Sun Fire™ Midrange Server Updated Best Practices for Firmware 5.18.x

Ken Kambic, PTS Engineering Group
James Hsieh, PTS Engineering Group

Sun BluePrints™ OnLine — May 2005

Revision 3.1

http://www.sun.com/blueprints

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95045 U.S.A.
650 960-1300

Part No. 819-2681-10
Revision 3.1, 4/29/05
Edition: May 2005

Please
Recycle

Sun Fire Midrange Servers Updated Best Practices for Firmware 5.18.x

Sun has introduced many improvements to the Sun Fire Midrange servers (Sun Fire E6900, E4900, 6800, 4810, 4800, and 3800 systems) since the last revision of this document for firmware 5.13.x. The purpose of this document is to provide guidance to system administrators on how to apply many of those improvements, and to describe how to implement the new features to improve system reliability, availability, and serviceability.

To achieve the highest degree of availability it is important to develop a well planned and efficient administrative environment. The best practices outlined in this article can help administrators properly plan tasks in advance, thus eliminating many failures or minimizing their impact.

While much of this document is new material, this article revisits the best practices presented in the previous version of this document:

- Platform configuration
- Platform and domain administration
- Platform security
- Error analysis, diagnosis, and recovery
- System controller maintenance procedures

The following sections detail best practices for new enhancements in firmware since version 5.13.x

- Changing POST levels and other settings
- Configuring log messages on the midframe service processor
- Console server
- Configuring the Sun™ Explorer software
- Telnet and Secure Shell Sessions (SSH)

Background Information

This section provides some background information on understanding the system controller, updating the firmware, the midframe service processor (MSP), and other topics that are discussed in this paper.

System Controller

The system controller (SC) is an embedded system built into the Sun Fire midrange server chassis that runs a real time operating system (RTOS) and is responsible for configuring and monitoring the platform. It is accessed using either serial or Ethernet connections. It is the focal point for the platform and domain configuration and management. It is also used to connect to the domain consoles.When the system is powered on, the system controller boots the real-time operating system and starts the System Controller Application (ScApp).

Additional information about the SC is available in the *Sun Fire 6800/4810/4800/3800 Platform Administration Manual* and the *Sun Fire 6800/4810/4800/3800 System Controller Command Reference Manual*.

Midframe Service Processor

A midframe service processor (MSP) is a separate server that is used to provide services to the SC, including:

- Encrypted access point to SC via SSH
- `syslog` server
- Flash update services
- `dumpconfig` and `restoreconfig` services

It is recommended that the SC be configured to use an external MSP server. A system controller can function without a MSP, but some SC functionality and monitoring capabilities are not available without a MSP. These include flash updates to the SC, `syslog` message logging, and configuration backup through `dumpconfig`. These functions are all critical for a well administered system.

The MSP should be a dedicated server with the following recommended minimum configuration:

- Sun4U architecture or equivalent
- 8 GB disk
- 128 MB memory

- CD-ROM drive
- Ethernet card

For more information on the MSP see the Sun BluePrint: *Securing the Sun Fire Midframe System Controller, June 2002*.

Configuring the Platform

This section contains best practices for configuring the Sun Fire midrange server platform. The term platform, as used in this paper, refers to the collection of resources such as SCs, power supplies, the centerplane, and fans that are not for the exclusive use of a domain. The topics in this section include:

- Configuring the RS-232 serial port
- Configuring the Ethernet port
- Configuring a switched private network
- Configuring the Sun Fire SC failover
- Setting the date and time on the platform
- Configuring the SC to use an SNTP server
- Changing POST levels and other settings

Configuring the RS-232 Serial Port

Sun Fire servers are designed to be administered primarily through the system controller, which can be accessed through the built-in RS-232 serial port or through the 10/100BASE-T Ethernet port. The platform console is the system controller serial port, where the system controller boot messages and platform log messages are printed. It is necessary to be able to access the serial port during the initial setup of the system controller because it is the only connection on which the system controller power on self-test (SCPOST) output can be viewed. The port settings should be 9600 bps, 8-bits, no parity, and one stop bit (9600-8-N-1) to enable access by an ASCII terminal.

The serial port can also be accessed by using a network terminal server (NTS), by using the serial port on a MSP, or any other system with a serial port. For more information about the need for an MSP and on how to configure the MSP, refer to *Configuring the Midframe Service Processor* on page 12.

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 System, that data can also be used to diagnosis problems. 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, if something goes wrong with a firmware update the serial port is also the only source of control and diagnostic information.

