrary/AIX_72_5_3_ESD
Physloc
Mirrored              N/A
```

Boot the LPAR from the virtual DVD

Step 1: On the HMC, ensure that the Secure Policy is set to 1.
Run the following command replacing <server name> and <lpar name> with the values appropriate for your system.

 # chsyscfg -r lpar -m <servername> -i name=<lpar name>,secure_boot=1

For example:
If the server name is: `fvtzep2`
And the LPAR name is: `fvtzep2-lp6`
The command would be the following.

 # chsyscfg -r lpar -m fvtzep2 -i name=fvtzep2-lp6,secure_boot=1

Step 2: On the HMC, issue LPAR reboot while monitoring the LPAR console
a) Open a second terminal and login into HMC, using the following command to connect to LPAR console

 # vtmenu

Select the proper system name from the displayed system name pick list.
Then, select the LPAR from the LPAR pick list to open the LPAR's console.

On the first HMC console, activate the LPAR with the following command, replacing **<server name>** and **<lpar name>** with the values appropriate for your system. Note that Step 3 following this step will be time-sensitive.

 # chsysstate -m <server name> -r lpar -o shutdown -n <lpar name>

 # chsysstate -m <server name> -r lpar -o on -n <lpar name>

Step 3: Back on the LPAR console, quickly press 1 to select "SMS Menu" from the menu below when the following IBM screen appears.

IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM

```
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM

   1 = SMS Menu                      5 = Default Boot List
   8 = Open Firmware Prompt          6 = Stored Boot List
```

Step 4: Select "Select Boot Options" from the SMS menu below.

```
PowerPC Firmware
 Version FW950.00 (VM950_019)
 SMS (c) Copyright IBM Corp. 2000,2020 All rights reserved.
-------------------------------------------------------------------------------
 Main Menu
 1.  Select Language
 2.  Setup Remote IPL (Initial Program Load)
 3.  I/O Device Information
 4.  Select Console
 5.  Select Boot Options
-------------------------------------------------------------------------------
 Navigation Keys:
                              X = eXit System Management Services
-------------------------------------------------------------------------------
 Type menu item number and press Enter or select Navigation key:5
```

Step 5: Select "Select Install/Boot Device" from the Multiboot menu below.

```
PowerPC Firmware
 Version FW950.00 (VM950_019)
 SMS (c) Copyright IBM Corp. 2000,2020 All rights reserved.
-------------------------------------------------------------------------------
 Multiboot
 1.  Select Install/Boot Device
 2.  Configure Boot Device Order
 3.  Multiboot Startup <OFF>
 4.  SAN Zoning Support

-------------------------------------------------------------------------------
 Navigation keys:
 M = return to Main Menu
 ESC key = return to previous screen        X = eXit System Management Services
-------------------------------------------------------------------------------
 Type menu item number and press Enter or select Navigation key:1
```

Step 6: Select “Select CD/DVD” from the Select Device Type menu below.

PowerPC Firmware
Version FW950.00 (VM950_019)
SMS (c) Copyright IBM Corp. 2000,2020 All rights reserved.

Select Device Type
1. Tape
2. CD/DVD
3. Hard Drive
4. Network
5. List all Devices

Navigation keys:
M = return to Main Menu
ESC key = return to previous screen X = eXit System Management Services
---
Type menu item number and press Enter or select Navigation key:2

Step 7: Select “List All Devices” from the Select Media Type menu below.

PowerPC Firmware
Version FW950.00 (VM950_019)
SMS (c) Copyright IBM Corp. 2000,2020 All rights reserved.

Select Media Type
1. SCSI
2. SAN
3. SAS
4. SATA
5. USB
6. NVMe
7. List All Devices

Navigation keys:
M = return to Main Menu
ESC key = return to previous screen X = eXit System Management Services
---
Type menu item number and press Enter or select Navigation key:7

Step 8: Select “SCSI CD-ROM” from the Select Device menu below containing the LUN assigned in Step 7 of the previous section.

PowerPC Firmware
Version FW950.00 (VM950_019)
SMS (c) Copyright IBM Corp. 2000,2020 All rights reserved.

Select Device
Device Current Device
Number Position Name

1. - SCSI CD-ROM
(loc=U9040.MR9.132931X-V18-C3-T1-L8500000000000000)

Navigation keys:
M = return to Main Menu
ESC key = return to previous screen X = eXit System Management Services
---
Type menu item number and press Enter or select Navigation key:1

Step 9: Select "Normal Mode Boot" from the Select Task menu below.

Version FW950.00 (VM950_019)
SMS (c) Copyright IBM Corp. 2000,2020 All rights reserved.

Select Task

SCSI CD-ROM
(loc=U9040.MR9.132931X-V18-C3-T1-L8500000000000000)

1. *Information*
2. *Normal Mode Boot*
3. *Service Mode Boot*

Navigation keys:
M = return to Main Menu
ESC key = return to previous screen X = eXit System Management Services
---
Type menu item number and press Enter or select Navigation key:2

Step 10: Select "Yes" to exit the System Management Services and boot from the DVD-ROM.

PowerPC Firmware
Version FW950.00 (VM950_019)
SMS (c) Copyright IBM Corp. 2000,2020 All rights reserved.

Are you sure you want to exit System Management Services?
1. *Yes*
2. *No*

Navigation Keys:

X = eXit System Management Services

Type menu item number and press Enter or select Navigation key:1

Install AIX from the virtual DVD

After the LPAR boot from the virtual DVD, the console displays the following. The time and date values will be different on your system.

```
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM                         IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM    STARTING SOFTWARE    IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM       PLEASE WAIT...    IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM                         IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM IBM
|
Elapsed time since release of system processors: 0 mins 49 secs


-------------------------------------------------------------------------------
                                Welcome to AIX.
                   boot image timestamp: 14:47:17 10/19/2020
                 The current time and date: 14:50:09 03/18/2021
       processor count: 2;  memory size: 13216MB;  kernel size: 51872728
boot device: /vdevice/v-
scsi@30000003/disk@8200000000000000:\ppc\chrp\bootfile.exe
-------------------------------------------------------------------------------


 ******* Please define the System Console. *******

Type a 1 and press Enter to use this terminal as the
  system console.
Pour definir ce terminal comme console systeme, appuyez
  sur 1 puis sur Entree.
Taste 1 und anschliessend die Eingabetaste druecken, um
  diese Datenstation als Systemkonsole zu verwenden.
Premere il tasto 1 ed Invio per usare questo terminal
  come console.
Escriba 1 y pulse Intro para utilizar esta terminal como
  consola del sistema.
Escriviu 1 1 i premeu Intro per utilitzar aquest
  terminal com a consola del sistema.
Digite um 1 e pressione Enter para utilizar este terminal
  como console do sistema.
```

Step 1: Type 1 and press Enter to select current terminal as the console from the menu above.

Step 2: Type 1 and press Enter to select English from the menu below.

```
>>>  1 Type 1 and press Enter to have English during install.
     2 Entreu 2 i premeu Intro per veure la instal·lació en català.
     3 Entrez 3 pour effectuer l'installation en français.
     4 Für Installation in deutscher Sprache 4 eingeben
       und die Eingabetaste drücken.
     5 Immettere 5 e premere Invio per l'installazione in Italiano.
     6 Digite 6 e pressione Enter para usar Português na instalação.
     7 Escriba 7 y pulse Intro para la instalación en español.

    88  Help ?

>>> Choice [1]: 1
```

Step 3: Select “Change/Show Installation Settings and Install” from the Installation and Maintenance menu below.

```
                      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

    4 Make Additional Disks Available

    5 Select Storage Adapters



    88  Help ?
    99  Previous Menu

>>> Choice [1]: 2
```

Step 4: Select “System Settings” from the Installation and Settings menu below.

```
                           Installation and Settings

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

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

    2  Primary Language Environment Settings (AFTER Install):
         Cultural Convention................English (United States)
         Language ..........................English (United States)
         Keyboard ..........................English (United States)
         Keyboard Type......................Default
    3  Security Model.......................Default
    4  More Options  (Software install options)
    5  Select Edition.......................standard
>>> 0  Install with the current settings listed above.

                       +-------------------------------------------------
-
    88  Help ?         |    WARNING: Base Operating System Installation will
```

```
      99  Previous Menu  |    destroy or impair recovery of ALL data on the
                         |    destination disk hdisk0.
    >>> Choice [0]: 1
```

Step 5: Select “New and Complete Overwrite.”

```
                        Change Method of Installation

  Type the number of the installation method and press Enter.

    1 New and Complete Overwrite
      Overwrites EVERYTHING on the disk selected for installation.
      Warning: Only use this method if the disk is totally empty or if there
      is nothing on the disk you want to preserve.

>>> 2 Preservation Install
      Preserves SOME of the existing data on the disk selected for
      installation.  Warning: This method overwrites the usr (/usr),
      variable (/var), temporary (/tmp), and root (/) file systems.  Other
      product (applications) files and configuration data will be destroyed.









    88  Help ?
    99  Previous Menu

>>> Choice [2]: 1
```

Step 6: Select “Continue with choices indicated above” from the Change Disk(s) Where You Want to Install menu below.

```
                    Change Disk(s) Where You Want to Install

      Type one or more numbers for the disk(s) to be used for installation and
      press
      Enter. To cancel a choice, type the corresponding number and Press Enter.
      At least one bootable disk must be selected. The current choice is indicated
      by >>>.

