SUN SPARC
ENTERPRISE
SERVERS

An Oracle White Paper
July, 2010

Sun Fire Midframe & Entry-Level Servers Best Practices Update for Firmware 5.20.x

Introduction.. 1
Platform Configuration 2
Configuring the RS-232 Serial Port 2
Configuring the Ethernet Port 3
Configuring a Switched Private Network 3
Configuring the Alarms Port (Entry-Level only)...5
Periodic Sun Fire SC Reboots...6
Configuring SC Failover (Midframe server only)...7
Setting the Date and Time on the Platform 11
Configuring SNTP (Midframe Servers only)...12
Changing POST Levels and Other Settings 13
Configuring the Midframe and Entry-Level Service Processor 16
Configuring the SP to receive Log Messages...17
Sun MC Software 19
Preparing for Firmware Updates 19
Explorer Data Collector 20
Monitoring Domain Consoles 22
Platform and Domain Administration 23
Platform Security 28
Recommendations for User Authorization 29
Serial Port Access 29
Telnet and Secure Shell Sessions 30
Keyswitch Settings (Midframe Server Only)..33
Error Analysis, Diagnosis and Recovery 33
Maintenance Functions 34
Periodic Server Maintenance 34
Restoring the Sun Fire SC Configuration 35
Updating the Firmware and Real Time Operating System 36
Removing the SC from Platform Use 37
Appendix 38
Conclusion..41

Introduction

The Sun Fire Midframe and Entry-Level server has undergone many improvements since the last revision of this document for firmware 5.18.x. The purpose of this document is to give guidance to the reader on the application of many of those improvements, and describe how to implement the new features to improve the overall system reliability, availability, and serviceability. To achieve the highest degree of availability it is important to develop a well planned and efficient Administrative Environment. With proper advanced planning many failures can be eliminated, or their impact minimized.

System Notes:

- The Sun Fire Entry-Level family includes the single domain (and single SC) servers Sun Fire v1280, E2900, Netra 1280 and Netra 1290.
- The Sun Fire Midframe family includes the multi domain (also dual-SC) servers, Sun Fire 3800, 4800, 4810, 6800, E4900, and E6900.

This article revisits existing best practices that were presented in previous versions of this document and presents additional new material. Specific enhancements to this article are the inclusion of Entry-Level server recommendations, enhanced instructions relating to private networks, and System Controller maintenance best practices.

ScApp 5.20.x is the last release of the firmware which will be maintained on these systems. Users are encouraged to utilize the latest revision of this release as soon as possible in order to take advantage of the latest enhancements. No other release of ScApp is being maintained.

Platform Configuration

This section contains descriptions of how to configure the Sun Fire Midframe and Entry-Level platform.

The topics include:

- Configuring the RS-232 Serial Port
- Configuring the Ethernet Port
- Configuring a Switched Private Network
- Configuring the Alarms Port (Entry-Level server only)
- Periodic Sun Fire SC Reboots
- Configuring SC Failover (Midframe server only)
- Setting the Date and Time on the Platform
- Configuring SNTP (Midframe server only)
- Changing POST Levels and Other Settings

Configuring the RS-232 Serial Port

You can access the SC through the built-in RS-232 serial port or through its 10/100BASE-T Ethernet port. Be sure that access to the serial port is available during the initial setup of the SC because it is the only connection on which the SC *poweron* self-test (SCPOST) output can be viewed. The port settings should be 9600 bps, 8- bits, no parity, and 1 stop bit (9600-8-N-1).

You can also access the serial port by using a network terminal server (NTS), by using the serial port on a Midframe and Entry-Level Service Processor (SP) or any other system with a serial port. For more information about the need for an SP and on how to configure the SP, refer to the section, "Configuring the Midframe and Entry-Level Service Processor".

After you have set up the SC, serial port access should continue to be available on demand to provide an alternate access path to the SC in the event of a network problem. It can also be utilized to perform firmware updates and to monitor SC reboots or resets. Serial port access is also required to monitor certain SC and platform related errors because the serial port is the only place where these errors will be displayed.

Making sure there is viable serial port access to the SC is an important proactive measure to take. This access assures that a direct connection to the SC exists in a worst case situation, allowing an administrator to immediately obtain access to the SC error logs and perform platform or domain level tasks to troubleshoot or recover the configuration. Costly system downtime may be extended if serial port access is not proactively enabled. Connecting the serial port from the SC to a domain that the SC administers, in effect “self-monitoring” the platform, is NOT recommended. Use the SP, NTS, or an admin workstation instead.

Configuring the Ethernet Port

The Ethernet port should be used as the primary connection path for the speed, multisession access, and logging capabilities it provides. Ethernet connections to the SC are accomplished by using a Telnet or Secure Shell (SSH) session. A 100BASE-T link is strongly recommended for the SC Ethernet connection and required for use with Sun Management Center (Sun MC) software. The Ethernet port should not be used instead of the RS-232 serial port connection, but rather in addition to the RS- 232 port.

With ScApp 5.16.0 or higher the ethernet port is accessible by using SSH or telnet. Prior to 5.16.0, only telnet was available. SSH is a more secure communication protocol which provides session encryption across the network. SSH is discussed in more detail in the Platform Security section.

Configuring a Switched Private Network

You should configure the System Controller(s) on a switched private network and the SC(s) should not undergo any type of security or port scanning.

The Midframe and Entry-Level System Controller is a specialized, dedicated, network appliance for managing attached mainframes. It was never designed to handle network traffic and processes greater than those specifically needed to do the job for which it was designed. Additional artificial load on the SC can be detrimental to its operation by overwhelming it's limited resources.

Security port scanning is a specific example of artificial load on SCs that should be avoided. Scanning has been known to get SCs into a state where they are too busy handling extra scanning related traffic and they can not perform basic platform operations. Since the SC is not engineered to handle such extra load, it should not be exposed to it. If configured on a private network, you assure the configuration is physically isolated from the outside world and you negate any need to perform security port scanning on the SC at the same time.

If you are configuring two SCs for the network, assign each a separate IP address so that they do not conflict with each other on the network. If SC failover functionality (*Midframe only*) is used, a third IP address representing the logical hostname can be assigned. FIGURE 1 illustrates a simplified network topology of a Midframe (dual SC) configuration.

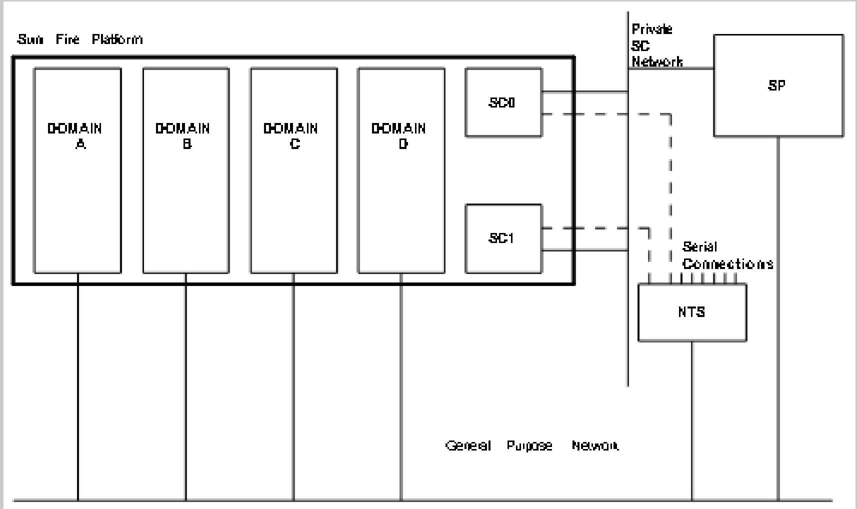


FIGURE 1: Simplified network topology of a Midframe SC Configuration

Figure 1 Notes:

- The example specifically shows a Midframe configuration. The same recommendation exists for Entry-Level Servers, but they only have a single domain and SC, so that topology is somewhat simpler.
- The Service Processor (SP) is a workstation placed on the private net to provide administrative support functions to the platform(s) and SCs (for example, firmware updates).
- The SC serial port can be attached to a Network Terminal Server (NTS) and if the same SP is monitoring multiple platforms, an NTS is a recommendation. If the NTS supports encrypted logins (for example, by using SSH), it may be connected to a public net.

