HP bh5700 ATCA 14-Slot Blade Server

READ ME FIRST

This document provides General Tips and Suggestions, and Known Issues for the HP bh5700 ATCA 14-Slot Blade Server.

General Tips and Suggestions

This section provides general Tips and Suggestions when using your HP bh5700 ATCA 14-Slot Blade Server.

Installing Blades in the Chassis

IMPORTANT The HP bc2100 ATCA Server Blades cannot take advantage of the Update Channel setup on the backplane of the chassis.

Before installing blades into your HP bh5700 ATCA 14-Slot Blade Server, read and follow these recommended blade configuration instructions:

- The two Ethernet Switch Blades must be loaded in the middle of the payload bay in Slots 7 and 8.
- To take advantage of the Update Channel setup on the backplane of the shelf chassis and to distribute the electrical load across the four power domains, blades other than the Ethernet Switch Blades should be installed using the following chassis slot sequence:

  1–2, 12–14, 3–5, 11–13, 4–6, 9–10

TELNET Client Use

IMPORTANT Hewlett-Packard strongly recommends that you do NOT use Windows TELNET sessions for configuring the BIOS, but that you use Linux Terminal sessions instead.

Use a TELNET client that supports VT100 and ANSI for serial terminal connection. The HP bc2100 ATCA Server Blade BIOS menu performs best when using ANSI.

Ethernet Port Mappings

NOTE If you are using a non-HP certified or supplied version of Linux based on 2.4.x, there will be a different Ethernet port mapping for the HP bc2100 ATCA Server Blades.

With two Ethernet Switch Blades installed in the card cage in hub Slot 7 (the left Switch Blade) and hub Slot 8 (the right Switch Blade), the Ethernet port mappings to the HP bc2100 ATCA Server Blades are based on the Linux kernel 2.6.x, as follows:

- Even-numbered Ethernet ports on the HP bc2100 ATCA Server Blade will always be linked to the Switch Blade installed in hub Slot 7 (on the left-side of card cage center).
- Odd-numbered Ethernet ports on the HP bc2100 ATCA Server Blade will always be linked to the Switch Blade installed in hub Slot 8 (on the right-side of blade cage center).

Booting a Fail-Safe Image on the Ethernet Switch Blade

CAUTION Possible loss of configuration changes. After you have made configuration changes to an Ethernet Switch Blade, you must first issue the `zsync` command when logged into that Switch Blade in order to save your changes or they will be lost at the next reboot.

Issuing this command will save your configuration changes ONLY for the Ethernet Switch Blade base switch portion or fabric switch portion on which you issue the `zsync` command. Issuing this command will take a few seconds.

IMPORTANT Factory default configuration settings are only temporary unless you issue a `zsync` command after restoring those settings. Note that any configuration settings saved with `zsync` are saved only until you change the settings again and issue another `zsync` command.

To boot into a fail-safe image on the Ethernet Switch Blade, you must first enter the `reboot -i` command and then the `zsync` command to overwrite your existing image with the fail-safe image. To do this, complete the following:

1. Log into either the base or fabric switch portion of the desired Ethernet Switch Blade, using the procedure “How to Log into an Ethernet Switch Blade in Hub Slots 7 or 8”, on page 3.

   There is one base switch and one fabric switch for the Ethernet Switch Blade in hub Slot 7, and one base switch and one fabric switch for the Ethernet Switch Blade in hub Slot 8, for a total of four switches. If you have made changes on more than one switch within either of the Switch Blades, you must log into and issue the `zsync` command on each switch you have made changes to in order to save those changes. For example, if you have made changes to both base switches and both fabric switches, you must log into each and issue the `zsync` command on each switch individually.

2. If you need to reinitialize a switch configuration to the factory defaults, you can issue the following command:

   ```
   reboot -i
   ```

   This command will immediately reboot the switch. Following the `reboot -i` command, the switch will have been returned to the factory default settings (including baud rate). Remember to then issue the `zsync` command if you want the default settings to remain in force following the next reboot.

How to Log into an Ethernet Switch Blade in Hub Slots 7 or 8

IMPORTANT If you do not see the `OpenArchitect login: prompt` or `Password:` prompt when completing Step 3 of this procedure, first check the serial cables, the connectors, and the settings of your serial terminal program, then repeat the login procedure from Step 1.

NOTE The default configuration for both serial ports on the Ethernet Switch Blade is; 9600 baud, 8 bits, no parity, 1 stop bit, no hardware or software flow control.

Each Ethernet Switch Blade (Hub Slots 7 and 8) has a separate internal base switch portion and a separate fabric switch portion. Individually, these portions are referred to simply as a "switch." You must log into and configure each of these internal switches through their dedicated RJ-45 connector serial ports (one for the base switch and one for the fabric switch), located on the face plate of each Ethernet Switch Blade.

The base switch port is the upper-most RJ-45 connector on the Ethernet Switch Blade face plate. The fabric switch port is the sixth RJ-45 connector up from the bottom on the Ethernet Switch Blade face plate.