              Name      Location Code   Size(MB)  VG Status   Bootable

      >>>  1  hdisk0    none             51200   rootvg          Yes    No









      >>>  0   Continue with choices indicated above
          55  More Disk Options
          66  Disks not known to Base Operating System Installation
          77  Display More Disk Information
          88  Help ?
          99  Previous Menu
```

```
>>> Choice [0]: 0
```

Step 7: Select “Security Model” from the Installation and Settings menu below.
Do not change any of the default settings on this menu.

```
                        Installation and Settings

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

    1  System Settings:
         Method of Installation.............New and Complete Overwrite
         Disk Where You Want to Install.....hdisk0

    2  Primary Language Environment Settings (AFTER Install):
         Cultural Convention.................English (United States)
         Language ...........................English (United States)
         Keyboard ...........................English (United States)
         Keyboard Type.......................Default
    3  Security Model.......................Default
    4  More Options  (Software install options)
    5  Select Edition.......................standard
>>> 0  Install with the current settings listed above.

                      +-------------------------------------------------
-
    88  Help ?        |    WARNING: Base Operating System Installation will
    99  Previous Menu |    destroy or impair recovery of ALL data on the
                      |    destination disk hdisk0.
>>> Choice [0]: 3
```

Step 8: Select “Continue to more software options” from the Security Models menu below.

```
                              Security Models

  Type the number of your choice and press Enter.


 1. Trusted AIX.......................................... No

 2. Digital Signature Policy............................. None

 3. Other Security Options  (Trusted AIX and Standard)
     Security options vary based on choices.
     LAS, SbD, BAS/CCEVAL


>>> 0   Continue to more software options.

    88  Help ?
    99  Previous Menu

>>> Choice [0]:
```

Step 9: Select both “OpenSSH Client” and “OpenSSH Server” from the Install Options menu below.

```
                            Install Options

 1.  Graphics Software.................................................. Yes
 2.  System Management Client Software.................................. Yes
 3.  OpenSSH Client Software............................................ No
 4.  OpenSSH Server Software............................................ No
```

```
 5.  Enable System Backups to install any system..... Yes
     (Installs all devices)


>>> 6.  Install More Software

    0  Install with the current settings listed above.

    88  Help ?
    99  Previous Menu

>>> Choice [6]: 3
```

The “OpenSSH Client Software” and “OpenSSH Server Software” should say “Yes” after they have been properly selected.

Step 10: Select “Install with the current settings listed above” in the Install Options menu below to return to be previous menu.

```
                              Install Options

 1.  Graphics Software..................................... Yes
 2.  System Management Client Software..................... Yes
 3.  OpenSSH Client Software............................... Yes
 4.  OpenSSH Server Software............................... Yes
 5.  Enable System Backups to install any system..... Yes
     (Installs all devices)


>>> 6.  Install More Software

    0  Install with the current settings listed above.

    88  Help ?
    99  Previous Menu

>>> Choice [6]: 0
```

Step 11: Select “Continue with Install” from the Overwrite Installation Summary menu below.
This will start the installation process.

```
                            Overwrite Installation Summary

Disks:  hdisk0
Cultural Convention:  en_US
Language:  en_US
Keyboard:  en_US
Graphics Software:  Yes
System Management Client Software:  Yes
OpenSSH Client Software:  Yes
OpenSSH Server Software:  Yes
Enable System Backups to install any system:  Yes
Selected Edition:  standard

Optional Software being installed:


>>> 1   Continue with Install
                      +-------------------------------------------------
-
    88  Help ?        |    WARNING: Base Operating System Installation will
    99  Previous Menu |    destroy or impair recovery of ALL data on the
                      |    destination disk hdisk0.
```

```
>>> Choice [1]: 1
```

The base AIX operating system will now install. It may take several minutes to install. The system will automatically reboot. Let the LPAR reboot and wait until the Set Terminal Type screen appears as shown in the next step.

Step 12: Select the appropriate Terminal Type (e.g. vt100 or vt320) for your console from the Set Terminal Type menu below.

```
                              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          aixterm
     ibm3151          tvi920          vt340          dtterm
     ibm3161          tvi925          wyse30         xterm
     ibm3162          tvi950          wyse50         lft
     ibm3163          vs100           wyse60         sun
     ibm3164          vt100           wyse100
     ibmpc            vt320           wyse350

                      +-----------------------Messages-----------------------
--
                      | If the next screen is unreadable, press Break (Ctrl-
c)
    88  Help ?        | to return to this screen.
                      |
>>> Choice []: vt320
```

Step 13: Select “Accept License Agreements” from the Software License Agreements menu below and press Enter.

```
                           Software License Agreements

Move cursor to desired item and press Enter.

  Show Installed License Agreements
  Accept License Agreements


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

Step 14: Select “yes” by pressing Tab, then press Enter to ACCEPT Installed License Agreements in the Accept License Agreements menu below. Press F10 (or Esc+0) to exit the License Agreement menu.

```
                           Accept License Agreements

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

                                                      [Entry Fields]
  ACCEPT Installed License Agreements                yes
+


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

```
                                COMMAND STATUS

Command: OK            stdout: no            stderr: no

Before command completion, additional instructions may appear below.


Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel        F6=Command
F8=Image            F9=Shell            F10=Exit            /=Find
n=Find Next
```

Step 15: Select “Accept Software Maintenance Terms and Conditions” from the Software Maintenance Agreement menu below and press Enter.

```
                        Software Maintenance Agreement

      Move cursor to desired item and press Enter.

        View Software Maintenance Terms and Conditions
        Accept Software Maintenance Terms and Conditions


      Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel          F8=Image
      F9=Shell            F10=Exit            Enter=Do
```

Step 16: Select “yes” by pressing Tab, then press Enter to ACCEPT Installed License Agreements in the Accept License Agreements menu below. Press F10 (or Esc+0) to exit the License Agreement menu.

```
                    Accept Software Maintenance Terms and Conditions

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

                                                          [Entry Fields]
        ACCEPT Installed License Agreements?             yes                +


      Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel        Esc+4=List
      Esc+5=Reset         F6=Command          F7=Edit             F8=Image
      F9=Shell            F10=Exit            Enter=Do
```

```
                                COMMAND STATUS

Command: OK            stdout: no            stderr: no

Before command completion, additional instructions may appear below.


Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel        F6=Command
F8=Image            F9=Shell            F10=Exit            /=Find
n=Find Next
```

Step 17: Select “Set Date and Time” from the Installation Assistant menu below and set the correct date, time, and time zone for your system. Press the F3 (or Esc+3) key to return to the Installation Assistant main menu.

```
                            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)
  Tasks Completed - Exit to Login


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

Step 18: Select "Set root Password" from the Installation Assistant menu below and set the root password for your system. Press the F3 (or Esc+3) key to return to the Installation Assistant main menu.

```
                              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)
  Tasks Completed - Exit to Login


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

Step 19: Select "Configure Network Communications" from the Installation Assistant menu below.

```
                              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)
  Tasks Completed - Exit to Login


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

Step 20: Select "TCP/IP Startup" from the menu.

```
                          Configure Network Communications

Move cursor to desired item and press Enter.

  TCP/IP Startup
  Add a Hostname to Access Other Systems
  Start NFS
  Mount a Remote File System
  Further Configuration
  Use DHCP for TCPIP Configuration & Startup


Esc+1=Help          Esc+2=Refresh       Esc+3=Cancel        F8=Image
F9=Shell            F10=Exit            Enter=Do
```

Step 21: Select “Standard Ethernet Network Interface” from the menu.

```
                        Available Network Interfaces

Move cursor to desired item and press Enter.

  en0      Standard Ethernet Network Interface
  et0      IEEE 802.3 Ethernet Network Interface

Esc+1=Help              Esc+2=Refresh           Esc+3=Cancel
F8=Image                F10=Exit                Enter=Do
/=Find                  n=Find Next
```

Step 22: 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.

The following network information needs to be entered and is specific to your site.

- HOSTNAME
- Internet ADDRESS
- Network MASK
- Default Gateway – Address
- NAMESERVER
- DOMAIN Name

Step 23: Select “Tasks Completed – Exit to Login” from the Installation Assistant menu below to exist the Installation Assistant.

```
                          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)
  Tasks Completed - Exit to Login


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

The console should display a login prompt.
AIX is now installed!

Configuration and ifix installation **are** still necessary before the product is in its evaluated configuration. This is explained in the following subsections, section 3, and section 4.

2.1 Displaying AIX Version and Maintenance Level

The following can be performed by an administrator or a user.
Check that the proper version of AIX is installed. The expected output is shown below.

1. Login to AIX

2. Run the **oslevel** command to display AIX version and maintenance level.