Configuring the Alarms Port (Entry-Level only)

On the back panel of Entry-Level servers, just below the external SCSI connector, there is an Alarms Port (see Figure 2).

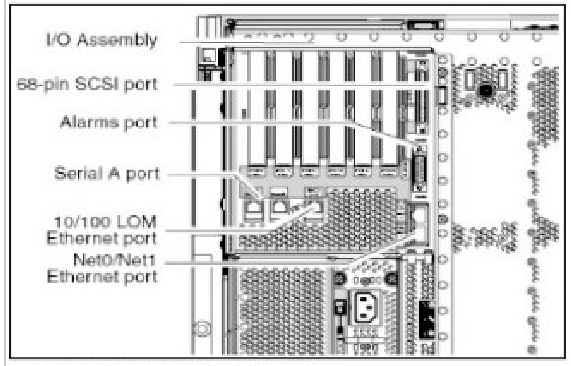


FIGURE 2: Rear view of Entry-Level Server

The Alarms Port allows the end user to trigger an external event of some sort such as an audible or visual alarm. The end user is expected to wire their own cable to this port since it is unknown in advance what type of alarm an end user might wish use.

> **Note** – The Entry-Level System Service Manuals contain the pin and signal diagram for the Alarms Port if needing to build a cable to take advantage of this option.

A Solaris script will be required to switch the alarm to ON, for example the following trivial example:

```
# if
> grep -i 'file system full' /var/adm/messages
> then
> lom -A on,1
> fi
```

Based on the script above, if the file system becomes full, the alarm is switched on. When the Alarms Port is switched on, it triggers a relay on the other end of the cable, which rings a bell (as an example). With suitable external amplification, the relay could equally close an emergency door, or do some other useful task depending on your desire or configuration (turn on a light, etc).

A useful command from the SC lom prompt to view alarm status is shown below:

```
lom> showalarm 1
alarm1 is off
```

Once again, the alarms port is entirely customer configurable. Support for the use of alarms extends only to ensuring that alarms go on or off when requested. See the appropriate Systems Service Manual for details of alarms port pinouts.

Notes:

- There are two useful alarms (alarm 1 and 2) for external events. Alarm 3 is dedicated to the boot state of Solaris, indicating whether Solaris is running or not.
- Alarm 3 will be in the ON state at the ok prompt, when Solaris is not running. When Solaris is fully booted, alarm 3 will automatically change state to OFF.

Periodic Sun Fire SC Reboots

As previously discussed, the Midframe and Entry-Level System Controller is a specialized, dedicated, network appliance for managing attached mainframes. It has limited resources at it's disposal and is somewhat susceptible to "out of memory" issues under certain situations.

Example issues which might be encountered are SC Time of Day (TOD) inconsistencies, a "hung" or otherwise unresponsive SC, or an SC that encounters a Watchdog Reset. This is not an exhaustive list of symptoms and in many cases are avoidable by a simple periodic reboot of the SC(s).

If an SC gets into an out of memory state, the domain(s) is usually unaffected at the time. But, if a domain should require an SC to take action (such as run POST on it, recover a domain from a hardware error, or instruct it to boot), the SC may not be able to take that action due to the "out of memory" condition that it is suffering from.

Advice: Avoid "out of memory" situations by preventing an SC from accumulating high uptime by performing periodic SC reboots.

A period of one reboot each 3-6 months should be sufficient.

It would also be good advice to connect via the SC serial port to watch the SC reboot in case anything goes wrong with the reboot process.

> **Caution** – If you reboot your domains frequently, you would be advised to reboot the Sun Fire SC at a more frequent rate then noted above. Domain reboots fragment SC memory and can more quickly bring upon an "out of memory" condition. So, you may be best advised to just reboot the SC at the same time as the domains to avoid any issues.

An Entry-Level SC is reset as follows (make sure the domain is not currently performing a DR or being turned on or booted when this is executed):

```
lom>resetsc –y
Are you sure you want to reboot the system controller now? yes
(-y)
Waiting for critical processes to finish. This may take a
while.
Critical processes have finished.
Rebooting. All telnet connections closed. Reestablish any
needed connections.
Fri Dec 12 08:51:25 mylw8 lom: Stopping all services on this SC
Fri Dec 12 08:51:25 mylw8 lom: All services on this SC have
been stopped.
Software Reset...
```

The following shows how to reboot a Midframe SC (make sure no domain is currently performing a DR or being turned on or booted when this is executed):

```
schostname:SC> reboot
Are you sure you want to reboot the System Controller now?
[no]yes
```

Configuring SC Failover (Midframe server only)

SC Failover was first introduced in ScApp 5.13.0. You should configure the two Sun Fire Midframe System Controllers for failover functionality in case one of the SCs fail and to keep the domains in the system running. In the event that the main SC fails, the spare SC can take over administrative and system clock functionality for the platform.

Note - Entry-Level servers contain a single SC, so they do not have failover functionality.

Before enabling the SC failover, both SCs and all boards in a Sun Fire platform should be at the same firmware version. While it is possible to have mixed versions of firmware, it is recommended that all boards and SCs use the same version of firmware because the system is not qualified to operate in an untested, mixed firmware, configuration.

You can determine the firmware version as follows:

```
sf4800-sc0:SC> showboards -p version

Component   Compatible Version
---------   ---------- -------
SSC0        Reference  5.20.14
/N0/IB6     Yes        5.20.14
/N0/IB8     Yes        5.20.14
/N0/SB0     Yes        5.20.14
/N0/SB2     Yes        5.20.14
sf4800-sc0:SC>
```

The above output does not include the version of firmware from the spare SC.

To gather information on the SPARE SC, you must connect to it and use the *showsc -v* command as shown below:

```
sf4800-sc1:sc> showsc -v
SC: SSC1
Spare System Controller
SC Failover: disabled
SC date: Tue May 11 12:47:10 CST 2010
 CST  GMT-6     Central Standard Time
SC uptime: 5 days 4 hours 3 minutes 38 seconds
ScApp version: 5.20.14
Version build: 1.0
Version String:  5.20.14
RTOS version: 49
SC POST diag level: off
Clock source is: 75MHz
sf4800-sc1:sc>
```

When SC Failover is enabled, the two SCs communicate with each other by using an internal communications link. They exchange health information and synchronize internal configuration information over the link. The SC that is acting as the MAIN SC also generates a heartbeat. If the heartbeat unexpectedly disappears, the SPARE SC takes over the MAIN functionality.

SC failover functionality includes a number of commands and settings. The *showfailover* command can be used to check failover status, and the *-v* option (for *verbose*) gives the most detail. It is a good idea to run the *showfailover -v* command whenever you reboot an SC to ensure that SC failover functionality has restarted and is functioning properly.

Using the example below, the information shows that the *showfailover -v* command was run on SC0 and it indicates that:

- SC0 is currently in the role of MAIN.
- Both SC failover function and clock function failover are enabled and active as is desired.

```
sf4800-sc0:SC> showfailover -v
Main System Controller
SC Failover: enabled and active.
Clock failover enabled.

sf4800-sc0:SC>
```

You can obtain additional SC failover status information by using the *showplatform -p sc* command, as in the following example:

```
sf4800-sc0:SC> showplatform -p sc

SC POST diag Level: min
SC Failover: enabled and active.
Logical Hostname: sf4800-sc

sf4800-sc0:SC>
```

The Logical Hostname

In the previous example, the value for the logical hostname is displayed (*sf4800-sc* in that example). Each SC continues to have a unique IP address and hostname (*sf4800-sc0* and *sf4800-sc1* in this example) assigned to it. The logical hostname is a third IP address that always points at whichever SC is currently functioning in the role of MAIN. You could also refer to this as a "floating" or a dynamic hostname. If your network is configured properly, when you utilize the Logical Hostname or IP address, you will be assured to always connect directly to the MAIN SC.