Configuring the Ethernet Port

For routine tasks, the preferred method of accessing the SC is the Ethernet interface. The Ethernet port should be used as the primary connection path for the increased connection speed, multi session access, and logging capabilities. By default, serial connections to the SC are enabled and remote connections are disabled. To enable remote connections, use the `setupplatform` command. For details on the `setupplatform` command, refer to the command description in the *Sun Fire Midrange System Controller Command Reference Manual*.

Ethernet connections to the system controller are accomplished by using a telnet or SSH session. A 100BASE-T link is strongly recommended for the system controller Ethernet connection and required for use with Sun Management Center 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. In addition, the Ethernet port is required to perform firmware upgrades using the `flashupdate` command.

With 5.16.0 or higher the ethernet port is accessible by using SSH or telnet. SSH is a more secure communication protocol, providing session encryption across the network. SSH is discussed in more detail in the *Platform Security* section on page 20.

The system controller supports one logical connection on the serial port and multiple logical connections with a remote connection using SSH (as many as 5 connections) or telnet (as many as 12 connections) on the Ethernet port.

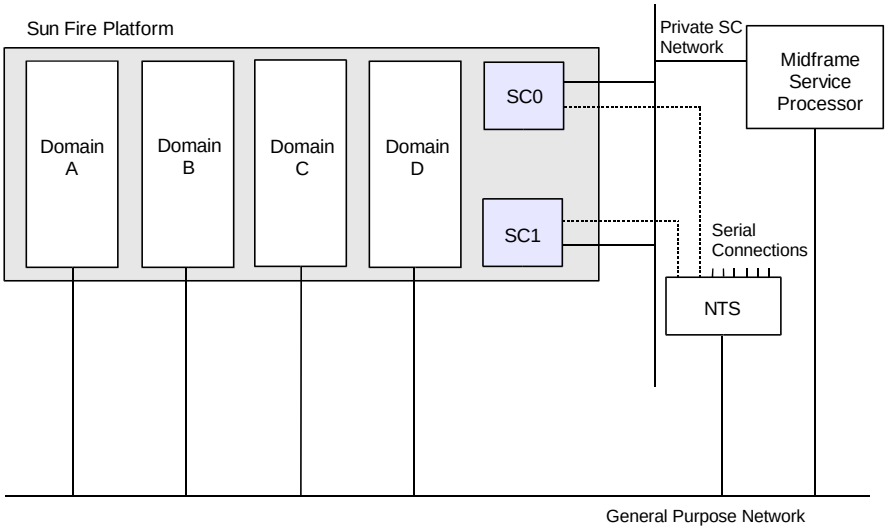
Configuring a Switched Private Network

The SC should be configured on a switched private network to isolate it from network sniffing or other network-based attacks. Each SC on the network should be assigned a separate IP address so that they do not conflict with each other on the network. If the SC failover functionality introduced in firmware 5.13.x is used, a third IP address representing the logical hostname for SC failover purposes can be assigned.

Figure 1 illustrates a simplified network topology. The MSP is also installed on the private ethernet network of the Sun Fire platform to provide administrative support functions to the Sun Fire platform and the SCs.

The serial connection in the illustration below can be a NTS if the same MSP is monitoring multiple Sun Fire platforms. If the terminal server supports encrypted logins and sessions (for example, by using SSH), the terminal server can be connected to the public Ethernet network. If `telnet` is used to access the terminal server, then all passwords are passed over the intranet in clear text, thus defeating the security features of the architecture. A terminal server is recommended to improve the ability of a single MSP to monitor multiple platforms.

FIGURE 1 Sample Network Topology



Configuring the Sun Fire SC Failover

It is recommended that two SCs be installed in a Sun Fire system to provide failover of the SC functionality and to keep the domains in the system running. Prior to firmware version 5.13.0, if the main SC suffered a failure, administrative capabilities such as the ability to access domain consoles would be unavailable. With the introduction of firmware 5.13.0, full failover is available, so if the main SC fails, the spare SC can take over administrative functions, in addition to the system clock functionality. The spare SC functions as a hot standby and is used only as a backup for the main SC.