```
# oslevel -s
```

Output:

```
7200-05-03-2136
```

2.1.1 Modes of Operation

AIX provides two operation modes.

- Normal Mode
- Maintenance Mode

Normal Mode is the Common Criteria evaluated operation mode. Maintenance Mode is for offline maintenance by an administrator and requires the root password to be entered in order to enter into this mode.
System administrator can boot AIX into Normal Mode or Maintenance Mode using one of the follow methods.

- Select the boot mode in the SMS (System Management Services) menu during a boot.
- Use the **bootlist** command to change the boot mode, then reboot the system.

For Normal Mode, the system performs a **rootvg** boot when starting the system for general operations. The Normal Mode is the multiuser mode.
Maintenance Mode (also known as Service Mode) is used by system administrators to install the machine, restore an operating system backup, or perform maintenance on the **rootvg** volume group.
The Maintenance Mode has the follow functions:

Function	**Description**
Diagnostic Routines	This selection will test the machine hardware. Wrap plugs and other advanced functions will not be used.
Advanced Diagnostic Routines	This selection will test the machine hardware. Wrap plugs and other advanced functions will be used.
Task Selection (Diagnostics, Advanced Diagnostics, Service Aids, etc.)	This selection will list the tasks supported by these procedures. Once a task is selected, a resource menu may be presented showing all resources supported by the task.
Resource Selection	This selection will list the resources in the system that are supported by the diagnostic programs. Once a resource is selected, a task menu will be presented showing all tasks that can be run on the resource(s).
Single User Mode	The system will enter single-user mode for software maintenance.

2.2 List of LPPs Included

At this point of the configuration process, the following packages are now installed.

LPP name	**Description**
bos	AIX base operating system
device	AIX supported devices
sysmgt	System management tools

An additional OpenSSL LPP update must be performed as described in section 2.4.

2.3 Initialization of Trusted Update Keystore

Run the following command to initialize the public keystore for trusted update. This step must be done before OpenSSL FIPS module is installed and configured (section 2.4)

```
# /usr/sbin/pkgverify -I
```

Archieve the keystore:

```
# tar -cvf dsckeydb.tar /usr/lib/objrepos/dsc_key*
```

Store dsckeydb.tar in a safe location in case recovery is needed.

2.4 Installation and Configuration of OpenSSL FIPS Fileset

AIX ships the non-FIPS version of OpenSSL as the default fileset. The evaluated configuration requires the FIPS version of OpenSSL. The following steps installs the "openssl-fips-20.16.102.2103" fileset. The OpenSSL FIPS version needs to be installed and then enable using the environment variable "OPENSSL_FIPS". This ensures that commands that incorporate the OpenSSL module use the module in FIPS mode.

List the CD devices:

```
# lsdev |grep ^cd
```

Output:

```
cd0        Available       Virtual SCSI Optical Served by VIO Server
cd1        Available       Virtual SCSI Optical Served by VIO Server
cd2        Available       Virtual SCSI Optical Served by VIO Server
cd3        Available       Virtual SCSI Optical Served by VIO Server
```

Find the CD device that matches your LUN by iterating through each device from the **lsdev** command using the **lscfg** command below. This CD device will be used in the following commands.

Replace **cd3** below with each of the devices found in the **lsdev** command output above until you find the CD device that matches your LUN.

```
# lscfg -vpl cd3
```

Output:

```
cd3            U9040.MR9.132931X-V18-C3-T1-L8500000000000000
Virtual SCSI Optical Served by VIO Server
```

In this example, the AIX 7.2 TL 5 SP 3 ISO file is assigned to **cd3** and this should be used to access the LPPs. This is done through the following commands. Replace all instances of **cd3** with the proper value for your system.
First, use the **mkdir** command to create the mount directory, if it does not exist.

```
# mkdir /cd3
```

Then, create the CD filesystem and mount the device.

```
# crfs -v cdrfs -p ro -d'cd3' -m'/cd3' -A'no'
# mount /cd3
```

The **crfs** command creates the filesystem **/cd3** using the **/dev/cd3** device. The **mount** command mounts the device. It is not auto-mounted while creating the filesystem.
Once mounted, the FIPS-based OpenSSL fileset will be in the **/cd3/installp/ppc/FIPSopenssl** directory.
This directory will contain the following files.

```
fipsopenssl.base
fipsopenssl.license
fipsopenssl.man.en_US
```

Change Directory (**cd**) to this path and execute the **installp** command to install these filesets. Replace **cd3** with the proper value for your system.

```
# cd /cd3/installp/ppc/FIPSopenssl
# installp -acXYgd . all
```

After installing the fileset, enable FIPS mode for commands that use the OpenSSL module by adding the following line to the **/etc/environment** file.

```
OPENSSL_FIPS=1
```

Start new terminal sessions for the changes in **/etc/environment** file to be effective.

2.5 Installation of Required ifixes

AIX ifixes are digitally signed by IBM. The digital signatures are generated during the ifix creation process at IBM using an IBM private key specifically created for signing. The public key is provided with the evaluated configuration. This allows the evaluated configuration to verify the signature of the ifix prior to installing the ifix.

When installing any ifix in the evaluated configuration, the administrator is required to use the ifix commands defined in section 4.8.

The following paragraphs describe how to use the ifix commands to install the ifixes required for the evaluated configuration.

Before installing an ifix, please ensure sufficient space is available in the **/tmp** directory. The free space can be increased using the **chfs** command.

```
# chfs –a size=+32768 /tmp
```

The above **chfs** command increases the space of the **/tmp** directory by 32768 512-bytes blocks or 16MB. Note that the TD0325_fix.tar file is approximately 29MBs. Use this command again if more space is required.

First download the emgr ifix and its signature from the link below. This ifix must be installed before the other ones.

https://aix.software.ibm.com/aix/efixes/cc/CCEMGR_fix.tar

https://aix.software.ibm.com/aix/efixes/cc/CCEMGR_fix.tar.sig

```
# emgr_download_ifix -L <https_link> -P /tmp/
```

The above command download the ifix and its signature in /tmp dir. The signature of the ifix tar file needs to be validated as follows:

```
# openssl dgst -sha256 -verify
/etc/security/certificates/AIX_PSIRT_pubkey.txt -signature
/tmp/CCEMGR_fix.tar.sig /tmp/CCEMGR_fix.tar
```

If the result show "`Verified OK`", proceed to unpack and install the fix. Otherwise check if the previous download step is successful.

Unpack the ifix:

```
# tar -xvf /tmp/CCEMGR_fix.tar -C /tmp
```

Output

```
 x CCEMGR_fix/Advisory.asc, 2114 bytes, 5 media blocks.
 x CCEMGR_fix/Advisory.asc.sig, 256 bytes, 1 media blocks.
 x CCEMGR_fix/CCEMGR_fix.211215.epkg.Z, 15275 bytes, 30 media blocks.
 x CCEMGR_fix/CCEMGR_fix.211215.epkg.Z.sig, 256 bytes, 1 media blocks.
```

Install the ifix

```
# emgr_sec /tmp/CCEMGR_fix/CCEMGR_fix.211215.epkg.Z
```

The following ifixes must be installed for the evaluated configuration.

https://aix.software.ibm.com/aix/efixes/cc/CCECCSUMA1_fix.tar

https://aix.software.ibm.com/aix/efixes/cc/InstTU_fix.tar

https://aix.software.ibm.com/aix/efixes/cc/TD0325_fix.tar

https://aix.software.ibm.com/aix/efixes/security/efs_fix.tar

https://aix.software.ibm.com/aix/efixes/security/lscore_fix.tar

https://aix.software.ibm.com/aix/efixes/security/mount_fix.tar

https://aix.software.ibm.com/aix/efixes/security/openssh_fix14.tar

https://aix.software.ibm.com/aix/efixes/security/audit_fix.tar

https://aix.software.ibm.com/aix/efixes/security/kernel_fix3.tar

https://aix.software.ibm.com/aix/efixes/security/java_feb2022_fix.tar

Ifix Sha256 values
SHA256(CCEMGR_fix.tar)= 21917e86ea568d2b28dc87c4cf2b5e6727567cd51d6249b12dfa66faa415947f
SHA256(CCECCSUMA1_fix.tar)= 7ab9a64cd98d0b8160e6fc0b67b0cd72c9779315b9ad293659e9a98dfa5c33e8
SHA256(InstTU_fix.tar)= a2606ac587237cdc60ab30ebc6793e94c607f69f8bdf0d4910b4d9749d79d414
SHA256(TD0325_fix.tar)= cbbdff7aabec93b022872a4e57c9cf683ac806b1e0bcbf0dbbc1fa4fd9f32a5b
SHA256(efs_fix.tar)= 206fa67aae93f1a1df78b287e50a3d972092998a80b5320b1dfe3e4c00651cf3
SHA256(lscore_fix.tar)= c4f97465829e8a25cccf3260057383626635b5922f181a9450e6a5fbbf3558b9
SHA256(mount_fix.tar)= 438f2e0d1bddedbb4983e962538664b8f0c14899233b859c9dd2e66228484835
SHA256(openssh_fix14.tar)= 23a32151be35c6322d80d4a3633efff92ed3bab8b45cc21f3494c5d92cf7678
SHA256(audit_fix.tar)= 0c2ef6fcc0f743e0a1a0ab71a9451f1ca592c663eb434c6af5219bea98cd1aeb
SHA256(kernel_fix3.tar)= b217d346b5a6312ec15911ca9cbf64a5da098edbf8b47644273d71736c12de18
SHA256(java_feb2022_fix.tar)= 68f682d919024ab8eb1db5ab4fdcd1037709605424a55df5b7980baa9ff003e7

For each ifix, use the following command to download the ifix replacing **<https_link>** with one of the ifix links from above.

```
# emgr_download_ifix -L <https_link> -P /tmp
```

For each ifix, use the following command to apply the ifix to the system replacing ifix_tar_file with the actual ifix file name found in the /tmp directory.