See FIGURE 3 for a graphical representation of this arrangement:

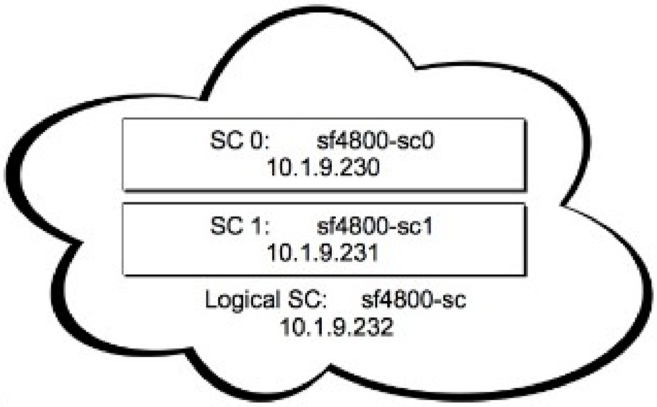


FIGURE 3: Logical SC Naming Example

The following is an example of how to set up the Sun Fire SC failover functionality and logical hostname (configuring the hostname to be *sf4800-sc*):

```
sf4800-sc0:SC> setupplatform -p sc

SC
--
SC POST diag Level [max]:
Enable SC Failover? [no]: yes
Logical Hostname or IP Address []: sf4800-sc

sf4800-sc0:SC>
```

If the Logical Hostname is already set up, a user can simply run *setfailover on* to turn on failover. To force the SPARE SC to assume the role of MAIN, use the *setfailover force* command. This should not be necessary under normal operating conditions, but the functionality should be tested during a maintenance window after you enable the failover functionality to verify correct failover operations.

Even though SC Failover copies configuration information from the MAIN SC to the SPARE SC, it is not a replacement for backing up the SC. Users should perform a *dumpconfig* of the SC after enabling failover and on a regular basis. See the *Sun Fire Midrange System Controller Command Reference Manual* for details on how to use the *dumpconfig* command.

> **Note** – Entry-Level server does not utilize *dumpconfig* for backup purposes. A backup copy of critical NVRAM data is automatically copied to the System Configuration Card (SCC) and kept in sync. See the Appendix section on the SCC for more details.

For failover to work properly the time on both SCs must be as close as possible. A variation of more than 5 minutes can prevent failover from functioning properly. It is recommended that the SCs be configured to sync their clocks to a common source and when a failed system controller is replaced the time should be checked and synced with the running SC.

SNTP is strongly recommended with SC failover and is discussed in a later section of this article. If it is not enabled, the time on the two SCs needs to be manually checked to ensure that they are the same.

Setting the Date and Time on the Platform

When a Sun Fire Midframe platform is installed, the platform time should be set from the platform shell and in each individual domain using the *setdate* command.

The following example illustrates one method for changing the Platform time on a Midframe SC:

```
sf4800-sc0:SC> setdate -t America/New_York 051200502010
Wed May 12 00:50:00 EST 2010
sf4800-sc0:SC> showdate -v
Wed May 12 00:50:11 EDT 2010
America/New_York              GMT-05:00 Eastern Standard Time
sf4800-sc0:SC>
```

On Midframe servers, each domain can have a separate time setting. Setting each domain's time individually is required. Instead of executing the *setdate* in the platform shell, you execute it in each domain shell as the following example indicates (The following example shows how to change into Domain A's shell and then change the domain's time):

```
sf4800-sc0:SC> console -d a
Connected to Domain A
Domain Shell for Domain A
sf4800-sc0:A>setdate -t America/New_York 051201032010
sf4800-sc0:A>showdate
Wed May 12 01:03:13 EDT 2010
sf4800-sc0:A>
```

An Entry-Level server SC date/time is set as follows (very much the same as Midframe except there is not an individual setting for Platform versus domain):

```
lom> setdate 051200502010
lom> showdate
Wed May 12 00:50:08 EDT 2010
```

You can also utilize the Solaris *date* command on the Entry-Level domain if it is booted and running Solaris to change the domain's time.

Use the *setdate -h* command to review the various options for setting the time. There are a number of different ways to change the date/time, so the *-h* (or help) option to the *setdate* command is quite useful.

It is important to note that setting a timezone with an explicit offset from GMT will result in the system controller not adjusting for daylight savings time. If you want to adjust for daylight savings time specify a timezone setting that adjusts to daylight savings time such as EST, or by using the method shown above. *showdate -tv* can be used to get the full list of acceptable locations and timezones.

Configuring SNTP (Midframe Servers only)

With ScApp 5.13.0 and higher, the SC is capable of synchronizing its time-of-day clock with a network time server using SNTP. SNTP usage is encouraged to keep both SCs at an accurate time.

The following example shows how to enable SNTP:

```
sf4800-sc0:SC> setupplatform -p sntp
SNTP
----
SNTP server []: 10.1.63.251
sf4800-sc0:SC>
```

An SNTP server is a system or device (such as a router) which supports the NTP protocol. The SNTP server you select should be as close to the System Controller as possible on the network to reduce the chances of network latency affecting the time stamp.

It is also a good idea to configure each domain to utilize the same network time server as chosen for the SC(s). This assures that the SC(s) and Domains are all synchronized from the same clock source. A configuration such as this avoids any problems which could arise if SC or Domain time was significantly different.

More information on the recommendation and how to avoid known clock related issues is available in Document 1004720.1 *Sun Fire[TM] 3800, 4800, 4810, 6800, E4900, E6900: How do the clocks work?*

Changing POST Levels and Other Settings

To provide thorough testing of all components power-on self-test (POST) level for both the SC and domains should be set to perform the maximum amount of testing in the time available.

System Controller POST (SC POST)

In normal operation on both Entry-Level and Midframe SCs, the SC POST level should be set to *min*. Maximum (*max*) SC POST should be run at least once during system installation and anytime a System Controller hardware problem is suspected, but is not necessary for normal system operation.

The following example shows an Entry-Level SC being configured for *min* SC POST:

```
lom> setupsc
System Controller Configuration
-------------------------------
SC POST diag Level [off]:min
Host Watchdog [enabled]:
Rocker Switch [enabled]:
Secure Mode [off]:
PROC RTUs installed: 0
PROC Headroom Quantity (0 to disable, 4 MAX) [0]:
Tolerate correctable memory errors [false]:
Enable Memory Page Retirement [false]:
lom>
```

Midframe utilizes the *setupplatform* command to change SC POST setting as shown below:

```
sf4800-sc0:SC> setupplatform -p sc

SC
-
SC POST diag Level [max]:  max
Enable SC Failover? [yes]:
Logical Hostname or IP Address [sf4800-sc]:
sf4800-sc0:SC>
```

Domain POST

In normal operation, domain POST should be set to maximum (*max*) or default. The *default* and *max* levels are functionally the same for domain POST.

The following shows how to view and then modify an Entry-Level domain POST setting at the open boot prom (OBP) or "ok" prompt:

```
ok printenv diag-level
diag-level          init  (init)
ok setenv diag-level quick
diag-level=quick
```

The following shows an example of suggested Midframe server boot parameters on domain A:

```
sf4800-sc0:A> showdomain -p bootparams
diag-level = default
verbosity-level = min
error-level = min
interleave-scope = within-board
interleave-mode = optimal
reboot-on-error = true
hang-policy = reset
OBP.use-nvramrc? = true
OBP.auto-boot? = true
OBP.error-reset-recovery = sync
sf4800-sc0:A>
```

At certain times it will be desirable to use a different level of domain POST. The highest level POST, *mem2*, should be run as it performs the most thorough testing of all components for a number of different reasons, for example:

- During system installation to confirm the hardware sanity of the configuration.
- Following a hardware replacement service action to confirm sanity of the serviced parts.
- Following any hardware moves (relocation or system move).
- When a hardware issue is suspected in causing a system problem where error messaging is insufficient to provide root cause (and under Support Services recommendation).

Note – Don't forget to change *diag-level* back to default POST setting after extended testing is complete. Doing so prevents unnecessary delays in normal domain reboot recovery.