The SC failover capability is enabled by default on Sun Fire midrange servers that have two system controllers installed. The two SCs communicate with each other by using an internal communications link. They also exchange health information and synchronize internal configuration information over the link. The SC that is acting as the main system controller generates a heartbeat. If the heartbeat unexpectedly disappears, the spare SC takes over the main SC functionality. Before enabling the SC failover feature, both SCs and all of the boards in a Sun Fire platform should be at the same firmware version. While it is possible to

have mixed versions of firmware under certain circumstances, it is highly recommended that all of the boards and the SCs use the same version of firmware. The firmware versions can be determined by using the `showboards` command, as follows:

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

Component   Compatible Version
---------   ---------- -------
SSC0        Reference  5.17.0
/N0/IB6     Yes        5.17.0
/N0/IB8     Yes        5.17.0
/N0/SB0     Yes        5.17.0
/N0/SB2     Yes        5.17.0
sun-sf4800-sc0:SC>
```

The above output does not include the version of firmware from the spare SC. To gather that information, connect to the spare SC and use the `showsc` command to determine the ScApp revision, as in the following:

```
sun-sf4800-sc1:sc> showsc -v
SC: SSC1
Spare System Controller
SC Failover: disabled
SC date: Tue Nov 16 12:47:10 CST 2004
         CST  GMT-6     Central Standard Time
SC uptime: 5 days 4 hours 3 minutes 38 seconds
ScApp version: 5.17.0
Version build: 1.0
Version String: 5.17.4
RTOS version: 38
SC POST diag level: off
Clock source is: 75MHz
sun-sf4800-sc1:sc>
```

The SC failover software available in 5.13.x or higher introduced a number of new commands and settings, some of which are discussed below.

The `showfailover` command is used to check on failover status. The `-v` option provides the most information about the configuration.

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

sun-sf4800-sc0:SC>
```

The above information shows the output of `showfailover -v` command running on SC0. It indicates that the SC is currently in the role of main system controller and that both SC administrative function failover and clock failover are enabled and functioning. The `showfailover -v` command should be executed whenever a SC is rebooted to help ensure the SC failover functionality is restarted and functioning properly. An additional piece of information about the SC failover status can be obtained by using the `showplatform -p sc` command, as in the following example.

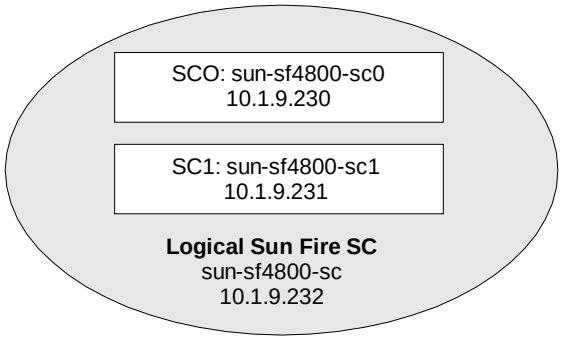
```
sun-sf4800-sc0:SC> showplatform -p sc

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

sun-sf4800-sc0:SC>
```

In the above example, the value for the logical hostname is displayed. Each SC continues to have a unique IP address assigned to it. The logical hostname is a third IP address that always points to whichever SC is currently functioning in the role of main. In Figure 2, the logical SC is the logical hostname.

FIGURE 2 Sun Fire Logical Hostname



The following is an example of how to set up the Sun Fire SC failover functionality using the `setupplatform` command:

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

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

sun-sf4800-sc0:SC>
```

If the logical hostname is already set up, the administrator can simply run the command `setfailover on`. 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 the failover functionality is enabled to verify correct failover operations.

The failover software copies data from the main SC to the spare SC at regular intervals so that the data on both system controllers is synchronized if a failover occurs. However, this is not a replacement for backing up the SC. Administrators should still perform a backup of the SC using the `dumpconfig` command after enabling failover and on a regular basis.

Each system controller provides a system clock signal to each board in the system. Each board automatically determines which clock source to use. Clock failover is the ability to change the clock source from one system controller to another system controller without affecting the active domains.

In a redundant SC configuration, the platform date and time on both the main and spare system controller must always be synchronized for SC failover purposes. Sun strongly recommends configuring both the main and spare system controller to synchronize their date and time settings against a Simple Network Time Protocol (SNTP) server, as discussed in *Configuring the SC to Use an SNTP Server* on page 9. If SNTP is not enabled, the time on the two SCs needs to be checked to make that they are the same.

For failover to work properly it is important that the time on both system controllers be as close as possible. A variation of more that five minutes can cause failover to not function properly. Therefore it is recommended that they 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 system controller.

Setting the Date and Time on the Platform

When a Sun Fire platform is installed, the platform time should be set from the platform shell and in each individual domain using the `setdate` command. Each domain shell can have a separate time setting. Therefore, it is necessary to set each one individually. The following shows an example of how to set the date and time.