To log into either the base portion or the fabric portion of an Ethernet Switch Blade, complete the following steps:

1. Use the RJ-45/DB-9 adapter cable (part number A6900-63006 that was shipped with your HP bh5700 ATCA 14-Slot Blade Server system) with a modem eliminator cable (DB-9/DB-9) to connect your local terminal or PC to the desired Ethernet Switch Blade switch port (base or fabric).
2. Ensure that your serial terminal program is set to the default configuration for the Ethernet Switch Blade serial ports (9600 baud, 8 bits, no parity, 1 stop bit).
3. Press the **Enter** key repeatedly until you see the following prompt:

   ```
   OpenArchitect login:
   ```

   If you see the prompt `Password:`, press **Enter** one more time to get the `OpenArchitect login:` prompt.
4. At the `OpenArchitect login:` prompt, enter the default username of `root`.
5. At the `Password:` prompt, press only the **Enter** key. The default password is a blank (no character) entry.
6. After you have successfully logged in, you will see a prompt similar to the following, which will allow you to issue commands:

   ```
   [ZX7100-OA3.2.2j]#
   ```

How to Log Into a Shelf Management Module (ShMM)

IMPORTANT Always issue ShMM commands from the Active ShMM. Many commands will return an error when issued on the backup ShMM. If the `clia shmstatus` command returns `Host: "Backup"`, this indicates that you are logged into the Backup ShMM. Move the console cable to the other ShMM RJ-45 connector on the Alarm Display Panel and log into the Active ShMM.

NOTE By default, there is no password prompt for the ShMM unless you set a personal password.

There are two ShMM mounting slots located on the front lower-left and the lower-right face plate of the chassis. Typical chassis configuration will include a ShMM in each of these slots.

To log into a ShMM (to issue chassis and ShMM commands, and to configure the chassis), you must first connect a serial terminal to the desired ShMM serial interface port. Serial interface ports for both ShMMs are provided by the two RJ-45 connectors located on the Alarm Display Panel face plate. The Alarm Display Panel is mounted on the upper-left-front of the chassis face plate. These ports are labeled as **ShMgr-Left** and **ShMgr-Right**, and provide a serial connection to the lower-left and the lower-right ShMM, respectively.

To log into a ShMM, complete the following:

Step 1. Use the RJ-45/DB-9 adapter cable (part number A6900-63006 that was shipped with your HP bh5700 ATCA 14-Slot Blade Server system) with a modem eliminator cable (DB-9/DB-9), to connect your local terminal or PC to the desired ShMM.

Step 2. Ensure that your serial terminal program is set for the ShMM serial port default configuration of 9600 baud, 8 bits, no parity, 1 stop, no flow control.

Step 3. Following the kernel boot process for the ShMM, the following login prompt should appear:

```
sentry login:
```

By default, there is no password prompt for the ShMM. However, if the `sentry login:` prompt is passed over and you see the prompt `Password:`, press **Enter** to regain the `sentry login:` prompt and proceed to the next step

Step 4. At the prompt `sentry login:`, enter the default username of `root`.

Step 5. After login as root, you will see the following command prompt:

```
#
```

Step 6. Your chassis should have two ShMMs; one will be the “active” and the other will be the “backup.” Most commands you will use must be issued on the active ShMM. You can determine which ShMM you are logged into by entering the following command at the command prompt (`#`):

```
clia shmstatus
```

This command will return either `Host: "Active"` or `Host: "Backup"`.

Known Issues

This section provides information on issues known to exist at the time of shipment of the HP bh5700 ATCA 14-Slot Blade Server.

Shelf Management Module (ShMM) Issues

1. **Issue:** The procedure for "Reinitializing the U-Boot Environment" may render the ShMM permanently inoperable on systems running ShMM firmware Version 2.2.1.

   Symptom: The ShMM boot process will halt upon reaching the U-Boot prompt, and will not continue.

   Probable Cause: A firmware bug.

   Resolution: Update the system firmware to recipe BH57004639 or later. This firmware update includes new ShMM firmware version 2.2.3 and will allow the "Reinitializing the U-Boot Environment" procedure to operate correctly.

2. **Issue**: USB1 interface is not listed in the configuration table after hot swap or switchover.

   Symptom: Enter `ifconfig` command at Linux prompt – The USB1 interface is not listed.

   Probable Cause: The ShMM-1 & ShMM-2 channels are crossed to allow switchover.

   Resolution: This is functioning as designed, and occurs on the active ShMM. Since the active ShMM controls the ShMM interconnect link and uses USB0 for this, it does not configure or enable USB1, and does not show up in the configuration table for the active ShMM. It is present in the configuration table for the backup ShMM as it is the active link for USB1 in this case.

3. **Issue:** Inconsistent information from the Backup ShMM.

   Symptom: The Backup ShMM will display incorrect FRU information.

   Probable Cause: A firmware bug.

   Resolution: It is recommended that all `clia` commands are executed only from the Active ShMM. The active ShMM can be determined by issuing a `clia shmstatus` command. If the response is "`Active`", then you can proceed.