```
# emgr_sec_patch /tmp/ifix_tar_file
```

Note **emgr_download_ifix** command may fail if there is not enough space in the **/tmp** directory. Check the file size of the ifix in the **/tmp** directory. If the file size is 0, it could be because there was not enough free space in the **/tmp** directory. Increase the size of **/tmp** and download the ifix again.

For more information on the patch management utilities, see section 4.8.

Warning: Failure to install all required ifixes will result in a non-conforming evaluated configuration and possible security vulnerabilities.

3 Configuring AIX for Common Criteria

The following subsections apply to the AIX operating system. All the configuration is to be done on AIX unless otherwise stated explicitly.

3.1 Root User Enabled

The Common Criteria evaluated configuration requires the root mode enabled. This is the default setting. No configuration is needed.

3.2 Boot Integrity (Secure Boot)

The following steps require an administrative account on the LPAR and an account on the HMC.

The AIX operating system supports the following Secure Boot policies:

Secure policy 1. Enabled (or log only)
Secure policy 2. Enforce (abort the boot operation if signature verification fails)

The evaluated configuration requires the Secure Policy to be set to 2.

Set the Secure Boot policy to 2 by performing the following.

1. On the HMC, run the following command replacing **<server name>** and **<lpar name>** with the values appropriate for your system.

   ```
   # chsyscfg -r lpar -m <server name> -i "name=<lpar name>,secure_boot=2"
   ```

   For example:

   If the server name is: `fvtzep2`
   And the LPAR name is: `fvtzep2-lp6`
   The command would be the following.

   ```
   chsyscfg -r lpar -m fvtzep2 -i "name=fvtzep2-lp6,secure_boot=2"
   ```

2. Reboot the LPAR to activate the new Secure Boot policy.
3. Check the Secure Boot policy from the LPAR.

   ```
   # lsattr -El sys0 -a secure_boot
   ```

   Output:

   ```
   secure_boot    Policy_2(Enabled,Stop-Check-Fail)   Secure Boot Mode
         False
   ```

   which shows the current Secure Boot polity value to be **Policy_2** and user-settable flags is **False** (last column), meaning non-administrators cannot change the value of this attribute.

This feature uses the IBM CLiC cryptographic modules (kernel and user space). The CLiC cryptographic modules do not require any special configuration.

3.3 Trusted Update for the OS and Applications

The following steps require an administrative account on the LPAR.

IBM digitally signs the **installp** command's cumulative updates prior to publishing the updates. The digital signatures are generated during the update creation process at IBM using an IBM private key specifically created for signing. The public key is provided with the evaluated configuration.

AIX supports 4 levels of **installp** package digital signature verification policies: none, low, medium, high.

- `none`: The installation process doesn't check for the signature for any package during the installation and update.

- `low`: If the signature verification fails, the file set is marked as UNTRUSTED and a warning message is issued, but the installation is allowed to complete.
- `medium`: If the signature verification fails, this policy expects a user response to confirm a force installation. If the operation is enforced, the failure is handled as specified by the low signature policy setting. Otherwise, the installation is marked as failed.
- `high`: If the signature verification fails, the installation is marked as failed.

The evaluated configuration requires the digital signature verification policy to be set to **medium**.

The **chsignpolicy** command is used to set the digital signature verification policy. Set the policy to **medium** using the following command. Setting the policy can only be performed using an administrative account.

```
# chsignpolicy -s medium   // set the policy to medium
```

To view the current policy, use the following command. Anyone can view the policy.

```
# chsignpolicy -p          // list the current policy
```

The **installp** command enforces the digital signature verification policy when the it installs a package. With the policy set at **medium**, the user is prompted for confirmation when the package signature validation fails. Answer "No" if that happens.
Warning: Allowing packages to install that fail the digital signature validation exposes the system to packages containing malware or virus. This must be prevented by answering "No" in the package installation dialog.
A summary report is given at the end of the **installp** output that lists the status of each of the software products that were to be installed by the update (success or failure). For those software products that could not be installed or whose installation failed, the user can search for the cause in the more detailed information that is continually displayed from the **installp** command during the installation process. In addition, the **installp** process' return code is 0 on success and nonzero on failure.
If the **installp** command fails to install the update due to a failed digital signature verification, delete the update and re-download the update. If the re-downloaded update fails, contact IBM.
If the **installp** command fails to install the update due to lack of available storage space, increase the file system size where the update is to be installed and try again.
The **installp** command may also fail if the update is already installed or the update is superseded by an previously installed update. In these cases, the LPAR already has the update applied.
The **installp** command uses the OpenSSL cryptographic module. Configuration of the OpenSSL module is described in section 2.4.

3.4 Stack Execution Disable (SED) Protection

The following steps require an administrative account on the LPAR.

AIX provides the **sedmgr** command for managing the Stack Execution Disable (SED) facility. You can use the command to enable and control the level of stack execution done in the system. Any changes to the system wide mode setting will take effect only after a system reboot.

The evaluated configuration requires the SED value to be set to **all**.

Set the system-wide SED as below. Then reboot the LPAR.

```
# sedmgr -m all
```

Check the configuration:

```
# lsattr -El sys0 |grep sed
```

Output:

```
sed_config    all      Stack Execution Disable (SED) Mode        True
```

3.5 Address Space Layout Randomization (ASLR)

The following steps require an administrative account on the LPAR.

AIX ASLR implementation defines three randomization attributes for all programs (main-program text, main-program data, and stacks) and two more randomization attributes for 64-bit programs (privately loaded libraries, and **shmat()** and **mmap()**).

Use the **vmo** command to configure the ASLR settings.

```
# vmo -r -o aslr=2 -o aslr32=0 -o aslr32r=333 -o aslr64=0 -o aslr64r=33333
```

aslr: global tuneable value controlling randomization supporting the following values.

- 0: ASLR is disabled or controlled by a restricted tunable.
- 1: Randomization is used for shared library areas
- 2: Randomization is used for shared library areas and for marked programs.

aslr32=0: allows 32bit application behavior controlled by the tunable aslr32r

aslr64=0: allows 64bit application behavior controlled by the tunable aslr64r

aslr32r=333: randomizes code and all data segments for 32bit applications

aslr64r=33333: randomizes code and all data segments for 64bit applications

Reboot the system for the new setting to take effect.

```
# shutdown -rF
```

To check the ASLR settings after the system reboots, log in and use the following command.

```
# vmo -F -L |grep -E "MAX|aslr"
```

Output:

```
NAME                      CUR    DEF    BOOT   MIN    MAX    UNIT           TYPE
aslr                      2      0      2      0      2      numeric          D
aslr32                    "0"    "1"    "0"                  string           D
aslr64                    "0"    "1"    "0"                  string           D
aslr32r                   333    0      333    0      333    numeric          D
aslr64r                   33333  0      33333  0      33333  numeric          D
aslr_r                    0      0      0      0      3      numeric          D
```

3.6 EFS Enablement

The following steps require an administrative account on the LPAR.

EFS must be enabled in the evaluated configuration. The administrator must only use the values specified below for the algorithms and ciphers.

Use the following **efsenable** command to enable the EFS.

```
# efsenable -a -k <key_algo> -f <cipher> -e <adm_key_algo>
```

where

<key_algo> and **<adm_key_algo>** must be: *RSA_2048* or *RSA_4096*
<cipher> must be: *AES_128_CBC or AES_256_CBC*

Check the settings using the following two commands.

```
# lssec -f /etc/security/user -s default -a efs_keystore_algo
```

Output:

```
default efs_keystore_algo=RSA_2048
```

```
# lssec -f /etc/security/user -s default -a efs_file_algo
```

Output:

```
default efs_file_algo=AES_256_CBC
```

For more information on EFS, please see EFS Encrypted File System in AIX Version 7.2 Security and AIX Version 7.2 commands. The EFS feature uses the IBM CLiC cryptographic modules (kernel and user space). The CLiC cryptographic modules do not require configuration.

3.7 Audit Configuration

The following steps require an administrative account on the LPAR.

The auditing subsystem enables the system administrator to record security-relevant information, which can be analysed to detect potential and actual violations of the system security policy.

A list of audit events built into AIX, along with a list of predefined audit objects, can be found in the **/etc/security/audit/events** file**.**

Auditing all possible events can produce a huge amount of data. Through audit controls (that is, modifying the **/etc/security/audit/config** configuration file), you can select events to be recorded.

Detailed audit configuration steps are given below for the evaluated configuration.

1. Edit the **/etc/security/audit/config** file to contain the following, if they don't already exist. Use the tab character to indent lines.

```
start:
        binmode = on
        streammode = off
        ignorenonexistentity = no

bin:
        trail = /audit/trail
        bin1 = /audit/bin1
        bin2 = /audit/bin2
        binsize = 10240
        cmds = /etc/security/audit/bincmds
        freespace = 65536
        backuppath = /audit
```

```
        backupsize = 0
        bincompact = off

stream:
        cmds = /etc/security/audit/streamcmds
        streamcompact = off

classes:
        CC_audit =
FILE_Open,FILE_Rename,FILE_Owner,FILE_Mode,FILE_Unlink,FILE_Close,FILE
_Read,FILE_Write,USER_Create,USER_Remove,USER_Change,USER_Chpass,USER_
Locked,User_Unlocked,GROUP_Change,GROUP_Create,GROUP_Remove,AUD_It,AUD
_CONFIG_WR,USER_Reboot,USER_Login,SSH_failpasswd,SSH_failpubkey,SSH_in
vldusr,SSH_connabndn,SSH_authsuccess,USER_Exit,S_ENVIRON_WRITE,S_GROUP
_WRITE,S_LIMITS_WRITE,S_LOGIN_WRITE,S_PASSWD_READ,S_PASSWD_WRITE,S_USE
R_WRITE,PROC_Setpri,PROC_Privilege,PROC_Change,PROC_SetUserIDs,PROC_Se
tpgid,PROC_SetGroups,PROC_SetRoles,USER_SU,LPA_Change

users:
        default = CC_audit
role:
```

Note that the `CC_audit` events include the following aspects.

- File and object events: FILE_Open, FILE_Rename, FILE_Owner, FILE_Mode, FILE_Unlink, FILE_Close, FILE_Read, FILE_Write
- User and Group management events: USER_Create, USER_Remove, USER_Change, USER_Chpass, USER_Locked, User_Unlocked, GROUP_Change, GROUP_Create, GROUP_Remove
- Audit start up, shutdown, and log data access events: AUD_It, AUD_CONFIG_WR
- System reboot, restart, and shutdown events: USER_Reboot
- Authentication events: USER_Login, SSH_failpasswd, SSH_failpubkey, SSH_invldusr, SSH_connabndn, SSH_authsuccess, USER_Exit
- Use of privileged/special rights events: S_ENVIRON_WRITE, S_GROUP_WRITE, S_LIMITS_WRITE, S_LOGIN_WRITE, S_PASSWD_READ, S_PASSWD_WRITE, S_USER_WRITE
- Privilege or role escalation events: PROC_Setpri, PROC_Privilege, PROC_Change, PROC_SetUserIDs, PROC_Setpgid, PROC_SetGroups, PROC_SetRoles, USER_SU, LPA_Change

2. Edit the **/etc/security/audit/objects** file to include the following, if they do not already exist in the file. Use the tab character to indent lines. Note that a blank line is required between the entries.

