![Sun Microsystems logo]

Sun Fire™ B10n Content Load Balancing Blade Version 1.3 Product Notes

Please
Recycle

Adobe PostScript

Contents

Declaration of Conformity

Compliance Model Number: BP-4
Product Family Name: Sun Fire B10n blade

EMC

USA—FCC Class A

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This equipment may not cause harmful interference.
2. This equipment must accept any interference that may cause undesired operation.

European Union

This equipment complies with the following requirements of the EMC Directive 89/336/EEC:

As Telecommunication Network Equipment (TNE) in Both Telecom Centers and Other Than Telecom Centers per (as applicable):
EN300-386 V.1.3.1 (09-2001) Required Limits:

EN55022/CISPR22	Class A
EN61000-3-2	Pass
EN61000-3-3	Pass
EN61000-4-2	6 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m 80-1000MHz, 10 V/m 800-960 MHz, and 1400-2000 MHz
EN61000-4-4	1 kV AC and DC Power Lines, 0.5 kV Signal Lines
EN61000-4-5	2 kV AC Line-Gnd, 1 kV AC Line-Line and Outdoor Signal Lines, 0.5 kV Indoor signal Lines > 10m
EN61000-4-6	3 V
EN61000-4-11	Pass

As Information Technology Equipment (ITE) Class A per (as applicable):
EN55022:1998/CISPR22:1997   Class A
EN55024:1998 Required Limits:

EN61000-4-2	4 kV (Direct), 8 kV (Air)
EN61000-4-3	3 V/m
EN61000-4-4	1 kV AC Power Lines, 0.5 kV Signal and DC Power Lines
EN61000-4-5	1 kV AC Line-Line and Outdoor Signal Lines, 2 kV AC Line-Gnd, 0.5 kV DC Power Lines
EN61000-4-6	3 V
EN61000-4-8	1 A/m
EN61000-4-11	Pass

EN61000-3-2:1995 + A1, A2, A14   Pass
EN61000-3-3:1995   Pass

Safety: This equipment complies with the following requirements of the Low Voltage Directive 73/23/EEC:

EC Type Examination Certificates:

EN60950:2000, 3rd Edition	TÜV Rheinland Certificate No. xxxxxxxxxxxx
IEC 60950:2000, 3rd Edition	CB Scheme Certificate No. xxxxxxxxxxxx
Evaluated to all CB Countries	
UL 60950, 3rd Edition, CSA C22.2 No. 60950-00	File: Vol. Sec.
UL 60950, 3rd Edition, CSA C22.2 No. 950-00	File: Vol. Sec.
FDA DHHS Accession Number (Monitors Only)	

Supplementary Information: This product was tested and complies with all the requirements for the CE Mark.

/S/   /S/

Dennis P. Symanski   DATE   Pamela J. Dullaghan   DATE
Manager, Compliance Engineering   Quality Program Manager
Sun Microsystems, Inc.   Sun Microsystems Scotland, Limited
4150 Network Circle, MPK15-102   Springfield, Linlithgow
Santa Clara, CA 95054 U.S.A.   West Lothian, EH49 7LR
Tel: 650-786-3255   Scotland, United Kingdom
Fax: 650-786-3723   Tel: +44 1 506 672 395   Fax: +44 1 506 670 011

Sun Fire B10n Content Load Balancing Blade Version 1.3 Product Notes

This document contains important information about the Sun Fire™ B10n Content Load Balancing Blade Version 1.3.5 application software and the new server modules. This version includes all the features from Version 1.1, 1.2, 1.2 Update, and 1.3. The application software for this release is Version 1.3.5.

Refer to the latest issue of the Sun Fire™ Blade Application Journal for further configuration and architectural overview information. The Application Journal is available at:
`http://www.sun.com/products/networking/blades/index.html`

Note – The current Sun Fire B10n content load balancing blades are shipped with the Version 1.2 software. This document explains how to upgrade your software to the latest version.

Note – If you make configuration changes and the system is rebooted before entering `commit`, the configuration changes since the previous commit will be lost. Always enter the `commit` command after making configuration changes.

Viewing the Latest Product Notes

Additional issues may arise after the publication of this version of the product notes. For the latest information, refer to the latest version of this document available at:

```
http://wwws.sun.com/products-n-
solutions/hardware/docs/Servers/Workgroup_Servers/Sun_Fire_Blad
e_Platform/Sun_Fire_b10n/index.html
```

Software Release Features

Key Features for Version 1.3.5

Key Features for 1.3.5:

- Application monitoring through user scripts
- Weighted Least Connections load balancing scheme
- Response Time load balancing scheme

Software release 1.3.5 includes support for the following operating systems listed in
TABLE 1.