Recommended Domain Parameters for POST and Hang Condition Recovery

PARAMETER	**SETTING**	**DESCRIPTION**
reboot-on-error	true	Automatically reboots the domain when a hardware error is detected. Also boots the Solaris operating environment when the OBP.auto-boot parameter is set to true.
hang-policy	reset *	Automatically resets a hung domain through an externally initiated reset (XIR). *See note on following page if upgrading from <5.15.0.*
OBP.auto-boot	true	Boots the Solaris operating environment after POST runs.
OBP.error-reset-recovery	sync	Automatically reboots the domain after an XIR and generates a core file. However, sufficient disk space must be available to hold the core file.
Log-reset-data	true	Allow reset information to be logged which can be displayed showresetstate.
verbose-reset-data	on	Archive verbose reset information which can be displayed via showresetstate -v.
reset-data-ftp-url	varies	Location where to ftp reset data automatically.
max-panic-diag-limit	mem2	Max POST level run when domain is caught in a panic reboot loop.

Note – If you are upgrading from a version prior to 5.15.0, the *hang-policy* variable is set to *notify* by default. When you upgrade, that setting will remain at *notify*, but it is beneficial to change it to *reset* instead.

Configuring the Midframe and Entry-Level Service Processor

While the Sun Fire platform can be administered in a standalone fashion, for ease of problem diagnosis, accessibility to platform information, and updating system firmware and software, an external system such as a Midframe and Entry-Level Service Processor (SP) is strongly recommended to provide a centralized location for these functions.

An SP (which is sometimes known as an Administrative Workstation) is helpful because of the need to access and monitor the SC on a regular basis (console output or SC platform messages) and because the SC attempts to log messages to an external host (by using SNMP or *syslog*).

Choosing an Appropriate SP:

This article does not recommend a particular type of system to use an a SP.

Each site will have different needs to address, for instance the total number of systems for the SP to monitor, or whether Sun MC software will be utilized. *Syslog*(3) and *sclogger*, do not require as many system resources to monitor hosts as does the Sun MC software. See the section of this article relating to Sun MC for more information on system requirements.

When choosing an appropriate SP (or SPs), some additional capabilities need to be considered, such as how to access the serial ports on multiple SCs and how many devices need to be monitored on the same system.

This section contains descriptions of how to configure the Midframe and Entry-Level Service Processor (SP):

- Configuring the SP to Receive Log Messages
- Sun MC software
- Sun Explorer
- Monitoring Domain Consoles

Configuring the SP to receive Log Messages

There are several places information can come from to help diagnose a problem. The domain's operating system and the Sun Fire system controller are both capable of providing messages about system errors. Many error messages show up in only one of those places, while others are seen from both. Since they each have their own view of the problem, sometimes the data provided by one is better at diagnosing the error.

Many times it is necessary to see the error messages from both sources to get the full view of a problem. From a support standpoint, having to request additional data takes very valuable time in a situation where time is critical. So, when a system error is encountered, it is best to gather data from both the SC and the domain OS because only collecting data from one source is not always sufficient.

In early versions of the SC hardware, there was a very small amount of memory for storing errors. In certain cases, it was possible for critical error messages to be lost as a result since the SC only retained the most recent error messages. With the newer system controller, called the SC v2 (version 2), additional memory was added to store additional messages. The additional memory helps minimize the chance that messages are lost.

To check if you have an SC v2 in your Entry-Level server configuration, look for the “V2” notation in the following output:

```
lom> showsc
SC: SSC1
System Controller V2
Clock failover disabled.
 ...remainder of output truncated...
```

To check if you have an SC v2 in your Midframe server configuration, look for System Controller V2 in the following output:

```
sf4900-sc0:SC> showboards
Slot     Pwr Component Type                 State      Status
Domain
----     --- --------------                 -----      ------
------
SSC0     On  System Controller V2           Main       Passed -

SSC1     On  Present                        Spare     -     -
 ...remainder of output truncated...
```

One way to assure that older messages are not lost, regardless of which SC version is being used, is to configure a loghost. Setting up an loghost will cause the SC to forward error messages to this host, where it will be stored in the remote server's messages file.

Note – Entry-Level server is unable to be configured to utilize a loghost. This section regarding the loghost is applicable only to Midframe servers.

The SP provides a centralized and secured access point for logging messages. However, because of the limited number of *syslog* logging facilities available per host, it might not be possible to monitor as many systems as a single, larger, Sun MC server can without generating large unmanageable log files.

- Many people have solved this problem with shell scripts that parse this large log file and sort the logs into files based on the host they came from.
    - The scripting method is prone to many errors, such as updating the script for each new platform to be monitored.
- Another way to accomplish the logging of several systems to a single SP is the addition of the Sun Fire System Controller Logger package (*sclogger*).
    - *sclogger* is available at http://www.sun.com/download/products.xml?id=4068a5fd
    - See Document ID 1008676.1 '*Best Practices' and configuring loghost on Sun Fire[TM] 3800,4800,4900,6800, and E6900 servers* for more information.

sclogger can monitor several machines and SCs while only using one *syslog* facility. *Syslog* forwards the messages to a named pipe where it is sorted and placed in a file that is named according to the domain or sc that it was received from. *sclogger* creates a directory on the SP called /var/log/sunfire.

The naming convention for the files created in /var/log/sunfire are documented in the table below:

messages.SCNAME	platform messages
messages.SCNAME.Domain-A	domain A messages
messages.SCNAME.Domain-B	domain B messages
messages.SCNAME.Domain-C	domain C messages
messages.SCNAME.Domain-D	domain D messages

Sun MC Software

A Sun MC software server normally requires a higher level of system resources, such as a correctly configured dual processor system capable of having 1 gigabyte of RAM or more. However, a Sun MC software server also has a greater capability to monitor and administer a large number of systems. Whether or not the Sun MC software proxy agent is running on the same host as the server agent might influence the Sun MC software server configuration.

The Sun MC software should be implemented with two systems. One small system should act as a proxy agent for one or more Sun Fire platforms, and the second system should be a larger Sun MC software server that is tasked with monitoring the entire network. This configuration provides additional monitoring capabilities in case the system containing the Sun MC software server becomes unavailable. It also provides flexibility in the SP and security configuration.

To be able to monitor SNMP traps generated by the SC, you must install the Sun MC 3.0 Platform Update 1, or higher. This version of Sun MC is available with the Solaris 8 OE 04/01 release. Currently, the Sun MC software is the only package that can understand the SNMP traps generated by the SC. MIBS information is not publicly available.

Preparing for Firmware Updates

For purposes of firmware updates to the SC, you must set up an FTP or HTTP service on the SP. You can set up an anonymous FTP server by following the instructions in the *ftpd*(1M) man page, or you can use normal FTP by specifying a user and password in the FTP URL.

If the SP uses the Solaris 8 OE or higher, a version of the Apache Web server is provided with the Solaris OE, which you can use to provide HTTP services. Because the HTTP service is more configurable than the FTP service and because it may be restricted to listen only on certain network interfaces, the HTTP can have less of a security impact than FTP.

> **Note** - It's a good idea to execute an SC reboot prior to the *flashupdate*. This assures the SC is already able to successfully boot prior to the upgrade.

It's a good idea to execute the *flashupdate* via the serial port connection to the SC or at least have a serial port connection open to the SC when executing the *flashupdate* procedure. An SC reboot is part of the upgrade procedure. If connected via the network interface, the reboot will disconnect this connection while the network is cycled during the reboot process. If a problem occurs during the reboot, you will be "blind" to it during this period of time unless you have a serial port connection active.

A typical *flashupdate* command for Midframe server looks like this (on the MAIN SC):

```
sc0:SC>flashupdate -f ftp://anonymous:ftp-
user@01.23.45.67//pub/114527-15 all rtos
```

An Entry-Level SC firmware update can be executed using *flashupdate* from the System Controller's lom prompt (identical process to Midframe server) or via the *Lom -G* method from the SP (assuming lom packages are installed on the SP). The *Lom -G* method is detailed in Document ID 1003856.1 but not shown in this document.

Below is an example Entry-Level upgrade utilizing *flashupdate* and this method has historically proven to be less problematic then the *Lom -G* method:

```
lom>flashupdate -f ftp://anonymous:ftp-
user@01.23.45.67//pub/114527-15 all rtos
```

You can install the operating system for Sun Fire domains either from an attached DVD-ROM drive or over the network from a Solaris JumpStart" software server. The function of a JumpStart software server may also be well suited for an SP. Detailed instructions for setting up a Solaris JumpStart software server can be found in the Solaris OE systems administration guides.