```
sun-sf4800-sc0:SC> setdate -t America/New_York 082500502004
Wed Aug 25 00:50:00 EDT 2004
sun-sf4800-sc0:SC> showdate -v
Wed Aug 25 00:50:11 EDT 2004
America/New_York              GMT-05:00 Eastern Standard Time
sun-sf4800-sc0:SC>
```

The time and date on the domains can be set in a similar manner. Use the `setdate -h` command for additional help and options for setting the time. It is important to note that setting the timezone with an explicit offset from GMT (Greenwich Mean Time) results in the system controller not adjusting for daylight savings time. To adjust for daylight savings time, specify a timezone setting that adjusts to daylight savings time such as EST (Eastern Standard Time), or use the method shown above. The command `showdate -tv` can be used to see the full list of acceptable locations and timezones.

Configuring the SC to Use an SNTP Server

With SC firmware versions 5.13.0 and higher, the SC is capable of synchronizing its time-of-day clock with a network time server using SNTP. The default SC configuration for SNTP is `off`. The following shows an example of how to enable the SC to set its clock against an SNTP server.

```
sun-sf4800-sc0:SC> setupplatform -p sntp

SNTP
----
SNTP server []: 10.1.63.251

sun-sf4800-sc0:SC>
```

SNTP, described in RFC 2030, is simplified protocol based on the Network Time Protocol (NTP), described in RFC 1305. SNTP supports a simple, stateless remote procedure call (RPC) mode. SNTP clients, such as the Sun Fire server SC, can interoperate with existing NTP or SNTP clients or servers. The system controller can be directed to either a SNTP or

NTP server since the SNTP client on the system controller can understand either. However, the SNTP/NTP server should be located as close on the network as possible to the system controller in order to minimize network latencies that can affect the time stamp.

Changing POST Levels and Other Settings

To provide thorough testing of all components, the 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. In normal operation, the SC POST level should be set to minimum, but maximum (max) should be run at least once during system installation, and if the SC hardware is possibly causing a problem. In normal operation, the domain POST level should be set to maximum (max) or default. The default and max levels are functionally the same for domain POST.

At certain times it might be desirable to use a different level of domain POST. For instance, during system installation, the highest level POST (mem2) should be run, as it performs the most thorough testing of all components. Other times when mem2 POST should be run are when hardware is replaced or moved, or when the hardware is suspected of causing system problems. The following shows an example of setting the platform SC POST level:

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

SC
--
SC POST diag Level [max]:  max
Enable SC Failover? [yes]:
Logical Hostname or IP Address [sun-sf4800]:

sun-sf4800-sc0:SC>
```

Note – For SCs running firmware versions lower than 5.13.0, the commands for controlling SC failover are not visible.

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. Keep this information where it can be easily accessed in case a SC replacement is required.

The following uses the command `showdomain -p bootparams` to illustrate the domain boot parameters suggested in the above discussion:

```
sun-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

sun-sf4800-sc0:A>
```

Several parameters were added in 5.15.0 and above that allow the domain to better recover from a hang condition. Table 1 contains the recommended values to options in the `setupdomain` command. These options provide the most information from the system, while still allowing the domain to recover without manual intervention.

TABLE 1 Recommended Domain Boot Parameters

`reboot-on-error`	`true` <default>	Automatically reboots the domain when a hardware error is detected. Also boots the Solaris Operating System when the `OBP.auto-boot` parameter is set to `true`.
`hang-policy`	`reset` <default>	Automatically resets a hung domain through an Externally Initiated Reset (XIR).
`OBP.auto-boot`	`true` <OBP default>	Boots the Solaris Operating System after POST runs.
`OBP.error-reset-recovery`	`sync` <OBP default>	Automatically reboots the domain after an XIR occurs and generates a core file that can be used to troubleshoot the domain hang. However, be aware that sufficient disk space must be allocated in the domain swap area to hold the core file.

Note – If upgrading from a firmware version prior to 5.15.0 those versions of the firmware had the `hang-policy` set to `notify`. When the SC is upgraded, that setting remains set to `notify`. If upgrading to 5.15.0 or higher, it is beneficial to change the `hang-policy` setting to `reset`.

Configuring the Midframe Service Processor

While the Sun Fire platform can be administered in a standalone fashion, an external system such as a MSP is strongly recommended to provide a centralized location for functions such as easier problem diagnosis, accessibility to platform information, and updating system firmware and software. A MSP 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 using either the Simple Network Monitoring Protocol (SNMP) or `syslog`.