TABLE 1   Supported Servers and Operating Systems

Operating System	Version	SPARC/x86	SF B1600 Server Blades			External Server		VLANs
			SF B100s	SF B100x	SF B200x	SF V60/65x	SF V210/240	
Solaris	8 HW 12/02	SPARC	X				X	Yes
Solaris	8 HW 5/03	SPARC	X				X	Yes
Solaris	8 HW 7/03	SPARC	X				X	Yes
Solaris	8 HW 2/04	SPARC	X				X	Yes
Solaris	9 8/03	SPARC	X				X	Yes
Solaris	9 12/03	SPARC	X				X	Yes
Solaris	9 4/04	SPARC	X				X	Yes
Red Hat Enterprise Linux (RHEL)	AS 2.1	x86		X	X			No
Red Hat Enterprise Linux (RHEL)	AS 2.1 Update-2	x86		X	X	X		No
Red Hat Enterprise Linux (RHEL)	AS 3.0	x86		X	X	X		Yes

TABLE 1   Supported Servers and Operating Systems

Operating System	Version	SPARC/x86	SF B1600 Server Blades			External Server		VLANs
			SF B100s	SF B100x	SF B200x	SF V60/65x	SF V210/240	
SuSe	SLES 8.0 SP-3	x86		X	X	X		Yes
x86 Solaris	9 8/03	x86		X	X	X		No
x86 Solaris	9 12/03	x86		X	X	X		No
x86 Solaris	9 4/04	x86		X	X	X		No

Zip files are available at the Sun Download Center at the following URL:
`http://wwws.sun.com/software/download/network.html`

Enter **B10n** and select Search the Download Center. Select Sun Fire B10n Content Load Balancing. Zip files listed in TABLE 2 are available.

New Monitoring Features Supported in Version 1.3.5

A new feature has been added that checks the configuration of the backend servers for the services offered on the load balancer periodically. The monitoring, which is based on ICMP PING messages, checks for the VIPs being configured on the loopback interface and the service VLANs being configured properly on the server and the switch. The result of this configuration check is shown in the show service *service_name* and show service-lb-group *service_name lb_grp_name* outputs on the CLI. In the case of a bad configuration, the Path column is marked as DN, otherwise it is marked UP for a server in a service.

In addition, a new column, Valid, has been added to the output for a server in a service. A server marked invalid is not being used for load balancing in that particular load balancing group. A server is valid only if all the following conditions are true:

1. The server status is UP. This is true if the module is loaded properly on the server, the interface on the server configured with the real IP is up and the management VLAN, if applicable, is configured properly on the load balancer, switch and server.

2. The server is enabled globally.

3. If application monitoring is enabled for the service, then the application must be up on the server.

4. The server is enabled in the service.

5. The configuration check on the server (as described above) passes.

The following provides sample outputs:

```
puma{admin}# show service-lb-group svc1 default
*---------*---------*---------*----------*---------*---------*----------*

Server Group:
=============
Name                                    : default
Scheme                                  : wt-least-conn
Total and Active servers                : 3 / 3
Rules in group                          : 0

Group Server Table:
================================================================================
Server Name          Port   Wt/CWt   Status       App      Conf Path Valid Conn/s
--------------------------------------------------------------------------------
--
10.4.128.152          0      1/18    UP/EN/ACT    UP/EN    Done  UP   Yes  1
10.4.128.151          0      1/14    UP/EN/ACT    UP/EN    Done  UP   Yes  1
10.4.128.150          0      1/14    UP/EN/ACT    UP/EN    Done  UP   Yes  1
================================================================================
```

```
puma{admin}# show service-lb-group svc1 rt-grp
*----------*----------*----------*-----------*---------*---------*-----------*

Server Group:
=============
Name                                    : rt-grp
Scheme                                  : response-time
Total and Active servers                : 3 / 3
Rules in group                          : 0
                          Group Server Table:
================================================================================
Server Name          Port   Wt/CWt   Status       App      Conf Path Valid RT(ms)
--------------------------------------------------------------------------------
--
10.4.128.152          0      1/19    UP/EN/ACT    UP/EN    Done  DN   No   25
10.4.128.151          0      1/12    UP/EN/ACT    UP/EN    Done  UP   Yes  27
10.4.128.150          0      1/12    UP/EN/ACT    UP/EN    Done  UP   Yes  27
================================================================================
```

New Features Introduced in Version 1.2 Update

The Sun Fire B10n content load balancing blade application software release 1.1 adds high availability pair blade failover and path failover as well as support for the Sun Fire B10p SSL proxy blade.