Explorer Data Collector

After completing the initial installation of a Sun Fire server, you should install the *Explorer* software utility on the domain(s) and the SP. You should also set it up to periodically collect system configuration information and error messages.

Explorer can not be installed on the SCs themselves, since the SCs do not run the Solaris OE which the tool requires. Instead, extended options to the *explorer* command are necessary to collect SC data when the tool is executed from a network attached system (such as the SP).

> **Note** - See Document ID 1002383.1 *Sun[TM] Explorer Data Collector* for updates to the *Explorer* software including download links and command usage information.

It is strongly suggested that the latest *explorer* version be utilized, as enhancements are being added to the product all the time. If possible, the output from the *Explorer* should be automatically sent to the *Explorer* software database at the email address specified when you set up the software.

The following command extended options gather diagnostic information from the SC(s). You should execute it from the SP since this has access to the SC(s) on the private net. Use of the following command assumes that the *Explorer* software has already been installed on the system in the default location, */opt/SUNWexplo* (If installed in a different directory, adjust the command appropriately).

For Midframe servers, execute (as root):

```
# /opt/SUNWexplo/bin/explorer -w fru,scextended,default
```

For Entry-Level servers, execute (as root):

```
# /opt/SUNWexplo/bin/explorer -w default,1280extended,fru
```

See Document ID 1019066.1 if you require additional information on executing Explorer on Sun Fire Midframe and Entry-Level servers.

When you execute this command from an SP, the *Explorer* software will collect data from the SP and the SC(s) that the SP manages. To collect data from the SC, the *Explorer* software uses a telnet or SSH connection. Therefore, the SP must be able to establish a telnet or ssh session to the SC prior to executing the *Explorer* script. On system controllers utilizing SSH, *explorer* version 4.3 or higher must be used.

The above examples execute *Explorer* from an interactive session and the *scextended* or *1280extended* option will prompt the user for a hostname and password for each SC.

To automate the process, so that *Explorer* can be run non-interactively through *crontab*(1) and forwarded to Oracle support, an administrator can put login information into a file on the SP or host where Explorer is being executed from, */etc/opt/SUNWexplo/scinput.tx*t.

The format for the *scinput.txt* file is basically, “Hostname Password” as shown below:

```
# more /etc/opt/SUNWexplo/scinput.txt
# Input file for extended data collection
# Format is HOST PASSWORD
4800-sc0 <sc0's password >
4800-sc1 <sc1's password >
```

If security considerations prevent the automatic sending of *Explorer* software results to the *Explorer* software database, you should still install the *Explorer* software utility so that it is available to collect information in the event that service is required on the system and information needs to be collected.

If *sclogger* is implemented, it is important that *explorer* on the SP also collect this data. To automate this process, a line can be added to the */opt/SUNWexplo/tools/messages* file in *Explorer* to include the */var/log/sunfire* directory in the list of files *explorer* collect. If you are using *Explorer* 4.4 or greater, this change is not required as *Explorer* will automatically gather this data.

```
      SYSLOG=/etc/syslog.conf

      get_file "/var/adm/messages*"    messages
      get_file "/var/log/syslog"       messages
      get_file "/var/log/sunfire/*"    messages
      get_cmd  "/usr/bin/dmesg"        messages/dmesg
```

The initial installation is also a good time to record and check the system serial number, hostid, and MAC address provided with the system and to become familiar with how these values are reported by the SC *showplatform -v* command (Midframe server) or *showsc -v* (Entry-Level server). Keep this information where it can be easily accessed in case a SC replacement is required.

If *Explorer* is unable to be collected for some reason, see Document ID 1003529.1 which documents the manual commands which are required to help enable Support Services to troubleshoot your technical issue.

Monitoring Domain Consoles

It is also advantageous to keep monitoring the consoles of active domains in order to make sure no messages sent to the domain consoles are lost. Since simultaneous multiple domain console access needs to be done across the network through the System Controller, traditional logging terminal server solutions are not as suitable as they were in the past.

One potential solution is to use a software logging solution such as *conserver* which is available at http://www.conserver.com. The software's configuration file can be set up to directly telnet to specific ports on multiple SCs to access domain consoles and record their activities. To directly access Midframe domains A-D, telnet to ports 5001-5004 respectively. SSH does not allow the ability to directly telnet to a console port directly, however, it should be possible to script the login process. conserver also allows multiple users to connect to the domain consoles without interrupting the logging.

Another solution would be to open up multiple terminal windows running the UNIX *script*(1) command through the *nohup* command which would allow for recording of console messages even if the terminal window is disconnected. This solution however does not allow for connecting to the domain console without interrupting the console logging.

Platform and Domain Administration

The Midframe SC has an administration scheme in which operations affecting the entire system are administered through a platform shell and operations affecting separate domains are administered through a domain shell. The Entry-Level server really doesn't have a "domain shell", because there is only a single domain. You get access to the domain on Entry-Level server from the platform shell by using the lom *console* command.

The remainder of this section concentrates on the Midframe server, but where applicable Entry-Level server information will be highlighted.

This section contains general descriptions of administering the SC and detailed descriptions of the following topics:

- Monitoring Through the Serial Port, syslog, and SNMP
- Setting Up Information Recording and Logging

You can access multiple platform shells simultaneously. As previously mentioned in this document, SSH has a limit of five simultaneous connections on Midframe server and up to 2 connections after ScApp 5.20.15 on Entry-Level server. On Midframe server Telnet is capable of 12 connections. Those connections can be used for any combination of platform and domain shells.

The platform shell can view the status of any component within the system and can also control its allocation. The platform shell also controls the access to resources by allowing the administrator to create Access Control Lists (ACLs). The *setupplatform -p acl* command is used to control access to the various system resources. This command is not available on Entry-Level server since there is only a single domain (thus no reason to allocate system resources to various domains).

While the platform shell manages and administers overall system resources, domain operations, such as the turning of the virtual keyswitch, are controlled in the Midframe domain shell. The domain shell can only access resources specified in it's ACL. Also, only one shell per domain can be active at any time. The ACL restricts the domain shell so that it views only the resources that the domain is currently using, resources that are allocated to the domain, or any resources that are unassigned on the platform and are available to the domain according to the ACL.

This setup allows the ability to restrict the access to the platform shell (and administration of the overall system resources) to a group of administrators, who are separate from a group of administrators for the domains. You can control access to platform and domain shells by using passwords that you can set and change by using the *password* command on the SC.

From the platform shell, you can set or change the platform and domain shell passwords. From a domain shell, you can change only the password of that domain. Because the platform has additional privileges, its password should be different from those selected for the domains.

Monitoring Through the Serial Port, syslog, and SNMP

Administration of a Sun Fire server is designed to be performed primarily through the SC, which can be accessed in two ways:

- RS-232 serial port.
- 10/100BASE-T Ethernet.

Both ports should remain available at all times, and you should monitor the platform console and all of the domain consoles.

After the initial platform setup, the serial port performs an important role in the administration of the Sun Fire server. First, it can provide a connection to the system controller in the event of a network outage. Second, if the console log is saved with a capture mechanism like *script*(1) in the Solaris Operating Environment, that data can also be used in problem diagnosis. This is especially useful in diagnosing problems with the system controller itself, since the System Controller's POST messages go to the serial port. Finally, during a firmware upgrade network connectivity is lost, and if something goes wrong with a firmware update the serial port is also the only source of diagnostic information available when the network is down.

For routine tasks, the preferred method of accessing the SC is the Ethernet interface. In addition to providing multiple high-speed shell connections, the Ethernet interface on the SC enables you to set up *syslog*(3) and SNMP messages to be sent to a designated administration platform. The Ethernet interface is required for performing firmware updates on the system and for saving and restoring the SC configuration information. You should enable and configure both *syslog* and SNMP facilities; However, you should record system consoles by using a mechanism such as *script*(1M) because not all of the messages can be logged with *syslog* or SNMP.

Note - SNMP should not be enabled unless a Sun MC server has been configured to support the system.

Setting Up Information Recording and Logging

You should perform the setup of information recording and logging during the initial platform setup. Although you can also make these changes at other times, you should set up *syslog*(3) to record the information to a central location so that information can be quickly located in the event of a problem and to prevent the SC message buffer from being overwritten.

