Common Criteria Installation Instructions for IBM Logical Partitioning Architecture on System i and System p

1 About This Information

This information will tell you how to plan, install, set up and manage the logical partitioning of your System p and System i, based on the IBM Logical Partitioning Architecture on System i and System p for Power6 Common Criteria evaluation.

You can find related information at the following URLs:

- http://csrc.nist.gov/cc/index.html (Common Criteria information)
- http://www.niap-ccevs.org (IBM Logical Partitioning Architecture on System i and System p for Power6)

The IBM Logical Partitioning Architecture on System i and System p is designed to meet the Common Criteria requirements listed in the IBM Logical Partition Architecture for Power6 Security Target. The hardware and firmware allow you to set up more than one virtual platform on your System i or System p, so that you can run separate operating systems concurrently. Each virtual platform is called a *partition*. The design of the architecture provides the following security features:

- The hardware and firmware provide the operating system on each separate partition with the resources it needs to function
- The hardware and firmware keep the resources for each partition separate, so that they will not interfere with each other.

The IBM Logical Partitioning Architecture on System i and System p has been developed and evaluated in accordance with the Common Criteria EAL4 (Evaluation Assurance Level) assurance requirements listed below:

Objectives

- EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.
- EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity targets of evaluation (TOE) and are prepared to incur additional security specific engineering costs.

Assurance components

- EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behavior. Assurance is additionally gained through an informal model of the TOE security policy. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

- EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.
- This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, a subset of the implementation, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development or delivery.

Common Criteria security requires the following documentation:

- *Administrator Guidance*, which describes the tasks that a security administrator must perform to install and manage a Common Criteria-evaluated system.
- *User Guidance*, which describes the user's responsibilities for security. In this case, once a System i or System p has been configured to run with multiple partitions, the user of the partition does not need to do anything to support security. All the security features are enforced by the firmware and hardware.

This information is designed to meet the Common Criteria requirement for administrator guidance, when used together with the following documents:

- *SA76-0098-00 Logical partitioning guide*
- *SA76-0084-00 Installation and Configuration Guide for the Hardware Management Console Version 7 Release 3.1.0 Maintenance Level 0*
- *SA76-0085-00 Operations Guide for the Hardware Management Console and Managed Systems Version 7 Release 3.1.0*

You can find these documents in the IBM support center through the IBM support website, under Support for IBM Systems (*http:/www.ibm.com/systems/support*):

1. Select "System p" or "System i"
2. Under "Select your product," press the GO button.
3. Under "Documentation," choose "IBM system hardware information library."

You should read this guide first, and you should consider it your primary source of information for setting up logical partitioning of your system p or system i to meet the Common Criteria security requirements that are listed in the IBM Logical Partition Architecture for Power6 Security Target.

2 Who should read this information

This information is intended for system administrators or security administrators that want to customize a system i or system p with Logical Partitioning within the valid Common Criteria configuration. This information details the unique requirements of Common Criteria security, and it is intended as a supplement to other manuals describing how you install and set up your system.

3 Overview of security features

There are three categories of security features provided by the IBM Logical Partition Architecture implementation for Power6:

1. The Logical Partitioning Architecture implementation ensures that resources can be assigned to partitions by an authorized user and that those resources will not be accessible to other partitions.

2. The Logical Partitioning Architecture implementation ensures that communication between partitions can occur only using channels established by an authorized user.

3. The Logical Partitioning Architecture implementation ensures that each partition cannot access resources or communicate with other partitions except when explicitly allowed by an authorized user.

In addition, the following assumptions are made about the operating environment when the system is in operation:

1. A suitable management console must be configured for use by a capable and trustworthy user assigned to follow the applicable guidance in order to install and operate the system within the evaluated configuration.

2. The system must be installed and configured in accordance with its guidance documents, including connecting appropriate device resources and disconnecting the management console when the system is operational.

3. The system must be within a physical environment suitable to protect itself and its external connections from inappropriate access and modification.

4 Target of Evaluation (TOE)

The Logical Partitioning Architecture Target of Evaluation (TOE) is the combination of hardware and software that provides security protection within a computer system. The TOE includes both System i and System p as described below:

- System i:
  - Any IBM System i listed in the System I model table below
  - Firmware level EM310_048.
- System p:
  - Any IBM System p, listed in the System p model table below
  - Firmware level EM310_048.

System i and System p servers can be configured to house multiple independent systems within the same server. Each independent system within the server is called a partition. The partitions do not have to run the same type of operating system. During the configuration process, an administrator determines what resources within the System i or System p will be assigned to each independent partition. There are many partition features. The following Logical Partitioning Architecture features are allowed in the evaluated configuration:

- Micro-partitioning: This feature allows a processor to be shared between two partitions. One partition may get 10% while another gets 90%.

- LPAR Grouping: This feature allows partitions to state, at configuration time; they are part of a group. Within a partition group, each partition's administrator can request or release memory or CPU. The act of getting or releasing resources is done explicitly by the partitions administrator. It is not done dynamically by any partition in the group. If an administrator requests more resources than are currently free, the request will fail.

  NOTE: Enterprise Work Load Manager and Partition Load Manager for AIX use interfaces that are within the evaluated configuration. Therefore these products can be used.

- The Logical Partitioning Architecture was evaluated independent of the OS in the partition. Any operating system may be installed in the partition.

Products that are included in the TOE have been evaluated and tested for Common Criteria security compliance. Products that are not included in the TOE have not been evaluated for Common Criteria security compliance. Because the TOE is a general building block, many installations require changes or additions to the evaluated configuration. For U.S. Government installations, any changes or additions to the TOE should be approved by your Designated Approving Authority (DAA). For other installations, your security administrator should assess the security risk of any changes or additions to the TOE configuration.