TABLE 2   Zip Files Available at the Sun Download Center

Software Components	Zip File Name
BSC firmware	`SunFire_B10n-`*version*`#-BSCFirmware.zip`
B10n application software	`SunFire_B10n-`*version*`#-Application.zip`
Blade server module	`SunFire_B10n-`*version*`#-SolarisModule.zip`
	`SunFire_B10n-`*version*`#-LinuxModule.zip`
Administration Guide and Product Notes	`SunFire_B10n-`*version*`#-Docs.zip`

VLANs Optional for SSL Proxy Blades

The use of VLANs within the Sun Fire B1600 blade system is preferred when using the Sun Fire B10p SSL proxy blade. VLANs are configured at the SSC switches to create logical groups of endpoints that can communicate as if they were on the same LAN. VLANs also prevent or restrict traffic between endpoints on separate VLANs. However, some environments might not support VLANs. To disable VLAN operation for the Sun Fire B10p SSL proxy blade, use the `set vlan filter disable` command from the CLI interface.

If you choose to use VLANs, refer to the *Sun Fire B10n Content Load Balancing Blade Administration Guide* for detailed information.

Hardware and Software Requirements

Before using the Sun Fire B10n blade, ensure your system meets the hardware and software requirements listed in TABLE 3. If you need a server module for a later operating system release check the Sun Download Center at:

http://wwws.sun.com/software/download/network.html

TABLE 3 Hardware and Software Requirements

Hardware and Software	Requirements
Hardware	• Sun Fire™ B10n content load balancing blade • Sun Fire B10p SSL proxy blade (optional) • Sun Fire B1600 blade system chassis • Sun Fire B100s blade server for SPARC or Sun Fire B100x/B200x blade servers for x86 • Sun Fire V60/V65 and V210/V240 Servers (External to B1600 Chassis)
Software	• Sun Fire B10n content load balancing blade application software 1.3.5 or subsequent compatible version
	• Sun Fire B10n content load balancing blade BSC (blade support control) firmware v5.1.4* or subsequent compatible version

	• Sun Fire B100s Solaris Operating System versions:
	  Solaris 8 HW 12/02
	  Solaris 8 HW 5/03
	  Solaris 8 HW 7/03
	  Solaris 8 HW 2/04
	  Solaris 9 8/03
	  Solaris 9 12/03
	  Solaris 9 4/04

	• Sun Fire V210/V240 Operating System versions:
	  Solaris 8 HW 12/02
	  Solaris 8 HW 5/03
	  Solaris 8 HW 7/03
	  Solaris 8 HW 2/04
	  Solaris 9 8/03
	  Solaris 9 12/03
	  Solaris 9 4/04

	• Sun Fire B100x/B200x Operating System versions:
	  x86 Solaris 9 12/03
	  x86 Solaris 9 8/03
	  x86 Solaris 9 4/04
	  Red Hat Enterprise Linux (RHEL) Advanced Server 2.1
	  Red Hat Enterprise Linux (RHEL) Advanced Server 2.1 Update 2
	  Red Hat Enterprise Linux (RHEL) Advanced Server 3.0

TABLE 3 Hardware and Software Requirements *(Continued)*

Hardware and Software	Requirements

Software *(Continued)*	• Sun Fire V60/V65 Operating System versions:
	  Solaris 9 8/03
	  Solaris 9 12/03
	  Solaris 9 4/04
	
	  Red Hat Enterprise Linux (RHEL) Advanced Server 2.1 Update 2
	  Red Hat Enterprise Linux (RHEL) Advanced Server 3.0
	
	• Sun Fire B1600 SC (system controller) 1.2 or subsequent compatible system controller firmware
	
	• B10n Solaris server module version v1.65 for Solaris, or B10n Linux server module version xxx1.41-1 for Red Hat Enterprise Linux Advanced Server 2.1.**
	
	• Sun GigaSwift Ethernet Adapter Patch ID 111883-18 or subsequent compatible patch for supported versions of the Solaris 8 software. Sun GigaSwift Ethernet Adapter Patch ID 112817-10 or subsequent compatible patch for supported versions of the Solaris 9 software.**
	
	• Sun Ethernet VLAN Patch ID 112119-04 or subsequent compatible patch for supported versions of the Solaris 8 software. Sun Ethernet VLAN Patch ID 114600-02 or subsequent compatible patch supported versions of the Solaris 9 software.***

* The version number displayed from the `showplatform -v` command from the Sun Fire B1600 SC CLI printout refers to the BSC firmware version. The application software version is observed using the console `show version` command.