```
/etc/security/environ:
        w = "S_ENVIRON_WRITE"

/etc/security/group:
        w = "S_GROUP_WRITE"

/etc/security/limits:
        w = "S_LIMITS_WRITE"

/etc/security/login.cfg:
        w = "S_LOGIN_WRITE"

/etc/security/passwd:
```

```
        r = "S_PASSWD_READ"
        w = "S_PASSWD_WRITE"

/etc/security/user:
        w = "S_USER_WRITE"

/etc/security/audit/config:
        w = "AUD_CONFIG_WR"
        r = "AUD_CONFIG_READ"
```

3. Edit the **/etc/security/audit/events** file to include the following, if they do not already exist. Use the tab character to indent lines.

```
* SSH
       SSH_failpasswd = printf "%s"
       SSH_failpubkey = printf "%s"
       SSH_invldusr = printf "%s"
       SSH_authsuccess = printf "%s"
       SSH_connabndn = printf "%s"
```

The following table provides a description of these OpenSSH events.

OpenSSH event	Description
SSH_failpasswd	Authentication failure in Password auth method
SSH_failpubkey	Authentication failure in publickey-based or RSA-based auth method
SSH_invldusr	SSH connection failure due to invalid user
SSH_authsuccess	User authentication success
SSH_connabndn	SSH connection is abandon

4. Start auditing by using the following command.

```
# audit start
```

Auditing is now configured for the evaluated configuration.

To stop auditing, use the following command.

```
# audit shutdown
```

To delete the audit trail, use the following command.

```
# rm /audit/trail
```

To generate an audit report, use the following command.

```
# /usr/sbin/auditpr -i /audit/trail -h eRlrcpt
```

For more information on AIX audit and explanation of base audit events, please see Auditing Overview in AIX Version 7.2 Security.

3.7.1 Audit Event Format

Each AIX audit record includes base information and event specific information. The base information data structure is defined as *struct aud_rec* in the **/usr/include/sys/audit.h** file on an installed AIX system. The event specific information is defined in the **/etc/security/audit/events** file. The base audit record contains:

<event>	the audit event name
<status>	the audit result
<real>	the real user id
<login>	the login user id
<command>	the program (command line) name
<process>	the process id
<parent>	the parent process id
<thread>	the thread id
<time>	the the time at which the audit event occurs
<host>	the CPU on which the audit record is captured
<wpar name>	the wpar name
<role>	the role name/id
<privilege>	the effective privilege
<SL>	the sensitivity and clearance label
<TL>	the integrity label
<tail>	the event specific information

Note that <privilege>, <SL> and <TL> data are only collected if Trusted AIX is enabled. For the common criteria configuration, they are left as blank since Trusted AIX is not enabled. In the audit event formats, these fields are omitted.
The administrator may use the **auditpr** command to display selectively fields of interest. For example, the follow command will display the event name, the audit result, the login id, the real user id, the command name, the process id, the time stamp, and event specific information.

```
# auditpr -i /audit/trail -heRlrcpt -w
```

The **-h** option selects the fields to display and the order in which to display them. The frequently used selectors for the **-h** option are included here. For a full list of selectors, please see **auditpr** man page in AIX Version 7.2 Commands. The **-w** option display event specific information.

e	The audit event.
R	The audit status.
l	The login name of the user.
r	The real user name.
c	The command name.
t	The time the record was written.
p	The process ID.

The audit events specified in the common criteria configuration and their formats are shown below by using the following command.

```
# auditpr -i /audit/trail -heRlrcpPThWit -w
```

Output:

```
event       status    login   real    command                 process  parent   thread   host          wpar name
role      time

AUD_CONFIG_WR  OK       root    root    vi                      9044386  7012854  15008155
00FA212C4C000000 Global             No associated roles         Thu Jul 08 23:33:50 2021       audit object
write event detected /etc/security/audit/config

AUD_It      OK        root    root    audit                   13435336 13304268 27656619
00FA212C4C000000 Global             No associated roles         Fri Jul 09 21:37:13 2021       cmd: 4 arg: 0
```

FILE_Close OK root root auditbin 18285006 1 29688227 00FA212C4C000000 Global No associated roles Wed Jul 07 23:40:26 2021 file descriptor = 6

FILE_Mode OK root root chmod 13173186 9437524 27328883 00FA212C4C000000 Global No associated roles Thu Jul 08 23:55:04 2021 mode: 644 filename /var/perf/pm/daily/rtc04/pm_stats.send

FILE_Open OK root root auditbin 18285006 1 29688227 00FA212C4C000000 Global No associated roles Wed Jul 07 23:40:26 2021 flags: 0 mode: 0 fd: 6 filename /etc/vfs

FILE_Owner OK root root uncompress 9634210 9240892 23593467 00FA212C4C000000 Global No associated roles Thu Jul 08 23:34:32 2021 owner: 0 group: 0 filename /audit/tempfile.09240892

FILE_Read OK root root auditbin 18285006 1 29688227 00FA212C4C000000 Global No associated roles Wed Jul 07 23:40:26 2021 file descriptor = 6 filename =

FILE_Rename OK root root mv 9306370 9437524 17695165 00FA212C4C000000 Global No associated roles Thu Jul 08 23:55:01 2021 frompath: /var/perf/pm/daily/rtc04/stats.2021.07.08.Thu topath: /var/perf/pm/daily/rtc04/pm_stats.2021.07.08.Thu

FILE_Unlink OK root root compress 16384320 10748350 26280355 00FA212C4C000000 Global No associated roles Wed Jul 07 23:40:31 2021 filename /audit/tempfile.10748350

FILE_Write OK root root ls 10748348 11993466 28705213 00FA212C4C000000 Global No associated roles Wed Jul 07 23:40:31 2021 file descriptor = 1 filename =

GROUP_Change OK root root chgroup 14746070 15073632 28967257 00FA212C4C000000 Global No associated roles Thu Jul 08 12:51:17 2021 mygroup adms=

GROUP_Create OK root root mkgroup 15139296 15073632 12976455 00FA212C4C000000 Global No associated roles Thu Jul 08 13:29:13 2021 mygroup2

GROUP_Remove OK root root rmgroup 15139298 15073632 12976457 00FA212C4C000000 Global No associated roles Thu Jul 08 13:29:23 2021 mygroup2

LPA_Change OK root root chsec 9699772 9241024 15008129 00FA212C4C000000 Global No associated roles Thu Jul 08 23:20:22 2021 database:smd5 new values: lpa_module=/usr/lib/security/smd5

PROC_Change FAIL root root setsecattr 14680396 14811644 14811597 00FA212C4C000000 Global No associated roles Thu Jul 08 13:56:46 2021 Process: uprivs=PV_DAC_O,PV_NET_CNTL,PV_NET_PORT Attribute: -p 7405838

PROC_Privilege FAIL test4 test4 swrole 9699668 9306396 23593403 00FA212C4C000000 Global sa Thu Jul 08 22:25:09 2021 cmd: 30009 privset: 2800006:40000

PROC_SetGroups OK root root cron 12517796 5636532 26673493 00FA212C4C000000 Global No associated roles Fri Jul 09 21:15:00 2021 group set: system,bin,sys,security,cron,audit,lp

PROC_SetRoles OK test4 test4 swrole 9699670 9306396 23593405 00FA212C4C000000 Global sa Thu Jul 08 22:27:41 2021 rc: 0 numroles: 1 roleset: 2,0,0,0,0,0,0,0

PROC_SetUserIDs FAIL_PRIV root sshd sshd 12910854 12976478 27328865 00FA212C4C000000 Global No associated roles Fri Jul 09 12:06:36 2021 effect: 0, real: -1, saved: -1, login: -1

PROC_Setpgid FAIL_ACCESS root root ksh 12910856 12976478 27328867 00FA212C4C000000 Global No associated roles Fri Jul 09 12:06:49 2021 pid: 12845332, pgrp: 12845332

PROC_Setpri OK root root xmgc 852254 0 1376559 00FA212C4C000000 Global No associated roles Fri Jul 09 00:00:01 2021 new priority: 60

SSH_authsuccess OK root root sshd 12648936 6423034 27591145 00FA212C4C000000 Global No associated roles Fri Jul 09 21:13:08 2021 audit event euid 0 user root event 2 (SSH_authsuccess) remote ip (9.65.202.13)

SSH_connabndn OK root root sshd 9437500 6423034 17891673 00FA212C4C000000 Global No associated roles Thu Jul 08 23:34:36 2021 audit event euid 0 user root event 12 (SSH_connabndn) remote ip (9.160.20.196)

SSH_failpasswd OK root root sshd 9699652 6423034 22479297 00FA212C4C000000 Global No associated roles Thu Jul 08 22:12:09 2021 audit event euid 0 user (invalid user) event 4 (SSH_failpasswd) remote ip (9.160.20.196)

SSH_failpubkey OK root root sshd 12648936 6423034 27591145 00FA212C4C000000 Global No associated roles Fri Jul 09 21:13:05 2021 audit event euid 0 user root event 6 (SSH_failpubkey) remote ip (9.65.202.13)

SSH_invldusr OK root root sshd 9437486 6423034 23265619 00FA212C4C000000 Global No associated roles Thu Jul 08 23:31:32 2021 audit event euid 0 user (invalid user) event 9 (SSH_invldusr) remote ip (9.160.20.196)

S_ENVIRON_WRITE OK root root vi 15204844 15073632 12976583 00FA212C4C000000 Global No associated roles Thu Jul 08 12:30:20 2021 audit object write event detected /etc/security/environ

S_GROUP_WRITE OK root root vi 14746052 15073632 22741409 00FA212C4C000000 Global No associated roles Thu Jul 08 12:27:51 2021 audit object write event detected /etc/security/group

S_LIMITS_WRITE OK root root vi 14746060 15073632 22741417 00FA212C4C000000 Global No associated roles Thu Jul 08 12:29:05 2021 audit object write event detected /etc/security/limits

S_LOGIN_WRITE OK root root vi 15139226 15073632 14811551 00FA212C4C000000 Global No associated roles Thu Jul 08 12:25:57 2021 audit object write event detected /etc/security/login.cfg

S_PASSWD_READ OK root root cron 12648800 5636532 23265693 00FA212C4C000000 Global No associated roles Fri Jul 09 02:10:00 2021 audit object read event detected /etc/security/passwd

S_PASSWD_WRITE OK root root vi 9044340 7012854 12845493 00FA212C4C000000 Global No associated roles Thu Jul 08 20:27:31 2021 audit object write event detected /etc/security/passwd