Prior to the introduction of the SCv2 (System Controller version 2), all system controllers had a limited amount of memory. All messages were in volatile memory (*showerrorbuffer*), and were lost when the SC lost power or was rebooted. With the introduction of the SCv2, dynamic memory was increased significantly, and non-volatile memory was also added. This allows SCv2 to store more messages, and retain those messages across reboots (s*howerrorbuffer -p*). However, even with the additional resources, it is still strongly recommended to set up *syslog* to an SP.

Note - The SCv2 was discussed in the section Configuring the SP to receive Log Messages and provides instructions on how to determine which version of SC is installed in your configuration.

On Midframe server, when setting up the platform or domain using the *setupplatform* or *setupdomain*, respectively, you are prompted for a *syslog*(3) loghost. You can supply a *syslog* loghost by using an IP address or hostname, as well as a facility level.

The following example shows how to configure the loghost on a Midframe server. The domain log configuration has the same prompts as what is shown below:

```
sf4800-sc0:SC> setupplatform -p loghost

Loghosts
--------
Loghost [0.0.0.0]: 10.1.12.13
Log Facility [local0]:

sf4800-sc0:SC>
```

Corresponding changes need to be made to the */etc/syslog.conf* file on the *syslog* host or on the SP. You can find further information on the configuration of *syslog* in the Solaris OE system administration guides in the Solaris OE System Administrator AnswerBook2 collection.

Based on the number of systems and *syslog* devices that a single loghost will be monitoring, you should establish a convention to maximize use of the limited number of *syslog* facilities. There are only eight *syslog* facilities available for users in the Solaris OE, so an administrator can quickly run out of unique *syslog* facilities if managing multiple platforms.

Organization of message logging is important to enable administrators to quickly find the desired information.

- A good way to organize *syslog* logging is to assign the *local0* facility to all platform messages.
- Then assign *local 1-4* to Midframe domains A through D, respectively.
- The *syslog* facility in the Solaris 8 OE identifies each *syslog* entry with the originating hostname and *syslog* facility. This identification makes it easy to quickly separate messages coming from different hosts.

> **Note** - All of the issues associated with the limited number of *syslog* are not applicable to systems running *sclogger*.
>
> *Sclogger* allows the usage of one log facility to handle many system controllers and domains, which is another reason why utilizing it is one of the recommendations in this document.

When setting up the platform, you can configure the SC to interface with the latest versions of the Sun MC software through SNMP. This improves the monitoring and administration capabilities of the platform. It is strongly recommended that the default community strings be changed during installation for security reasons.

The following values for platform and domain public and private community strings are set by default.

```
Platform Public: P-public
Platform Private: P-private
Domain A Public: A-public
Domain A Private: A-private
Domain B Public: B-public
Domain B Private: B-private
Domain C Public: C-public
Domain C Private: C-private
Domain D Public: D-public
Domain D Private: D-private
```

SNMP must be enabled on the Midframe platform by using the *setupplatform* command before SNMP can be enabled on any of the domains.

The following shows an example of the *setupplatform* command. The *setupdomain* command is very similar except the community strings will be *<domain>-public/private*.

```
sf4800-sc0:SC> setupplatform -p snmp

SNMP
----
Platform Description [Sun Fire 4800]:
Platform Contact [email address]:
Platform Location [Lab]:

Do not enable SNMP Agent unless you use Sun Management Center
software.

Enable SNMP Agent? [no]: yes
Trap Hosts [10.1.9.220]:
Public Community String []: P-public
Private Community String []: P-private

sf4800-sc0:SC>
```

For more information on how to set up SNMP, refer to the System Administration Manuals or the security articles by Alex Noordergraaf and Tony M. Benson at the Sun BluePrints Online website.

The port for the *Trap Hosts* value can be entered in the form of *hostname:port* in firmware 5.13.0, or higher. Do not change the port setting unless specifically instructed to do so for the installation of other software on the trap host. To find additional information on configuring the Sun MC software, refer to the Sun MC software documentation at http://docs.sun.com

In addition to setting up *syslog*(3) and SNMP, you should monitor domain console sessions in a manner similar to that described for the platform and the serial port connection. While the SC has a buffer for each domain shell's messages, the SC will not send domain console messages or error messages generated by the Solaris OE (such as panic strings and watchdog reset information) to an external log host. Therefore, if you do not constantly monitor the domain consoles, critical messages and valuable diagnostic information could be lost in the event of a failure. With multiple domains to monitor, you should access the domain shells through the Ethernet port because it allows multiple connections.

Platform Security

System security is important for any computing system, and the Sun Fire server is no exception. This section contains descriptions of the following basic platform security topics:

- Recommendations for User Authorization
- Serial Port Access
- Telnet and Secure Shell Sessions
- Keyswitch Settings (Midframe Server only)

Because the Sun Fire domains run the same Solaris OE as other systems, basic security practices that apply to any Solaris OE system also apply to the Sun Fire servers. These practices include regular patch maintenance, stopping unnecessary network services, and choosing good passwords to prevent account abuse. Even though the SC does not run the Solaris OE, many of the same concepts still apply to its administration, such as regular patching, and password maintenance. The SC is key to the operation of the Sun Fire platform, and the protection of the SC really represents the protection of the whole platform.

Great care should be taken in the setup of the system to ensure that access is restricted only to authorized personnel. Failure to properly secure access to the SC can adversely affect the operation of the Sun Fire server.

Recommendations for User Authorization

To help deter unauthorized access, passwords should be set on the SC platform and domain shells. You can set these passwords by using the *password* command.

A platform administrator may also set domain shell passwords using with the *-d <ID>* option from the SC platform shell. The *password* command issued from a domain shell, can only be used to change the password for that particular domain.

The SC does not enforce password standards, and it maintains no records of failed login attempts or the source of the login attempts. Given the importance of these passwords, especially in terms of restricting access to critical system resources, choose passwords that cannot be easily guessed or discovered using a brute-force attack. Passwords for the SC can and should be longer than eight characters. This ability encourages the use of pass-phrases of 16 characters as a minimum, with mixed characters, numbers and punctuation marks.

> **Note** - It is strongly recommended that passwords for platform access and superuser (root) access on the domains be different.

Serial Port Access

It is extremely important to carefully control access to the SC serial port.

The serial port is the lowest level of access to the SC. An unprotected serial port could have serious consequences to the operation of the Sun Fire system because access to the serial port can compromise the application that runs on the SC. Because that application controls the entire Sun Fire system, improper access could result in undesired changes to critical settings or in system outages.

Attach the serial port connection of the SC to a password-controlled terminal server or directly to the SP where access can be monitored and logged.

Telnet and Secure Shell Sessions

Prior to 5.16.0, there was no facility for an encrypted network session between a management host and the system controller. The only network option available was to utilize telnet for connecting to the SC. Since 5.16.0, the administrator has had a choice of protocols, either telnet or secure shell (SSH).

<u>The Telnet Option</u>

The telnet option, is insecure, in that the text typed on the management host goes across the network in an unencrypted format. That traffic may be captured by utilities such as snoop(1M) from the Solaris Operating Environment.

For this reason, if the telnet protocol is chosen, it is even more important that the SP and the SCs be placed on a private, switched, non-routed network to assure the configuration is secure.

The SP should be the only way to access the SC(s), and access to the SP itself should be carefully secured, monitored, and encrypted if possible.

- Assuming the network is secure, there is no reason why telnet should not be utilized. It is a proven and reliable method to access the SC.
- Also, in the event that you have version 1 SCs (SCv1) it is actually recommended to utilize telnet to avoid any performance related issues. (which SSH can cause).

> In summary, telnet provides a proven and reliable method to connect to the Midframe and Entry-Level SC, assuming the network itself is private and secure. Utilize this method when an encrypted connection is not required and when the SC is version 1.

<u>Configuring the SC to utilize telnet:</u>

- In order to configure an Entry-Level server to utilize telnet, you use the lom command *setupnetwork*.
- On Midframe server, you configure the system to utilize telnet by using the command *setupplatform -p network*.

An example of these commands are shown in the next section, *The SSH Option*. The command is identical whether you choose SSH or telnet.

The SSH Option

The SSH option is more secure, as the traffic goes across the network in an encrypted format, and is unreadable by utilities such as snoop(1M). For configurations where the SC network is not truly private, or for sites that demand utilizing a secure communication method, this option is suggested.