4. **Issue:** ShMM does not retain user-set password.

   Symptom: Default ShMM password is persistent. User-set password not functioning.

   Probable Cause: A software bug.

   Resolution:

   a. Short term - complete the following procedure:

      1. Log into the ShMM as `root`.
      2. At the command prompt, enter the command string `passwd root`.
      3. You will then be asked to enter your password. (Note that your user password will be truncated to eight characters if you enter more than eight.)
      4. Open the password file `/etc/passwd` and find the text string, "`root::0:0:...`".

5. Enter an "x" in the text string following `root:`, and before the next colon, so that the string now appears as, "`root:x:0:0:...`" Save your changes to the file.
6. Your personal password will now be required for you to log into the ShMM beginning with the next boot.

b. Long term - Software update.

HP bc2100 ATCA Server Blade Issues

1. **Issue:** BIOS Boot Order changes are not retained when made at the same time as making changes to BIOS Boot Device settings.

   Symptom: BIOS does not retain Boot Order changes when made at the same time as making Boot Device setting changes.

   Probable Cause: BIOS firmware bug.

   Resolution:

   a. Short term - use a two-step process to make the BIOS modifications:

      1. Make any device related changes (enable/disable SAS, IDE, PXE, etc.), save the settings, then reboot.
      2. Make Boot Order changes, save the settings, then reboot.

   b. Long term - BIOS firmware update.

2. **Issue:** KCS interface errors are displayed during the IPMC firmware update using the ServiceOS.

   Symptom: KCS interface errors "`ipmi_kcs_sm:`" and "`kcs hosed:`" are displayed.

   Cause: Linux IPMI driver and IPMC firmware update tool contend for access to the IPMC during the IPMC update process. The firmware update tool then puts the IPMC in upgrade mode so the KCS driver cannot receive poll responses from the IPMC.

   Resolution: None - do not use the KCS driver during the firmware update process.

14-Slot Shelf Chassis

1. **Issue:** Chassis fan speed oscillates periodically at room temperature (approximately 20 degrees C / 68 degrees F).

   Symptom: A user will notice that the fan speed changes frequently as the thermal conditions inside the chassis change.

   Probable Cause: Heavy use of the Processor Blade in conjunction with the fan firmware algorithm.

   Resolution: Pending firmware updates of the ShMM and/or Processor Blade.

Diagnostic Boot Times Out - System Boots Normally

1. **Issue:** Due to changes in BIOS version TP752HRA.86H.0006.P.0609201503 you must disable the automatic boot timeout before requesting diagnostic boot.

   Symptom: After setting the one-time forced diagnostic boot request, the blade boots using its regular boot sequence instead of the diagnostic boot sequence.

   Probable Cause: It is taking more that 60 seconds to read the boot flags and start the boot. The IPMC has marked the flags as no longer valid and the blade boots using its regular boot sequence.

   Resolution:

   To avoid the automatic timeout which will disable the diagnostic boot request you must use an IPMI command generation utility such as ipmitool to disable the timeout. Using the command as described will disable the boot timeout until it is reset.

   The IPMI commands are described in the IPMI 1.5 Specification in the section on "Remote Access Boot Control" ("Set System Boot Options" command). Table 1 provides a summary of the command bytes to disable the 60-second timeout.

Table 1 ipmitool Command Bytes to Disable 60-second Timeout

Action	Net Function	Cmd Code	Request Data
Set System Boot Options	Chassis (00h)	08h	• Byte 1 = 0x3 - Parameter selector as "BMC boot flags valid bit clearing" • Byte 2 [7:4] = 0000b [3] = 1b - Do not automatically clear boot flag valid bit if Chassis Control command is not received within 60-second timeout [2:0] = 000b

The ipmitool command is used to send IPMI commands either locally (if `ipmitool` is running on the Server Blade's Linux OS) or from IPMI-over-LAN, if the command runs from a remote system manager.

For more information on `ipmitool` see:

http://ipmitool.sourceforge.net

Example 1 Send a local raw data request to disable the automatic 60-second timeout

```
# ipmitool raw 0x00 0x08 0x03 0x08
```

Where:

Data byte 2 = 0x08 Do not automatically clear boot flag valid bit if Chassis Control command is not received within 60-second timeout.

Example 2 Send an IPMI-over-LAN request to disable the automatic 60-second timeout for the blade in slot 4

```
# ipmitool  -I lan -H  192.168.1.2 -U root -P rootpass -t 0x8e raw 0x00 0x08 0x03 0x08
```

Where:

-I lan	Specifies the LAN interface used by `ipmitool`.
-H 192.168.1.2	The IP address of the ShMM through which the RMCP session is established. A hostname can also be specified instead of an IP address, if applicable.
-U root -P rootpass	The user login information (root/rootpass) for the ShMM RMCP session.
-t 0x8e	The target IPMB address for the bridged request. 0x8e is the address for the physical slot 4.

The disabled timeout setting will remain in effect until a cold reset or loss of power to the blade occurs.