```
S_USER_WRITE OK root root vi 9502998 7012854 22151527
00FA212C4C000000 Global No associated roles Thu Jul 08 20:12:59 2021 audit object
write event detected /etc/security/user

USER_Change FAIL root root chuser 14221576 15073632 29294953
00FA212C4C000000 Global No associated roles Thu Jul 08 13:07:55 2021 test4
group=mygroup

USER_Chpass OK root root passwd 15335890 15073632 22741289
00FA212C4C000000 Global No associated roles Thu Jul 08 12:16:51 2021 user: test4,
msg: OK

USER_Create OK root root mkuser 14942664 14483826 29557043
00FA212C4C000000 Global No associated roles Thu Jul 08 12:13:33 2021 test4

USER_Exit OK root root telnetd 9699734 4653502 22741389
00FA212C4C000000 Global No associated roles Thu Jul 08 20:48:36 2021 tty: User
logged out on /dev/pts/0

USER_Locked OK root root chsec 9044354 7012854 12845357
00FA212C4C000000 Global No associated roles Thu Jul 08 22:03:27 2021 user test4
has been locked

USER_Login OK root root tsm 9175374 9699682 23265645
00FA212C4C000000 Global No associated roles Thu Jul 08 20:30:43 2021 user: test4
tty: /dev/pts/0

USER_Reboot OK root root reboot 6095146 17498554 17695097
00FA212C4C000000 Global No associated roles Wed Jul 07 23:41:56 2021 root

USER_Remove OK root root rmuser 14483898 14680376 12976411
00FA212C4C000000 Global No associated roles Thu Jul 08 12:37:22 2021 test3
USER_SU OK test4 root su 8978862 14680482 28705235
00FA212C4C000000 Global No associated roles Thu Jul 08 14:21:48 2021 root

USER_Unlocked OK root root chsec 9306546 7012854 23593353
00FA212C4C000000 Global No associated roles Thu Jul 08 22:09:11 2021 user test4
has been unlocked
```

Warning: The size of the audit log may grow quickly if the system is running under heavy workload. The administrator should size the audit storage requirement adequately (by running the production work in rehearsal), monitor the audit space consumption, and archive the old logs periodically.

3.8 Configuration Options for OpenSSL

This section defines the configuration options for the **openssl s_client** command.
The **openssl s_client** command is included in the evaluated configuration. It is the only TLS client implementation and cryptographic module for direct use by users in the evaluated configuration. No other TLS client implementations and cryptographic modules shall be directly used by users in the evaluated configuration. When used, the **openssl** command must be configured in OpenSSL's FIPS mode as discussed in section 2.4.
Any administrator or non-administrator can execute the **openssl s_client** command on the LPAR to make an arbitrary TLS client connection to a TLS server.

The following cipher suites are supported by OpenSSL for TLS communication in the evaluated configuration.

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

To comply with the evaluated configuration, the following **openssl s_client** options must be included on the command line.

`-cipher cipherlist`

Specifies the TLS cipher suites used by the TLS client connection. To limit the cipher suites to those listed above, use the following values separated by a colon (:) character.

- AES128-SHA
- AES-256-SHA
- AES128-SHA256
- AES256-SHA256
- AES128-GCM-SHA256
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-GCM-SHA384

`-connect host:port`

Sets the reference identifier. The value for `host` will be used as the reference identifier when validating the server certificate.

`-crl_check_all`

Checks the revocation status of the certificate chain using a certificate revocation list (CRL).

`-CAfile file`

Specifies the file containing the trusted certificates.

`-tls1_2`

Limits the protocol version to only TLS v1.2.

`-verify_return_error`

Forces the connection to terminate when an error is detected from the server handshake.

`-x509_strict`

Forces X.509 certificate compliance checking.

3.9 Configuration for OpenSSH

The following steps require an administrative account on the LPAR.

The following OpenSSH configuration is required for the evaluated configuration. These steps configure both the OpenSSH server and client.

OpenSSH server:

1. In the **/etc/ssh/sshd_config** file, add or replace the following settings.

```
fipsforopenssh yes
RekeyLimit 500M 1h
```

The **fipsforopenssh** option above enforces the following configuration.

i. PubkeyAcceptedKeyTypes: rsa-sha2-256,rsa-sha2-512,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384
ii. Ciphers: aes128-ctr,aes256-ctr,aes128-cbc,aes256-cbc,aes128-gcm@openssh.com,aes256-gcm@openssh.com
iii. MACs: hmac-sha1,hmac-sha2-256,hmac-sha2-512
iv. KexAlgorithms: ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
v. DRBG uses aes256-ctr as the default

2. Restart the **ssh** daemon using the following commands. The daemon must be restarted for the changes to take effect.

```
# stopsrc -s sshd
# startsrc -s sshd
```

OpenSSH client:

1. In the **/etc/ssh/ssh_config** file, add the following settings for every defined host (including **Host ***). If no hosts are defined, then add **Host *** followed by the following settings.

```
fipsforopenssh yes
RekeyLimit 500M 1h
```

Only OpenSSH is included in the evaluated configuration. Other SSH authentication software is not included in the evaluated configuration.

Additionally, the OpenSSH host-based keys are generated while installing the OpenSSH fileset as part of AIX base image installation. The keys generated are stored in the **/etc/ssh** directory.

The OpenSSH client and server use the OpenSSL cryptographic module. Configuration of the OpenSSL module is described in section 2.4.

3.9.1 Disable telnet ftp rsh krsh rlogin krlogin rexec Services

Use the following commands to disable telnet, ftp, rsh, krsh, rlogin, krlogin, and rexec services:

```
# chsubserver -d -v telnet -p tcp
# chsubserver -d -v ftp -p tcp
# chsubserver -d -v shell -p tcp
# chsubserver -d -v kshell -p tcp
# chsubserver -d -v login -p tcp
# chsubserver -d -v klogin -p tcp
# chsubserver -d -v exec -p tcp
# refresh -s inetd
```

3.10 IBM Java and SUMA Configuration

The following steps require an administrative account on the LPAR. The evaluated configuration requires the following IBM Java configuration.

The **suma** command uses IBM Java's TLS to connect to the IBM fix server to download cumulative updates. The command is required to use the IBMJCEPlusFIPS cryptographic library provider in the evaluated configuration. The following steps configure IBM Java and the **suma** command to use this cryptographic library provider.

Modify the IBM Java configuration file **/usr/java8_64/jre/lib/security/java.security** as follows. (Note that the files to be edited in the section are typically read-only by default.)

1. Make sure the cryptographic library providers include the FIPS module (IBMJCEPlusFIPS).

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.crypto.plus.provider.IBMJCEPlusFIPS
security.provider.4=com.ibm.crypto.plus.provider.IBMJCEPlus
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.security.sasl.IBMSASL
security.provider.8=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.9=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.10=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.11=sun.security.provider.Sun
```

2. Enable Online Certificate Status Protocol (OCSP) checking by uncommenting the following line in the file.

```
ocsp.enable=true
```

Run the following **suma** commands to configure the command to use the IBMJCEPlusFIPS cryptographic library provider and to invoke IBM Java certificate status checking via OCSP.

```
# suma -c -a USE_FIPS_PROVIDER=yes
# suma -c -a USE_CC_CIPHERS=yes
# suma -c -a CHECK_CERTIFICATE_REVOCATION=yes
# suma -c                          // verify the setting
```

The reference identifier used by the **suma** command is pre-defined and fixed by default. It is not intended to be modified.

The **suma** process returns 0 on success and nonzero on failure.

If the **suma** command fails to connect to the IBM fix server, the failure may be local to your site. Check that your site network is working and that the system has access to the Internet, then retry the command. If the command continues to fail to connect to the IBM fix server, contact your IBM representative.

If the **suma** command fails to install the update due to lack of available storage space, increase the file system size where the update is to be installed and try again.