**Verify that you are using the supported Linux server module (xxx1.41-1) for the OS version on your Linux server.

***The patch currently installed can be displayed by entering `/usr/ccs/bin/mcs -p /platform/sun4u/kernel/drv/ce`. You can download patches from `http://sunsolve.sun.com`

Updating the B1600 System Controller

You can download the latest version of the `sc` firmware from the following web site:

`http://wwws.sun.com/software/download/network.html`

You need to set up a TFTP boot server to update the `sc` firmware. See the "Setting up a TFTP Server" section of the *Sun Fire B10n Content Load Balancing Blade Administration Guide.*

You can access all the Sun Fire B1600 documentation from the following web site:

```
http://www.sun.com/products-n-
solutions/hardware/docs/Servers/Workgroup_Servers/Sun_Fire_b100s
/index.html
```

▼ To Update the System Controller Firmware

1. **At the** `sc` **prompt, enter the following command:**

   ```
   sc> flashupdate -s install server -f path SSCn/SC.
   ```

   In the following example, 10.4.128.25 is the IP address for your TFTP boot server and
   `stiletto.1.1/c8/SunFireB1600-sc-v1.1.6.flashSSC0/SC` is the path to
   the file:

   ```
   sc> flashupdate -s 10.4.128.25 -f stiletto.1.1/c8/SunFireB1600-sc-v1.1.6.flash
   SSC0/SC
   Warning: Are you sure you want to flashupdate the SSC0/SC flash image (y/n)? y
   SSC0/SC: Preparing to flashupdate.
   flashupdate: erasing segment 36 programming address ffedfffd
   SSC0/SC: flashupdate complete.
   ```

2. **Reset the system using** `resetsc` **to load the new image.**

Updating B10n Application Software and BSC Firmware

It is important to verify that you have the latest software for the Sun Fire B10n
content load balancing blade. Check the following web site for the latest software
and documentation:

```
http://wwws.sun.com/software/download/network.html
```

You need to set up a TFTP boot server to update the `sc` firmware. See the "Setting
up a TFTP Server" section of the *Sun Fire B10n Content Load Balancing Blade
Administration Guide.*

You also need to configure the management IP address and default gateway address.
Refer to the "Configuring the Networking" section of the *Sun Fire B10n Content Load
Balancing Blade Administration Guide.*

> **Note –** If you are updating both the B10n application software and BSC firmware, be sure to update the B10n application software *first*.

▼ To Update the B10n Application Software

With the B10n blade in the booted and running state perform the following steps:

1. Access the Sun Fire B10n console. At the Sun Fire B1600 SC console `SC>` **type:**

```
sc> console Sn
```

Where *n* is the slot number of the B10n blade

2. Login to the B10n console.

```
Login: admin
passwd: admin
```

3. **Verify the boot image and versions:**

```
puma{admin}# show system

Boot Options:
================================================================================
Config Type   Config File   Boot Image   Diag Level    Verbose Mode
--------------------------------------------------------------------------------
running                  2   1 (1.2.3)                 0           0
next                     2   1 (1.2.3)                 0           0
0===============================================================================


Image Information Table:
=====================================================================
Image  Blade  Image Type     Version    Build Date:Time  Size
---------------------------------------------------------------------
1      B10n   Load Balancer  1.2.3      12/05/03 : 14:53   4046868
2      B10n   Load Balancer  1.2.2      11/26/03 : 12:15   4045472
diag   B10n   Diagnostics    1.1.9      10/16/03 : 15:36   2410733
=====================================================================

Flash FS /RFA0 free space = 13,033,472 bytes

puma{admin}#
```

The B10n software can be loaded with three different images and booted. The three images are image 1, image 2, and diag. These images denote software versions.

To load to image location 1, the blade expects image *filename* to be available in the TFTP server. Where *filename* is sunfire_b10n.1.3.5

4. **Determine which image to update (image 1 or 2), and update the empty or oldest image.**

5. **Update the B10n application software**

```
puma{admin}# update image
```

You can upgrade the software either interactively or noninteractively.

▼ To Update the Software Non-interactively

● **As admin, type the following command:**

```
puma{admin}# update image tftp server file image_name image location
```

The following image uses the TFTP server with the IP address of 192.50.50.201, the image name of sunfire_b10n.1.3.5, and the image at location 1.

```
puma{admin}# update image 192.50.50.201 file sunfire_b10n.1.3.5
image 1
```

The system returns the following output, verifying the parameters entered:

```
file exist! will overwrite /RFA0/BOOTIMAGE/boot_image_1
Start downloading sunfire_b10n.1.3.5... using TFTP
Transferring and writing to file /RFA0/BOOTIMAGE/boot_image_1...
please wait.

puma{admin}#
```

The following image uses the TFTP server with the IP address of 192.50.50.201, the image name of sunfire_b10n.1.3.5, and the image at location diag.

```
puma{admin}# update image 192.50.50.201 file sunfire_b10n.1.3.5
image diag
```

The system returns the following output, verifying the parameters entered:

```
file exist! will overwrite /RFA0/BOOTIMAGE/boot_image_diag
Start downloading sunfire_b10n.1.2.2_diag... using TFTP
Transferring and writing to file /RFA0/BOOTIMAGE/boot_image_diag
...............................
please wait.

puma{admin}#
```

See the "To Update the Software Interactively" section of the *Sun Fire B10n Content Load Balancing Blade Version Administration Guide*.