4.1 System i and System p evaluated models

System	Model Name
System i	9406-MMA
System p	9117-MMA

4.2 Physical System i and System p security

To be within the evaluated configuration, the system must be in a secured room with limited and monitored access. The systems HMC appliance must also be in the same secured area.

4.3 System i and System p HMC installation

A common criteria compliant system must be configured by an HMC. It doesn't matter if the HMC is directly connected to the system or connected to the system through a network. The HMC is used to partition the system. Once the partitioning has been completed, the HMC must be physically disconnected from the managed system.

The guidance for connecting an HMC to a system can be found in the Hardware Management Console Version 7 Release 3.1.0 Maintenance Level 0 document.

4.4 System i and System p firmware installation

The evaluated firmware level is 01EM310-048. Verify this level of firmware is on your machine. To check the level of firmware on your system, follow the instructions in chapter 9 of the Operations Guide for the Hardware Management Console and Managed Systems Version 7 Release 3.1.0 document. The first section of chapter 9 describes all of the tasks that can be performed from through the "updates" function. Use the "view system information" task to determine the level of firmware on your system.

If the firmware level does not match the evaluated firmware level, you must install the evaluated firmware on your machine. The evaluated firmware is in the 01EM310_048_048.iso fix pack. This can be obtained from either of these sources:

- System i customers order the 01EM310_048_048.iso fix pack through the "iSeries Recommended Fixes - Server Firmware: Update Policy Set to HMC" web page at http://www-912.ibm.com/s_dir/slkbase.nsf/ibmscdirect/E58D7BBF0EAC9A2786256EAD005F54D8.

- System p customers order the 01EM310_048_048.iso fix pack through the "Microcode update files on CD-ROM" web page at http://www14.software.ibm.com/webapp/set2/firmware/gjsn?mode=10&page=isoiec.html

If you need to install the evaluated firmware on your machine, follow the instruction in Chapter 9 of the Operations Guide for the Hardware Management Console and Managed Systems Version 7 Release 3.1.0 document. The first section of chapter 9 describes all of the tasks that can be performed from through the "updates" function. Use the "change licensed internal code for the current release" task to install the evaluated firmware. Prior to the installation, you should power down all the partitions and the system. When the installation is complete, activate the system and all the partitions.

4.5 Partition the System i or System p:

SA76-0098-00 the Logical Partitioning Guide contains all of the information necessary to configure your machine. The administrator should read chapters 1 and 2 to become familiar with the partitioning concepts.

There are no special instructions for partitioning the System i or System p. However, some features are not allowed in the evaluated configuration. The following features are excluded from the evaluated configuration:

- Virtual I/O (Virtual Ethernet and Virtual SCSI devices)
  - The Logical Partitioning Guide only provides the virtual I/O concepts. You cannot configure virtual I/O. Do *not* use the configuration steps in chapter 2 of the SA76-0100-00 Advanced POWER Virtualization Operations Guide. To check that a partition is not using Virtual Ethernet and Virtual SCSI, do the following:
    - From the HMC, select Configuration-> Manage Profiles for a partition.
    - Select the partition's profile check box.
    - Select the Actions -> Edit.
    - Select the Virtual Adapters tab.
    - There should only be Server Serial type adapters in the list.
    - If there are any other types of virtual adapters, they must be removed.
    - To remove a virtual adapter,
      - Select the virtual adapter.
      - Select Actions -> Delete.

  Note: If any virtual adapters were removed, the partition must be rebooted.
- Infiniband I/O devices
  - You must not install any 12X Channel CEC GX Adapters (feature code 1802).
- HMC capability
  - You must unplug the HMC from the system when configuration is complete.
- I/O Pools
  - You must not create a storage pool, and you must remove any storage pools that exist. To check if you have any storage pools, do the following:
    - From the HMC, select properties for a partition.
    - Follow the tabs hardware -> I/O.
    - Press the I/O Pools button
    - If any storage pools exist, you must remove them. Also, you must not add storage pools from this screen at any time.

    Note: If any storage pools were removed, the partition must be rebooted.
- OptiConnect (virtual and HSL)
  - You must not configure your partition to use OptiConnect. To check that a partition is not using OptiConnect, do the following:

    - From the HMC, select Configuration-> Manage Profiles for a partition.
    - Select the partition's profile check box.
    - Select the Actions -> Edit.
    - Select the OptiConnect tab.
    - If any of the check boxes are selected, the partition is using OptiConnect.
    - You must uncheck any selected check boxes and Press OK.

  Note: If any boxes were unchecked, the partition must be rebooted.
- Power Controlling
  - You must not allow any partition to have a power controlling partition, and you must remove any power controlling partitions if they exist. To check that a partition does not have a power controlling partition, do the following:
    - From the HMC, select Configuration-> Manage Profiles for a partition.
    - Select the partition's profile check box.
    - Select the Actions -> Edit.
    - Select the Power Controlling tab.
    - If there are any partitions in the power controlling partitions list, select them and press the remove button.

  Note: If any controlling partitions were removed, the partition must be rebooted.

To partition your system follow the instructions in chapter 4, section "partitioning a new or non-partitioned managed system using the HMC" in the Logical Partitioning Guide.

4.6 Final configuration step

After the system has been configured and put into normal operation, the HMC appliance's ethernet connection must be disconnected from the system.

NOTE: The selection and installation of the individual operating systems for the partitions is outside the scope of this evaluation. The evaluated hardware and firmware are indifferent to the OS of the partition.