The IBMJCEPlusFIPS cryptographic library provider uses the IBM ICC cryptographic module. No special configuration of the ICC module is required.

4 Administration Tasks

The following subsections apply to the AIX operating system.

4.1 Access Control of System Directories and Files

AIX uses the access control to prohibit unprivileged users from modifying the following.

Kernel and its drivers/modules in:

- /dev/
- /unix/
- /usr/lib/

Security audit logs in:

- /audit/

Shared libraries in:

- /usr/lib/

System executables in:

- /usr/bin/
- /usr/sbin/

System configuration files in:

- /etc/
- /etc/security/
- /etc/security/audit/

AIX uses the access control to prohibit unprivileged users from reading the following.

Security audit logs in:

- /audit/

System-wide credential repositories in:

- /etc/security/
- /var/efs/

For more information on access control, please refer to the DAC (Discretionary Access Control) mechanism in the section “Access Control List” in the AIX Version 7.2 Security. Additionally, please see the **chmod** command in the AIX Version 7.2 Commands

Warning: The permission and the integrity of the privileged system files are critical to the system security and function. Administrators are encouraged to use additional software such as IBM PowerSC to monitor them and to receive alerts if any of the file permission or content is modified. Note that PowerSC is not included in the evaluated configuration.

4.2 Setup for Login Warning Banner

The following steps require an administrative account. The evaluated configuration is required to support a login warning banner for sites that use these banners.

The following steps configure the login warning banner for both the local console and for SSH connections.

- For the local console:

  Set the herald attribute in the **/etc/security/login.cfg** file using the follow command.

```
    # chsec -f /etc/security/login.cfg -s default -a herald="\nThis banner comes
from the herald of login.cfg.\n\nlogin: "
```

- For remote login (OpenSSH)

  1. Edit **/etc/ssh/sshd_config** to contain the following line.

     ```
     Banner /etc/ssh_banner
     ```

  2. Create the SSH banner file **/etc/ssh_banner** and add a banner message in the file.
  3. Restart **sshd** for the banner to take effect.

     ```
     # stopsrc -s sshd
     # startsrc -s sshd
     ```

4.3 Setup for OpenSSH User Public Key Based Authentication

The following steps can be performed by administrative users and non-administrative users to create an asymmetric key pair used with OpenSSH for user public key authentication. The evaluated configuration supports both public key authentication and password authentication.

1. Generate ECDSA asymmetric key pair:

   ```
   # ssh-keygen -t ecdsa-sha2-nistp384 (or ecdsa-sha2-nistp256)
   ```

   This generates key pairs **~/.ssh/id_ecdsa** and **~/.ssh/id_ecdsa.pub**.

   For RSA asymmetric key pair generation:

   ```
   # ssh-keygen -t rsa -b 4096 -E sha256   #(or sha512)
   ```

   This generates key pairs **~/.ssh/id_rsa** and **~/.ssh/id_rsa.pub**.

2. On the remote server to allow key based authentication, add the content of **id_ecdsa.pub** (from the above step) to **~/.ssh/authorized_keys**.

4.4 Setup for Password Hash Algorithm

The following steps require an administrative account. It is highly recommended to change the default password hash algorithm in the evaluated configuration as follows.

Change the password hash algorithm to **sha256**.

```
# chsec -f /etc/security/login.cfg -s usw -a
pwd_algorithm=ssha256
```

4.5 Configuration of User Session Timeout

The evaluated configuration only specifies that the session timeout to be configurable. It does not require session timeouts to be enabled or disabled and it does not require specific timeout values. Configure these values according to your site policies.

The local console session timeout can be configured by both administrators and non-administrators and the configuration applies to their account's session.

To configure the local console session timeout for an account, add the following lines to the **/etc/profile** file (for the root account) or the **$HOME/.profile** file (for non-administrative users), replacing **time_in_seconds** with the actual number of seconds and export the TMOUT variable.

```
TMOUT = time_in_seconds
export TMOUT
```

The following OpenSSH-related steps require an administrative account when performed.

To configure the OpenSSH server's session timeout, add or edit the following lines in the **/etc/ssh/sshd_config** file. The evaluated configuration does not specify the values to be used; thus, the following is only an example of what can be used.

```
ClientAliveInterval 300
ClientAliveCountMax 3
```

OpenSSH calculates the timeout value as follows.

```
Timeout_value = ClientAliveInterval * ClientAliveCountMax
                  (equivalent to 900s or 15min using the above
                  settings)
```

Restart the sshd for the change to take effect.

```
# stopsrc -s sshd
# startsrc -s sshd
```

4.6 User Account Management

For the following steps require an administrative account to set/modify the referenced attributes.

Most user attributes can be found in the **/etc/security/user** file. They can be displayed via **lssec** and set by **chsec** commands using the syntax below. Replace **user_name**, **attribute**, and **attribute=value** with the appropriate values.

```
# lssec -f  /etc/security/user -s user_name -a attribute
# chsec -f  /etc/security/user -s user_name -a attribute=value
```

The **longretries** attribute controls how many times a user's authentication is allowed to fail before the account is locked. Once the account is locked, administrative action is required to unlock the account. The evaluated configuration does not define a specific value for unsuccessful login attempts, so organizations may choose their own value. The following example uses a value of 3.

```
# chsec -f  /etc/security/user -s default -a loginretries=3
```

Note that using **default** in the place of **user_name** makes the attribute applicable to any user who does not have the attribute set explicitly.

Password requirements can be set similarly using the following attributes. The evaluated configuration does not define specific values for the password requirements, so organizations may choose their own values. The following **chsec** commands contain example values only.

minlen—Minimum password length
minspecialchar—Minimum number of special characters in a password
mindigit—Minimum number of numeric characters in a password
minupperalpha—Minimum number of uppercase characters in a password
minloweralpha—Minimum number of lowercase characters in a password

```
# chsec -f /etc/security/user -s default -a minlen=16
# chsec -f /etc/security/user -s default -a minother=4
# chsec -f /etc/security/user -s default -a minspecialchar=2
# chsec -f /etc/security/user -s default -a mindigit=2
# chsec -f /etc/security/user -s default -a minupperalpha=2
# chsec -f /etc/security/user -s default -a minloweralpha=2
```

Warning: A strong password policy is vital to defending brute force password attacks. Administrators are encouraged to use additional authentication products such as PowerSC MFA to implement multi-factor authentication. Note that PowerSC MFA is not included in the evaluated configuration.

4.7 Service Update Management Assistant (SUMA)

The following steps require an administrative account.

The **suma** command is a tool to download the AIX technology levels and service packs from a fix server.

SUMA can be configured to periodically check the availability of specific new fixes and technology levels. Therefore, system administrators do not have to manually retrieve maintenance updates from the web.

Before you run the **suma** command to download any updates, ensure that the AIX LPAR is authenticated to access the internet. To verify that the LPAR is connected to the internet, enter the following command.

```
# suma -x -a Action=Preview -a RqType=Latest
```

This **suma** command allows you to preview only the download operation. When you run this command, files are not downloaded. If the LPAR is not authenticated to access the internet, the command returns the following message.

```
0500-013 Failed to retrieve list from fix server.
```

In this instance, you must contact your PowerVM/VIOS administrator.

Below are the some usage examples.

1. To download the latest filesets in the default location (DLTargrt=/usr/sys/inst.images)

   ```
   # suma -x -a Action=Download -a RqType=Latest
   ```

2. To download a specific service pack.

   ```
   # suma -x -a Action=Download -a RqType=SP -a RqName=7200-04-02
   -a DLTarget=/home/update_package/
   ```

3. To list the SUMA global configuration settings, type the following.

   ```
   # suma -c
   ```

   Output similar to the following is displayed.

   ```
   FIXSERVER_PROTOCOL=https
   DOWNLOAD_PROTOCOL=http
   DL_TIMEOUT_SEC=180
   DL_RETRY=1
   HTTP_PROXY=
   HTTPS_PROXY=
   USE_FIPS_PROVIDER=yes
   CHECK_CERTIFICATE_REVOCATION=yes
   USE_CC_CIPHERS=yes
   SCREEN_VERBOSE=LVL_INFO
   NOTIFY_VERBOSE=LVL_INFO
   LOGFILE_VERBOSE=LVL_VERBOSE
   MAXLOGSIZE_MB=1
   REMOVE_CONFLICTING_UPDATES=yes
   REMOVE_DUP_BASE_LEVELS=yes
   REMOVE_SUPERSEDE=yes
   TMPDIR=/var/suma/tmp
   WEB_IDENTITY_FILE=
   ```

4. Set DOWNLOAD_PROTOCOL to `https`.

   ```
   # suma -c -a DOWNLOAD_PROTOCOL=https
   ```

5. To list the SUMA task defaults, type the following:

   ```
   # suma -D
   ```

   Output similar to the following is displayed:

   ```
   DisplayName=
   Action=Download
   RqType=Latest
   RqName=
   Repeats=y
   DLTarget=/usr/sys/inst.images
   NotifyEmail=root
   FilterDir=/usr/sys/inst.images
   FilterML=
   MaxDLSize=-1
   Extend=y
   ```

```
MaxFSSize=-1
```

6. To create and schedule a task that downloads the latest fixes monthly (for example, on the 15th of every month at 2:30 a.m.), type the following:

   ```
   # suma -s "30 2 15 * *" -a RqType=Latest -a
   DisplayName="Latest fixes - 15th Monthly"
   ```

   Note: A task ID is returned for this newly created task. This example assumes some of the SUMA task defaults, as displayed in the **suma -D** example, are utilized. For example, when the task default of **DLTarget=/usr/sys/inst.images**, the installp images are downloaded into the **/usr/sys/inst.images/installp/ppc** directory.