▼ To Set the New Image to be the Default Image

1. **Configure the desired Boot Image. At the B10n console type:**

```
puma{admin}# config boot image x
```

Where *x* is the image you just updated

2. **Save the updated image using the** commit **command:**

```
puma{admin}# commit
commit : Are you sure to continue? [yes|no] yes
```

3. **Reboot to activate the new image:**

```
puma{admin} reboot

reboot: Are you sure to continue? [yes|no] yes
```

▼ To Update the BSC Firmware

1. **Escape to the system controller console by typing the pound sign (#) and period (.) in rapid succession:**

```
puma{admin} #.
```

Note – If the two characters are not typed in rapid succession nothing happens.

---

2. **At the** sc **prompt, check the current version of the BSC firmware:**

```
sc> showsc -v
FRU    Software Version               Software Release Date
-------------------------------------------------------------
S0     v5.1.4-SUNW,B10n,NetBlade1  Aug 12 2003 15:31:48
```

3. **At the** `sc` **prompt, enter the following command:**

```
sc> flashupdate -s TFTP_ip-addr -f filename sn
```

Where *TFTP_ip-addr* is the TFTP server IP address, *n* is the slot number, *filename* is the file name of the image

In the following example, 192.50.50.201 is the IP address for your TFTP boot server and `/tftpboot/525-2018-05-t2.a37`:

```
sc> flashupdate -s 192.50.50.201. -f /tftpboot/525-2018-05-t2.a37 S12
```

4. **Reset the system issuing** `reset s12` **to load the new image.**

Replacing Your B10n Blade

The upgraded B10n blade has the following features:

1. The 1.0 BSC firmware

2. Two B10n boot images—version 1.0.1 and 1.1. The default boot image is 1.1.

3. The B10n bootrom, version 1.1.

▼ To Export the Configuration From the Old Board

1. **Go to the /RFA0 directory**

```
puma{admin}# cd /
```

2. **Tar the CONFIG directory:**

```
puma{admin}# tar lbconfig.tar CONFIG
```

3. **Export the config tar file:**

```
puma{admin}# export file
The FTP server address: <ftp_server_ip>
The source directory path: type [cr] to use current directory:
    (null) source path, using current directory
    The source file name: lbconfig.tar
    The destination directory path: <path_on_ftp_server>
The destination file name: lbconfig.tar
    The user name: <user_name_for_ftp_server>
The user password: <user_password_for_ftp_server>
export file succeed!
```

▼ To Import the Configuration to the Upgraded Board

1. **Power off the old board and remove it from the chassis.**

2. **Install the upgraded board.**

   The board comes up with an empty configuration with the B10n 1.1 application image running.

3. **Configure the network interface. Optionally, configure the management VLAN (if applicable).**

4. **Go to the /RFA0 directory:**

```
puma{admin}# cd /
```

5. **Import the 1.0 or 1.1 configuration:**

```
puma{admin}# import file
    The FTP server address: <ftp_server_ip>
The source directory path: <path_on_ftp_server>
The source file name: lbconfig.tar
    The destination directory path:
    (null) path, using current directory...
    The destination file name: lbconfig.tar
    The user name: <user_name_for_ftp_server>
The user password: <user_password_for_ftp_server>

import file succeed!
```

6. **Untar the configuration file.**

```
puma{admin}# untar lbconfig.tar
```

7. **Reboot the B10n blade to get the imported configuration:**

```
puma{admin}# reboot
```

Note – To run traffic with B10n 1.3.5 application image, the blade server module has to be updated to version 1.3.5.

Updating Your Server

Use the appropriate instructions for updating your Solaris or Linux servers.

