



Implementing PLM

PLM Software Installation

- Install the following filesets:
 - plm.license
 - plm.server.rte
 - plm.sysmgt.websm

- Make sure SSL and OpenSSH are also installed

- For setup of PLM, create .rhosts files on the server and all clients. After PLM has been set up, you can delete the .rhosts files.

Create SSH Keys

- On the server, enter:
`# ssh-keygen -t rsa`
- Copy the HMC's secure keys to the server:
`# scp hscroot@hmchoostname:~/.ssh/authorized_keys2 \`
`~/tmp_authorized_keys2`
- Append the server's keys to the temporary key file and copy it back to the HMC:
`# cat ~/.ssh/id_rsa.pub >> ~/tmp_authorized_keys2`
`# scp ~/tmp_authorized_keys2 \`
`hscroot@hmchoostname:~/.ssh/authorized_keys2`

Test SSH and Enable WebSM

- Test SSH to the HMC. You should not be asked for a password.
`# ssh hscroot@hmchostname lssyscfg -r sys`
- On the PLM server, make sure you can run WebSM. Run:
`# /usr/websm/bin/wsmserver -enable`

Configure PLM Software

- On the PLM server, open WebSM and select Partition Load Manager.
- Click on Create a Policy File. In the window open on the General Tab, enter a policy file name on the first line
- Click on the Globals tab. Enter the fully qualified hostname of your HMC. Enter hscroot (or a user with the Systems Administration role) as the HMC user name. Enter the CEC name, which is the managed system name (not the fully qualified hostname).

Configure PLM Software

- Click on the Groups tab. Click the Add button. Type in a group name. Enter the maximum CPU and memory values that you are allowed to use for PLM operations.
- Check both CPU and Memory management if you're going to manage both.
- Click on Tunables. These are the defaults for the entire group. If you don't understand a value, highlight it and select Help for a detailed description.

Configure PLM Software

- Click on the Partitions tab. Click the Add button and add all of the running partitions in the group to the partitions list.
 - On the Partition Definition tab, use the partitions' fully qualified hostnames and add them to the group you just created.
- Click OK to create the policy file.
- In the PLM server, view the policy file you created. It will be in `/etc/plm/policies`.
- Perform the PLM setup step using WebSM. You must be root. Once this finishes, you'll see "Finished: Success" in the WebSM working window.

Configure PLM Software

- In the server and a client partition, look at the `/var/ct/cfg/ctrmc.acls` file to see if these lines are at the bottom of the file:

```
IBM.LPAR
```

```
root@hmchostname          *          rw
```

If you need to edit this file, run this command afterward:

```
# refresh -s ctrmc
```


Configure PLM Software

- Test RMC authentication by running this command from the PLM server, where *remote_host* is a PLM client

```
# CT_CONTACT=remote_host    lsrsrc    IBM.LPAR
```

If successful, a lot of LPAR information will be printed out instead of “Could not authenticate user”

- Start the PLM server. Look for “Finished:Success” in the WebSM working window.

Enter a configuration name. Enter your policy file name. Enter a new logfile name.

(If you have trouble with the logfile, you may need to touch the file before you can access it)

Configure PLM Software

- If the LPAR details window shows only zeroed-out information, then there's probably an RMC authentication problem.
- If there's a problem, on the server partition, run:

```
# /usr/sbin/rsct/bin/ctsvhbal
```

The output should list one or more identities. Check to see that the server's fully qualified hostname is in the output.
- On each partition, run `/usr/sbin/rsct/bin/ctsth1 -l`. At least one of the identities shown on the remote partition's `ctsvhbal` output should show up on the other partitions' `ctsth1 -l` output. This is the RMC list of trusted hosts.

Configure PLM Software

- If there are any entries in the RMC trusted hosts lists which are not fully qualified hostnames, remove them with the following command:

```
# /usr/sbin/rsct/bin/ctsth1 -d -n identity
```

where *identity* is the trusted host list identity

- If one partition is missing a hostname, add it as follows:

```
# /usr/sbin/rsct/bin/ctsth1 -l -n identity -m METHOD -p ID_VALUE
```

Identity is the fully qualified hostname of the other partition

rsa512 is the method

Id_value is obtained by running *ctsth1 -l* on the other partition to determine its own identifier