7. To create and schedule a task that checks for critical fixes monthly (for example, on the 20th of every month at 4:30 a.m.), type the following:

   ```
   # suma -s "30 4 20 * *" -a RqType=Latest -a RqName= -a
   Repeats=y
   ```

   Note: By setting **Repeats=y**, this task 'repeats forever' and is not deleted after a successful download.

8. To view SUMA scheduling information that has been set up by running a **suma -s CronSched** command, type the following:

   ```
   # crontab -l root
   ```

9. To list all SUMA tasks, type the following:

   ```
   # suma -l
   ```

10. To unschedule a task that removes its scheduling information from the crontab file in the **/var/spool/cron/crontabs** directory, type the following:

    ```
    # suma -u <task id>
    ```

11. To delete a task that also removes its scheduling information if it exists, type the following:

    ```
    # suma -d <task id>
    ```

For trusted update, one must install bos.dsc first, then bos.rte.install before anything else.

For bos.dsc, find the PTFs for bos.dsc and copy them to a separate directory. Assume the updates are downloaded to the default location:

```
# cd /usr/sys/inst.images/installp/ppc
# grep bos.dsc .toc

U889851.bff 4 R I bos.dsc {
bos.dsc 07.02.0005.0100 1 N U en_US Digital Signature Catalog
*prereq bos.dsc 7.2.5.100
U889517.bff 4 R S bos.dsc {
bos.dsc 07.02.0005.0103 1 N U en_US Digital Signature Catalog
*prereq bos.dsc 7.2.5.100
```

Copy the two *.bff to a separate location, e.g., /tmp/dsc_update

```
# cp U889851.bff /tmp/dsc_update
# cp U889517.bff /tmp/dsc_udpate
```

Install bos.dsc

```
# cd /tmp/dsc_update
# inutoc .
# installp -agXd /tmp/dsc_udpate bos.dsc
```

Install bos.rte.install

```
# installp -agXd /usr/sys/inst.images/installp/ppc bos.rte.install
```

Check the trusted update key database is intact

```
# ODMDIR=/usr/lib/objrepos odmget dsc_key
```

If the result is empty, restore the trusted key ODM database from the tar file saved in Section 2.3 (Initialization of Trusted Update Keystore).

4.8 Management of Security Patches

The following security patch utilities are provided for checking and downloading the available security patches and applying them to the system.

When installing any ifix in the evaluated configuration, the administrator is required to use the ifix commands defined in this section. The installation instructions included within the ifix should only be followed if they use the ifix commands in this section to install the ifix.

emgr_check_ifixes—Checks for available security ifixes for the current system level and downloads them in batch mode, if preferred. This command connects over HTTPS using the **openssl s_client** command to check for updates and to validate the authenticity of the response.

```
Usage: /usr/sbin/emgr_check_ifixes [-D] [-P path]
        -D [download all fixes]
        -P [Specifies the path to download the ifix, the default path is
           /tmp/ifix_$PID]
           This is optional flag and to be use along with -D flag only
Error messages:
   ERROR: SSL connection failed, logs saved in  $ssl_connectfile
   ERROR: failed to retrieve server certificate. Check errors in $server_cert_pem
   ERROR: failed to retrieve CRL URI from $server_cert_pem
   ERROR: failed to download CRL from $crl_hostname. Check errors in $crl_der
   ERROR: Server certificate validation failed: CRL Distribution Points extension
      is not found in $server_cert_pem
   ERROR: failed to verify server certificate
```

emgr_download_ifix—Downloads individual security patches.

```
Usage: /usr/sbin/emgr_download_ifix [-L [download Link]] [-P path]

        -L [http link for ifix download]
        -P [Specifies the path to download the ifix, the default path is
           /tmp/ifix_$PID.]
           This is optional flag and to be use along with -L flag only]
Error messages:
   SSL connection failed, logs saved in  $ssl_connectfile
   SSL Error: failed to retrieve server certificate. Check errors in
      $server_cert_pem
```

```
SSL Error: failed to retrieve CRL URI from $server_cert_pem
SSL Error: failed to download CRL from $crl_hostname. Check errors in $crl_der
ERROR Server certificate validation failed: CRL Distribution Points extension
   is not found in $server_cert_pem
ERROR Server certificate CRL verification failed
```

emgr_sec_patch—Installs individual security ifixes archived in tar format. It unpacks the tar file, identifies the ifix for the current system level, invokes digital signature validation, and installs the ifix if the signature validation is successful. It uses the **emgr_sec** command to perform the signature validation.

```
Usage: /usr/sbin/emgr_sec_patch ifix_tar_file
Error messages:
   TAR file $2 does not exist.\nPlease download $2 and try to install again
   Tar command failure
   ERROR: verifification of tar content failed
   ERROR: $FILE is not found in tar
   ERROR: $FILE.sig is not found in tar
   ERROR: Advisory.asc verification failed
   ERROR: $IFIX_NAME hash doesn't match that in Advisory.asc
   ERROR: Signature file $2 does not exist.\nPlease download ifix and try again\m
   ERROR: Signature verification failed on $2\n$2 not installed ...\n
   ERROR: Certificate file $2 does not exist.\nPlease ensure that $2 is
       installed\n
   ERROR: Installation failed, Please check the emgr display.\n
```

emgr_sec—Performs digital signature validation of an ifix and installs the ifix if the signature validation is successful. It uses the **openssl** command for signature validation.

```
Usage: /usr/sbin/emgr_sec ifix_name.Z
Error messages:
   ERROR: Signature file $2 does not exist.\nPlease download ifix and try again\m
   ERROR: Signature verification failed on $2\n$2 not installed ...\n
   ERROR: Certificate file $2 does not exist.\nPlease ensure that $2 is
       installed\n
   ERROR: Installation failed, Please check the emgr display.\n
```

The reference identifier used by the above commands is pre-defined and fixed by default. It is not intended to be modified.

For download and apply security fixes, make sure there is enough space in the download file system. If the security patches contain java update, recommend the file system hosting the security patches has at least 2GB free space. Using the following command to increase the filesystem size, replacing the file_system_name with the actual name.

```
chfs -a size=+2G file_system_name
```

4.9 Firewall Configuration

The following steps require an administrative account.

An administrator can configure a TCP/IP filter (i.e., firewall) using the following commands.

chfilt—Changes existing filter rules
genfilt—Adds a filter rule to the table; Also use to create new filters
lsfilt—Lists filter rules present in the table
mkfilt—Activate or deactivate the filter rules in the table, enable or disable logging for filters, and change the default rules
rmfilt—Removes existing filter rules

For more information on these commands, please see AIX Intrusion Prevention in AIX Version 7.2 Security.

4.10 Key Destruction

When stored in persistent storage, all private keys and symmetric keys are stored encrypted in keystores with the exception of the SSH server's private key. When the keystores are no longer needed, they must be manually zeroized and deleted from persistent storage using the script below.

```
#! /bin/ksh
# Overwrite the file with 0
# Usage:
# zerofile $filename

if [ $# != 1 ];
then
    echo "Usage: $0 filename"
    exit -1;
fi

filename=$1

if [ ! -f "$filename" ];
then
    echo File $filename does not exist
    exit -1 ;

fi

size=`ls -l "$filename" | awk '{print $5}' `
if [ $size !=  0 ]; then
    echo "dd if=/dev/zero of=$filename bs=$size count=1"
    dd if=/dev/zero of="$filename" bs=$size count=1
fi
```

The following keystores must be zeroized once they have been deemed no longer necessary.

- EFS keystores located under the **/var/efs/** directory. (Requires an administrative account.)
- SSH client keystores used for user public key authentication. (Users can zeroize their own SSH keystores or an administrator can zeroize any SSH keystore.)
- SSH server keystore used for server keys. (Requires an administrative account.)

EFS keystores typically remain on the system even after the user or group accounts are deleted in order to prevent loss of data (i.e., in case there are files remaining on the system that only those keys can decrypt). An administrator needs to determine when the appropriate

time is to delete a deleted user's EFS keystore and use the above script to zeroize the keystore.

SSH client keystores can be deleted by the user once the user no longer needs it. In this case, the user must use the above script to zeroize their own keystore.

SSH client keystores are typically no longer necessary once the user account is no longer necessary, but the keystores will remain on the system until they are deleted. An administrator needs to determine when the appropriate time is to delete a deleted user's SSH keystore and use the above script to zeroize the keystore.

Warning: For storage classes such as Flash devices, which implement wear levelling technology, zeroing out the file content may not guarantee the sensitive key materials are wiped clean from the device completely. When disposing such device, administrators are encouraged to overwrite the entire device multiple times or physically destroy the device if suitable.

The following software requires the system to be powered off to destroy keys in volatile memory.

- If EFS is enabled, the console login, SSH server, **efsenable**, **efskeymgr**, **mkuser**, **mkgroup**, and **passwd** commands and the kernel
- **suma, openssl, sshd, ssh, emgr_check_ifixes,** and **emgr_download_ifix** commands

5 References

- IBM AIX 7.2 Technology Level 5 Service Pack 3 Standard Edition Operating System Security Target
- AIX Version 7.2 Security
- AIX Version 7.2 File Reference
- AIX Version 7.2 Commands
- AIX Version 7.2 Base Operating System (BOS) Runtime Services

  https://aix.software.ibm.com/aix/efixes/cc/aix72_ref.tar
  SHA256(aix72_ref.tar)=5a55b80a6e9c356eb939a9a01b95d1263c6cb3b3e836923a22d299517b3098a3