▼ To Update the SPARC Solaris Server Module

1. **Download the 1.3.5 version of the server module software from the following site:**
   `http://wwws.sun.com/software/download/network.html`

2. **Unzip the file:**

```
# /usr/bin/unzip SunFire_B10n-1_2_Update-SolarisModule.zip
```

3. **Install the SPARC Solaris server module software packages:**

```
# cd path_to_unzipped_file/Solaris/sparc
# pkgadd -d .
```

4. **Restart the Solaris server module:**

```
# /etc/init.d/clbctl stop
# /etc/init.d/clbctl start
```

▼ To Update the x86 Solaris Server Module

1. **Download the 1.3.5 version of the server module software from the following site:**
   http://wwws.sun.com/software/download/network.html

2. **Unzip the file:**

```
# /usr/bin/unzip SunFire_B10n-1_2_Update-SolarisModule.zip
```

3. **Install the x86 Solaris server module software packages:**

```
# cd path_to_unzipped_file/Solaris/i386
# pkgadd -d .
```

4. **Restart the Solaris server module:**

```
# /etc/init.d/clbctl stop
# /etc/init.d/clbctl start
```

▼ To Update the Linux Server Module

1. **Download the 1.3.5 version of the server module software from the following site:**

   `http://wwws.sun.com/software/download/network.html`

2. **Unzip the file:**

   ```
   # /usr/bin/unzip SunFire_B10n-1_2_Update-LinuxModule.zip
   ```

   Different Linux OS subdirectories are available, such as, `RHAS_2.1`, `SLES_8.0`, ... additionally, hardware platforms such as `B100x`, `B200x` and `V60_65x` are available.

3. **Install the Linux server module for RHAS 2.1 Update 2, for example:**

   ```
   # rpm -i sun-clb-k2_4_9_e_24-1.41-1.i386.rpm
   # rpm -i sun-clb-admin-1.41-1.i386.rpm
   ```

4. **Restart the Linux server module:**

   ```
   # /etc/init.d/sun-clb restart
   ```

▼ To Upgrade the Linux Server Module From an Existing Installation

1. **Download the 1.3.5 version of the server module software from the following site:**

   `http://wwws.sun.com/software/download/network.html`

2. **Unzip the file:**

   ```
   # /usr/bin/unzip SunFire_B10n-1_2_Update-LinuxModule.zip
   ```

   Different Linux OS subdirectories are available, such as, `RHAS_2.1`, `SLES_8.0`, ... additionally, hardware platforms such as `B100x`, `B200x` and `V60_65x` are available.

3. **Upgrade the Linux server module for RHAS 2.1 Update 2, for example:**

   ```
   # rpm -U sun-clb-k2_4_9_e_24-1.41-1.i386.rpm
   # rpm -U sun-clb-admin-1.41-1.i386.rpm
   ```

4. **Restart the Linux server module:**

```
# /etc/init.d/sun-clb restart
```

Known Issues

This section outlines the known problems with the current version of the software and describes workarounds to overcome these problems.

Stopping Failover Monitoring or Unknown Failover State (Bug ID 5046437 and Bug ID 4925823)

When failover monitoring is stopped and the configuration is committed and then the system is rebooted it could come up without any of the load balancing configuration loaded. It could also happen if you skip the failover synchronization at boot time.

Work around:

1. **The configured failover peer and the B10n in consideration should not come up with the same load balancing configuration when failover is stopped. To prevent them from coming up with the same configuration turnoff the peer or erase the configuration on the peer (`config erase config-files`) and reboot.**

2. **Enter `show system` to find out what configuration file you are using, which is displayed in the second column. In this example, the `config` file is `config_X`, where `X` is 1 or 2.**

3. **Remove two failover configuration files:**

```
puma{admin}# rm /RFA0/config/failover/config_1/failover/failover_cmd.conf
puma{admin}# rm /RFA0/config/failover/config_1/failover.state
```

4. **Reboot the B10n blade.**

Stopping an Application Server While Running Application Monitoring (Bug ID 4997595)

If an application is reported as down (from application monitoring) on a B10n and when the application is down, if the application monitoring is disabled then when the server application comes back up this is not detected and traffic is not sent to that server for that service.

Workaround: Either enable application monitoring again or remove the server from the service completely (that is, from all the groups in the service) and then add it again to the service.

Unknown Filter Edge [b9000010] (Bug ID 4925821)

The B10n blade can hang up on boot after displaying the following message:

```
Unknown Filter Edge
```

This does not happen in normal operation. It happens only if the `classifier.pm` file gets corrupted in the `config/config_X` directory. Where *X* is the current configuration (1 or 2).

Workaround: Boot using the alternate configuration and remove the file `config/config_X/classifier.pm` where *X* is the configuration boot up that fails and has a value of 1 or 2.

VIP Address Conflict (Bug ID 4910001)

If the load balancer VIP address is mistakenly used on another device, the other device broadcasts a gratuitous ARP and forces all of the clients and routers to learn that ARP entry.

Use the `config vip-broadcast VIP-address mask` command to force the load balancer to send a gratuitous ARP and force the clients and routers to relearn the VIP ARP entry as that of the load balancer.

Configuring VIP Addresses to be the Same as `path failover` Target IP Address (Bug ID 4907833)

This problem indicates a bad network configuration. The VIP address cannot be the same as the `path failover` target IP address. A future release will check for this condition.