The enhanced security comes at a price and does burden the SCs resources more then telnet. As a result, SSH should only be when version2 (SCv2) SCs are installed (v2 have increased memory). Using SSH in SCv1 configurations can result in performance problems which can potentially be severe.

Note - See Configuring the SP to receive Log Messages to identify the SC version installed.

Even with the advantage of enhanced security, SSH does have some disadvantages:

- The number of SSH connections is limited to 5 simultaneous ssh connections on Midframe servers. On Entry-Level server, beginning in ScApp 5.20.15, the SC ignores attempts to initiate more than 2 SSH connections.
    - This allows each system to have one session for each possible domain, and another for the SC. This can be a disadvantage in environments with many administrators.
    - An idle timeout can be set when configuring the remote access type to save resources for others to connect. Idle timeout is also available in telnet, as a security precaution.
- As previously mentioned, SSH utilizes more SC resources then telnet and should not be utilized on SCv1 configurations.

Explorer software has been enhanced to be able to use use ssh to collect *scextended* or *1280extended* data. The minimum required version of Explorer that supports SSH is 4.3.

In summary, SSH provides a reliable and secure method to connect to the Midframe and Entry-Level SC, assuming the SC is version 2 (SCv2). It does utilize more SC resources then telnet so it should not be used on SCv1 configurations. It is suggested for use when the network is not a private and/or the site's security requirements dictate it's use.

The first time SSH is enabled, the SC will automatically run *ssh-keygen* and generate a key which much be accepted the first time a connection is made. If in the future the key needs to be changed, *ssh-keygen* can be run again and the SC rebooted to use the new key.

The following configures SSH on an Entry-Level server (*telnet* configured via same command):

```
lom> setupnetwork
Network Configuration
---------------------
Is the system controller on a network? [no]: yes
Use DHCP or static network settings? [DHCP]: static
Hostname []: somename
IP Address []: 129.xxx.xxx.xxx
Netmask [255.255.255.0]: 255.255.255.0
Gateway []: 129.xxx.xxx.xxx
DNS Domain []: somewhere.nowhere.com
Primary DNS Server []: 129.xxx.xxx.xxx
Secondary DNS Server []: 129.xxx.xxx.xxx
Connection type (ssh, telnet, none) [none]: ssh
Rebooting the SC is required for changes in network settings to
take effect.
Lom>
```

The following configures SSH on an Midframe server (*telnet* configured via same command):

```
sf4800-sc0:SC> setupplatform -p network

Network Configuration
---------------------
Is the system controller on a network? [yes]:
Use DHCP or static network settings? [static]:
Hostname [sf4800-sc0]:
IP Address [10.1.9.230]:
Netmask [255.255.255.0]:
Gateway [10.1.9.253]:
DNS Domain [sun.com]:
Primary DNS Server [129.147.62.1]:
Secondary DNS Server [129.153.224.10]:
To enable remote access to the system controller, select "ssh"
or "telnet".
Connection type (ssh, telnet, none) [telnet]: ssh
Rebooting the SC is required for changes in the above network
settings to take effect.

Idle connection timeout (in minutes; 0 means no timeout) [0]:

sf4800-sc0:SC>
```

Keyswitch Settings (Midframe Server Only)

During normal operations, it is recommended that the virtual domain keyswitch be set to secure by using the following command:

```
      sf4800-sc0:A> setkeyswitch secure
```

Setting the keyswitch to secure prevents firmware updates to I/O and system boards in the domain. It also prevents an operator from sending a break command to the running domain and accidentally terminating the Solaris OE. The keyswitch needs to be changed to the on position before sending a break command, sending a reset, or updating firmware. Only domain administrators with access to the domain shell can set the keyswitch to the secure position.

Entry-Level servers have secure mode as an option that can be set via the *setupsc* command.

Error Analysis, Diagnosis and Recovery

Sun Fire servers provide significantly enhanced diagnostics capabilities. In the event of a system fault, the system will provide data for both software and hardware failures that you can use to help determine the source of the fault. Errors can be generated and logged to several places, depending on the type of error. Use a utility such as *Explorer* to gather data from the system so that all error messages can be collected in a central location.

It is important to get an *Explorer* (with *scextendeded* or *1280extended* option depending on the type of server) run immediately after a failure. The storage area on the system controllers is limited, and other new errors may overwrite the original error that caused the outage. The error logs are also reset on system controller reboots, so the errors may be lost in a platform power cycle or SC reboot. SCv2 system controllers maintain the errors across reboots allowing persistent logging. SCv2 also has additional storage for more errors, but the space is not unlimited, and a quick *Explorer* is always recommended.

With firmware 5.15.0 and higher, the platform is capable of automatically diagnosing many hardware failures. After diagnosing the error, the SC's Auto Diagnose Engine (ADE) is capable of acting on the diagnosis, and disabling hardware to increase the availability of the system. Please refer to the Sun Blueprint "Sun Fire Midrange Server Auto Diagnosis and Recovery" available from http://www.sun.com/blueprints for more information.

After the appropriate error messages have been analyzed by the diagnosis engine, the source of the error is isolated as far as possible. Based on the results of the diagnosis, attempt to verify the failure using component blacklisting, segmenting, or Dynamic Reconfiguration before attempting to remove or replace components in the case of a suspected hardware problem.

After root cause of the failure has been determined, the platform is capable of having many components replaced with a running domain. This is accomplished through the use of Dynamic Reconfiguration (DR).

Maintenance Functions

There are maintenance functions that you must perform on a regular basis. The following functions are described in this section:

- Periodic Server Maintenance
- Restoring the Sun Fire SC Configuration
- Updating the Firmware and Real Time Operating System
- Removing the SC from Platform Use

Periodic Server Maintenance

It is important to perform the periodic server maintenance on the Sun Fire Midframe and Entry-Level server as documented in each server's System Service Manual.

Periodic maintenance should be performed every 3-6 months and is to be executed by customers (not Support Personnel).

This maintenance relates to air filter or air intake inspection depending on the system type.

Midframe servers have instructions documented in their particular System Service Manual, (Sun Fire 3800, 4800, 4810, & 6800, see Chapter 13 and Sun Fire E4900/E6900, see Chapter 12).

Entry-Level servers require the following air filter recommendations be executed immediately per Sun Alert 273971:

- Sun Fire v1280 & E2900 systems - REMOVE the LEFT air filter on the front door.
    - Reference the Sun Fire v1280 and E2900 Service Manual; Chapter 2.11 (page 46).
- Netra 1280 & Netra 1290 systems should immediately inspect, clean and/or replace the LEFT air filter on the front door. The Part Number for the filter kit is X6806A-Z.
    - Reference the Netra 1280 System Service Manual, Chapter 2.10 (page 48) or the Netra 1290 System Service Manual, Chapter C.1.

Restoring the Sun Fire SC Configuration

If an SC fails, you might need to manually restore the SC configuration information. After the configuration of the platform has been completed, including setting up domains and segments, create a backup of your SC configuration so that a quick restoration will be possible.

> **Note** – Entry-Level server does not utilize *dumpconfig* for backup purposes. A backup copy of critical NVRAM data is automatically copied to the System Configuration Card (SCC) and kept in sync. See the Appendix section on the SCC for more details.

The following shows an example of how to create a backup of the Sun Fire SC configuration on the SP.

```
sf4800-sc0:SC>dumpconfig -f ftp://<ftpusr>:<ftpuser
pswrd>@sp/dumps
```

For security purposes the dump files are encrypted so that important configuration information cannot be read out of the dump file. This security enhancement was added in SC firmware version 5.15.3

The following shows an example of how to restore a Sun Fire SC configuration from the SP.

```
sf4800-sc0:SC>restoreconfig -f ftp://<ftpusr>:<ftpuser
pswrd>@sp/dumps
```

Updating the Firmware and Real Time Operating System

Periodically, updates to the SC firmware and RTOS will be made available. These updates often contain critical bug fixes and functionality enhancements to the SC and should be applied as part of a regular patch maintenance routine.