Layer 7 Based Services and Layer 4 Services With Rules Will Fail to Respond (Bug ID 4998054 and Bug ID 5060108)

This error occurs rarely and only when the system is rebooted. The message on the console is as follows:

```
SPI3 IF not responding (powercycle the blade to recover)
```

Powercycle the B10n blade only if it prints out this message continuously every minute. To powercycle the system go to the B1600 platform console and enter `poweroff` to turn off the system and then enter `poweron` to turn it on. Just entering `reboot` on the B10n console does not solve the problem, the system must be powercycled.

Removing Services (Bug ID 5057931)

Removing all of the load balancing services and then entering `commit` does not remove the services from the files. The services will be loaded when the system is rebooted. Removing some of the services works correctly.

Workaround: Remove the services first and then remove the configuration file and enter `commit` to commit the changes. Use the following procedure:

1. **Enter `show system` to verify what configuration file you are using, which is displayed in the second column. In this example, the `config` file is `config_X` where `X` is 1 or 2.**

2. Remove the **/RFA0/config/config_*X*/service/services.conf** file where ′X′ is 1 or 2:

```
puma{admin}# rm /RFA0/config/config_X/service/services.conf
```

CRITICAL Message Displayed When Removing a Service (Bug ID 5057951)

The following message is not a critical message and just notifies that the service is going away.

```
CRITICAL: No valid servers in default group: Deactivating service
<servicename>
```

Ignore this message.

Rule Build Required Message (Bug ID 5057959)

When commiting changes, the system reports that a rule build is required when there are no services in the system.

The message is as follows:

```
The Rule Classifier is not saved. Rule build required.
```

Ignore this message.

Rule Build Complete Message Appears Only on the Console (Bug ID 4879355)

When the rule build process is complete, the message appears only on the console and not on the Telnet sessions.

Workaround: Enter the show build status command to verify if it is complete.

Message Indicates Configuration Change After Rebooting (Bug ID 5043929)

When a B10n blade is rebooted, a message reports that the configuration has changed even if rebooted immediately after entering `commit`.

This error occurs rarely. For safety, ensure all the changes are commited before entering `reboot`.

Using the `poweroff` and `poweron` Commands (Bug ID 5028523)

The B10n blade may fail to complete the booting process if no messages are being displayed on the console. Use the `showplatform -v` command to check for OS running status.

Workaround: Enter a `poweroff` command followed by a `poweron` command to restart the booting process.

Using the `app-monitor` Configuration Command (Bug ID 4997604)

Using the `app-monitor` configuration command with missing parameters (`interval` & `max-try`) returns an incorrect error message. For example, the following error message occurs:

```
puma{admin}# config service app-monitor name ssL4 proto http
Error: Invalid parameter.
```

To be more accurate, it should display "`Error: Missing parameter.`"

Time Not Kept Consistent With System Controller (SC) (Bug ID 4946746)

After rebooting the B10n blade, the time might be out of sync with the SC.

Workaround: Reboot the B10n blade to resynchronize the clocks.

Incorrect MAC Address Overwritten Message (Bug ID 4925709)

A message similar to the following could appear on the B10n console of both the active and standby blades.

```
0x8f5fc2b0 (tNetTask): arp info overwritten for c0a865ab by 00:03:ba:2a:05:60
```

The MAC addresses are not changed and no conflicts are caused in the network. The message displays the correct MAC address for the right server IP address.

Diag Back-To-Back(External) LoopBack Test (Bug ID 4928957)

This test passes with or without cable, but should only pass with a valid cable connected.

Disabling All VLANs (Bug ID 4886383)

In the command-line interface (CLI), the **config no enable vlan all** command only disables the Data and Management VLANs and not the Service VLAN.

Configuring Path-failover IP Addresses (Bug ID 4908470)

The failover active peer incorrectly allows configuring the path-failover IP address to be the same as the standby interface address. If this scenario is committed or failover is forced to the standby peer, the path-failover configuration information will not be transmitted. Consequently, when the standby becomes active, it will not have the path-failover configuration information.

Building Rules (Bug ID 4925705)

Building rules twice deletes the rule build status information. If rules are built without making any changes, it finishes up immediately, which resets the counters in the `show build status` output.

Error Messages for Updating the Bootrom Image (Bug ID 4926343)

If a non-bootrom image is mistakenly updated in flash with the `update image` command, the following error message is displayed: "`Bootrom image version is old.`" This error message should indicate that a non-bootrom image is not acceptable in flash.

Older Date Appears on `config_1` and `config_2` Files (Bug ID 4973992)

Jan 1 1980 date appears as the date for the `config_1` and `config_2` configuration files. This date is incorrect.

Application Monitor Commands (Bug ID 5003231)

The application monitor command parameters require the entire command to be typed even if only one parameter is being changed. For example, just changing the interval or max-try parameters requires the following syntax:

```
puma{admin}# conf service app-monitor name name interval num max-try num proto
http
```

SSL Traffic Without an SSL Device Cannot be Layer 7 Load Balanced (Bug ID 4950182)

In the absence of an SSL device, SSL traffic can only be Layer 4 load balanced as there is no way to look at the Layer 7 data and load balanced on that basis.

IP Persistence Does Not Release Its Persistence With Short Timeouts (Bug ID 5023896)

Short timeout values do not have the expected result. Timeout values must be at least 15–20 minutes, and the granularity of timing out entries is in the order of 10 minutes.

Output From the `show arp` Command (Bug ID 4819914)

The following example shows a typical output from the `show arp` command:

```
LINK LEVEL ARP TABLE
destination      gateway            flags Refcnt  Use           Interface
---------------------------------------------------------------------------
192.50.50.11     00:03:af:26:73:07405   0       35330         iq0
192.50.50.12     00:03:af:26:97:fb405   1       16653         iq0
---------------------------------------------------------------------------
```

In the ARP table the gateway and flags columns are improperly shown. In the example above, `405` in the first line `should be aligned under the flags heading.`

Online Help Documentation Error (Bug ID 4900728)

Due to errors in Wind River's Rapid Control software, the following commands print the same output:

- `config no dns ?` and `config dns ?`
- `config no service ?` and `config service ?`
- `config no ssl ?` and `config ssl ?`
- `config no path-failover ?` and `config path-failover ?`

In addition, the correct syntax for these "`config no`" commands is as follows:

```
puma{admin}# config remove dns server ip-addr
puma{admin}# config remove service service-name
puma{admin}# config remove ssl
puma{admin}# config remove path-failover
```

Specific Sequence Required

System may panic if the content load balancing module (`clbmod`) is added to a "down" `ce` interface

Workaround: Be sure the `ce` interface is "up" before you load `clbmod`.

Note – If the B10n software from the Solaris 8 7/03 Software Supplement CD is loaded onto an unsupported platform and the system is rebooted, the following message is displayed: "can't load module: No such file or directory."

Adding an SSL Service With a Duplicate Port (Bug ID 4908515)

When adding an SSL service, using the same VIP address with a different port, but the same SSL port is not allowed. The new SSL service must have a unique port number. For example, if an initial SSL service is running on SSL port 880, you must specify a different SSL port number for each new SSL service such as SSL port 881, 882, and so on.

Workaround: Remove the failover configuration from the system with the following commands as `admin` in config mode:

```
puma(config){admin}# config remove failover
puma(config){admin}# rm /RFA0/config/failover/config_x/failover/
failover_cmd.conf
```

Reboot the system.

If you still want to keep the blade failover configuration after the reboot, please refer to the "Configuring Failover" chapter in the *Sun Fire B10n Content Load Balancing Blade Version Administration Guide*.

Note – In all of the references to `config_x`, the 'x' is 1 or 2 depending on whether your load balancing is currently using configuration directory `config_1` or `config_2`.

Skipping the Failover Synchronization at Boot Time

At boot time, you have the option of skipping the blade failover synchronization. During boot the system prints the following message and waits for 5 seconds for you to respond:

```
Press Return key to skip the failover synchronization ...
```

config no ip interface *0|1*

If both interfaces of the B10n device are configured in the same subnet and if one of the interfaces is unconfigured, there might be loss of network connectivity from the B10n device. The device might not be able to switch all servers to the alternate interface. This can cause server/SSL devices to be marked down, and they will not be used in the load balancing.

Workaround: After unconfiguring the interface. Do a commit and then reboot the system.

Troubleshooting

You may notice the following behaviors, which might be interpreted as being problems. However, they are normal behaviors.

VIP IDs Not Checked

If another system in the subnet is configured with the IP address used in the VIP of a service configured on B10n the networking for that system will not work because the clients and routers will learn one machine's MAC and the other machine will not receive any traffic on that VIP.

Workaround: Because this is normal behavior, the only workaround is to ensure that you do not use duplicate VIP addresses.

commit Allowed Though No Changes

The B10n software still allows the commit command even though no changes have been made to the configuration.

Workaround: This problem causes no ill effects, so it can be noted and ignored.

Server/SSL Does Not Respond to ping Even Though it is Marked as Up.

If both interfaces are configured in the same subnet then in some scenarios it is possible that the default route to a server/SSL device might be down and the devices might be unreachable (ping fails) from B10n, but the monitoring shows them as up.

This is not a bug. The monitoring will switch to the alternate interface and try to reach the device. ping will only try the one default interface.