> **Caution** - ScApp 5.20.x (available via patch 114527) is the most recent version of ScApp. A seemingly "newer" version of ScApp, 5.21.x, was released to provide support for a hardware option that was obsoleted and never actually Revenue Released. As a result, ScApp 5.21.x has been obsoleted by 5.20.11 and higher.
>
> **ScApp 5.20.x will always be the latest version of the firmware, so you are urged to maintain this revision on these servers – and avoid utilizing ScApp 5.21.x.**

Before applying a firmware update it is a good idea to reboot the SC prior to any upgrade. This validates that the SC is bootable prior to an upgrade in the event a problem occurs during or after the firmware upgrade itself. Secondly, carefully read the *README, Install.info* file, and *Release Notes* in the patch package before proceeding with the update to familiarize yourself with the procedure. Backing up the SC configuration before updating is also strongly recommended (Midframe only).

Also be sure to perform the firmware updates regularly, and for Sun Fire systems which have dual SCs, remember to update the firmware on both SCs (per the patch *install.info* file) and all the boards.

> **Caution** - You must follow the instructions in the *Install.info* and the *README* file, included with each patch release, to ensure that both ScApp and RTOS are updated together. ScApp should only be run with the accompanying version of RTOS. Upgrading from some versions of the firmware may require that the upgrade to the SCs be done in a specific order.

Be sure to read and follow the instructions carefully. It is important to follow the instruction carefully, and not omit any steps such as the *setkeyswitch* commands, which are critical to a successful installation.

You can retrieve updates from http://sunsolve.sun.com

You should also have copies of important SC parameters that are displayed by the *showplatform* and *showboards* commands, as well as those displayed by the OpenBoot" PROM commands *printenv* and *devalias*.

Removing the SC from Platform Use

If an SC needs to be removed for maintenance purposes, you must follow the instructions for SC replacement that are specific for the version of firmware on the SCs. For specific instructions, refer to the Systems Platform Administration Manual for the appropriate system in question.

In general, an SC should never be removed from a system unless the SC can be powered off, either by using the *poweroff SSCx* command or by removing the power to the entire platform.

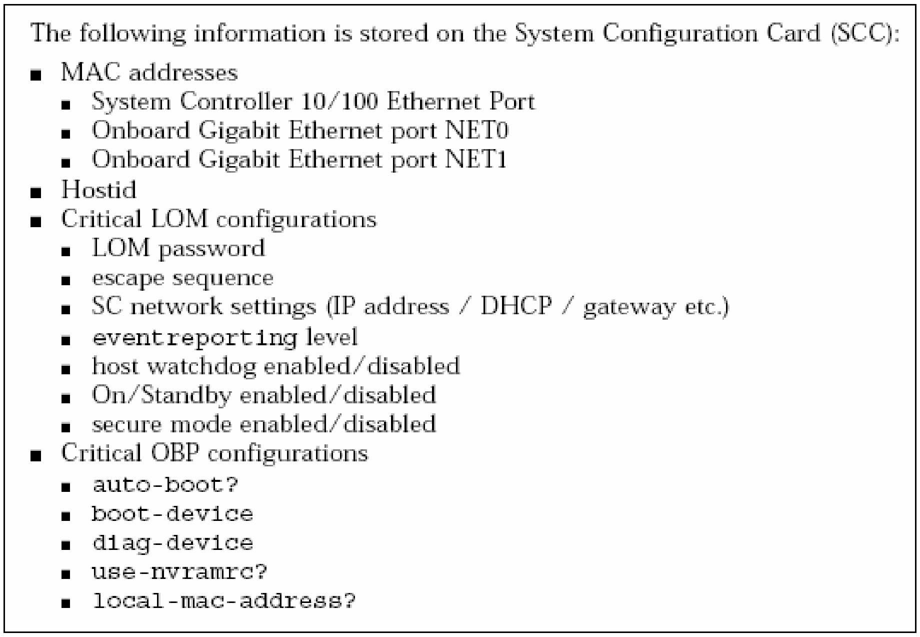
Appendix

Entry-Level Server System Configuration Card

Entry-Level servers do not utilize *dumpconfig* for backup purposes (as is the case on Midframe servers). A backup copy of critical NVRAM data is automatically copied to the System Configuration Card (SCC) and kept in sync.

- If the IB_SSC is replaced, a *restoreconfig* occurs automatically from the SCC to the new NVRAM.
- If the SCC is replaced, a *restoreconfig* occurs automatically from the NVRAM to the SCC.
- Not all data is backed up, just the critical data (see the list of information below).

The contents of an SCC card on Entry-Level server (which are synced automatically when an SCC or an IB_SSC is replaced). This card is inserted into the SCC Card Reader which is located on the front of the Entry-Level server chassis.



The following information is stored on the System Configuration Card (SCC):

- MAC addresses
  - System Controller 10/100 Ethernet Port
  - Onboard Gigabit Ethernet port NET0
  - Onboard Gigabit Ethernet port NET1
- Hostid
- Critical LOM configurations
  - LOM password
  - escape sequence
  - SC network settings (IP address / DHCP / gateway etc.)
  - `eventreporting` level
  - host watchdog enabled/disabled
  - On/Standby enabled/disabled
  - secure mode enabled/disabled
- Critical OBP configurations
  - `auto-boot?`
  - `boot-device`
  - `diag-device`
  - `use-nvramrc?`
  - `local-mac-address?`

References

The following sources were referenced in this article (Available for download via https://support.oracle.com and from http://docs.sun.com):

- Sun Fire 6800/4810/4800/3800 System Controller Command Reference Manual
- Sun Fire 6800/4810/4800/3800 Systems Service Manual
- Sun Management Center 3.0 Software Installation Guide
- Sun Management Center 3.0 Supplement for Sun Fire 6800, 4810, 4800, and 3800 Systems
- Securing the Sun Fire Midframe System Controller (Updated for SC Firmware 5.13.0) , Sun BluePrints Online, September 2001
- Sunfire Midrange Server Auto Diagnosis and Recovery
- Sun Fire 3800-6800 Server Dynamic Reconfiguration
- Sun Explorer Data Collector
- Solaris Security Toolkit (formerly known as jass)
- Sun Fire™ Entry-Level Midrange System Controller Command Reference Manual
- Sun Fire™ Entry-Level Midrange System Administration Guide

About the Authors

Joshua Freeman is a member of Oracle's Technical Support organization working in the Enterprise Server Group. He is currently focused on content management and product technical support for Oracle's Enterprise Servers and previously worked for Sun Enterprise Services in a variety of product technical support roles for more then 10 years.

Ken Kambic is a member of Oracle's Technical Support organization working in the Enterprise Server Group. He is currently focused on resolving issues with Oracle's Enterprise Servers and previously worked for Sun Enterprise Services in a various System Support Engineer roles for the last 16 years, and before that as a systems administrator for a variety of UNIX systems.

Paul Griffin is a member of Oracle's Technical Support organization working in the Enterprise Server Group. He is currently focused on resolving issues with Oracle's Enterprise Servers where he has a penchant towards resolving mechanical issues related to field replacement procedures. During his 15 years with Oracle, Paul has worked as a Field Engineer specializing in Workgroup Servers and Fault Tolerant systems followed by various technical support roles. Paul began his career as an electronics engineer repairing memory boards for early generation mini-computers.

James Hsieh is a member of Oracle's Hardware Engineering Team. Prior to his current position with Oracle, James worked in Sun Enterprise Services in various System Support Engineer roles. Before Sun/Oracle, James had over thirteen years of software engineer and systems administration experience on UNIX and high end server configurations.

Conclusion

The Sun Fire Midframe and Entry-Level server has undergone many improvements since the last revision of this document for firmware 5.18.x. The purpose of this document is to give guidance to the reader on the application of many of those improvements, and describe how to implement the new features to improve the overall system reliability, availability, and serviceability. To achieve the highest degree of availability it is important to develop a well planned and efficient administrative environment. With proper advanced planning many failures can be eliminated, or their impact minimized.

ORACLE®

An Oracle White Paper—Sun Fire Midframe & Entry-Level Servers Best Practices Update for Firmware 5.20.x
July 2010

Author: Joshua Freeman
Contributing Authors: James Hsieh, Ken Kambic, & Paul Griffin

June 2010 PN: A01-0002-10

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

SOFTWARE. HARDWARE. COMPLETE.