This article does not recommend any particular type or size of system to use (other than a minimum configuration recommendation) as a MSP because each site has different needs. One factor that impacts the type of system required for the MSP is the number of servers the MSP needs to monitor. Another is the requirement for additional functionality provided by Sun Management Center software. For example, `syslog(3)` and `sclogger` require fewer system resources to monitor hosts than Sun Management Center software.

When choosing an appropriate MSP (or MSPs), 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. For example, storage devices may also need to be monitored by the same MSP.

This section contains descriptions of how to configure the following functions on the MSP:

- Configuring the MSP to receive log messages
- Sun Management Center software
- Configuring the MSP as a firmware update server
- Sun Explorer software
- Monitoring domain consoles
- Other functions for the MSP

Configuring the MSP to Receive Log Messages

There are several places to gather information to help diagnose a problem. For example, the domain's operating system and the Sun Fire system controller are both capable of providing messages about system errors that are then stored in separate logs. Many error messages are output from only one of those places, while others are output from both. Since both the SC and the domain operating system have an individual view of the problem, the data provided by one is sometimes more useful for diagnosing the error. It is often necessary to view the error messages from both sources to fully understand a problem. From a support standpoint, having to request additional data takes very valuable time in a situation where time is critical. Therefore, when a system error is encountered it is best to gather the data from both the system controller and the domain in order to present a full detail of the problem.

Earlier versions of the system controller had a very small amount of memory for storing errors. In certain cases, it was possible for critical error messages to be lost because the SC only had space to retain the most recent error messages and messages were lost if the SC was rebooted or lost power. The newer system controller, SC v2, is equipped with additional memory to store more messages. In order to take advantage of the added memory, the SC must be running the proper firmware. The `showboards -e` command can be used check the version of the system controller. An example is provided below:

```
sun-sf4900-sc0:SC> showboards -e

Slot     Pwr Component Type               State      Status     Domain
----     --- --------------               -----      ------     ------
SSC0     On  System Controller V2         Main       Passed     -
SSC1     On  Present                      Spare      -          -
ID0      On  Sun Fire E4900 Centerplane              OK         -
PS0      Off No Grid Power                -          -          -
PS1      On  A185 Power Supply            -          OK         -
PS2      On  A185 Power Supply            -          OK         -
FT0      On  Fan Tray                     -          Failed     -
FT1      On  Fan Tray                     High Speed OK         -
FT2      On  Fan Tray                     High Speed OK         -
RP0      On  Repeater Board               -          OK         -
RP2      On  Repeater Board               -          OK         -
/N0/SB0  On  CPU Board V3                 Active     Passed     A
/N0/SB2  On  CPU Board V3                 Active     Passed     A
SB4      -   Empty Slot                   Available  -          Isolated
/N0/IB6  On  PCI I/O Board                Active     Passed     A
/N0/IB8  On  PCI I/O Board                Active     Passed     A

sun-sf4900-sc0:SC>
```

One way to assure that older messages are not lost, regardless of which system controller is used, is to configure a log host. Setting up a log host causes the system controller to forward error messages to this host, where they are stored in the remote server's messages file.

Log host set up should be performed during the initial platform setup. Both the `setupplatform` and `setupdomain` commands prompt for a syslog log host. The prompt accepts either an IP address or hostname, as well as a facility level. An example is shown below:

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

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

sun-sf4800-sc0:SC>
```

Corresponding changes need to be made to the `/etc/syslog.conf` file on the syslog log host or MSP.

The configuration of the log facility, on the SC, should be consistent with that of the syslog server to which the messages are sent. The default is `local0`. The syslog facility identifies each syslog entry with the originating hostname and syslog facility. This identification makes it easy to quickly separate messages coming from different hosts.The syslog protocol provides eight user-defined facility levels: `local0` through `local7`, Only the user-defined facility levels can be used when customizing the syslog behavior of the SCs.

Because all SC-generated syslog messages come from the same IP address — that of the SC — it is possible to use different syslog facilities to distinguish between messages originating from the platform and each domain. For example, the platform could use the syslog facility `local0`, while domain a could use `local1`, and so on.

The MSP provides a central and secure 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 Management Center server can, without generating large unmanageable log files. Many administrators solve 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 manage the logs of several systems on a single MSP installing and using the Sun Fire System Controller Logger package (`sclogger`).

The Sun Fire System Controller Logger is available at:

http://wwws.sun.com/software/download/products/4068a5fd.html

`sclogger` can monitor several machines and system controllers while only using one syslog facility. syslog forwards the messages to a named pipe where they are sorted and placed in a file that is named according to the domain or SC that it is received from. `sclogger` creates a directory on the MSP called `/var/log/sunfire`. The naming convention for the files created in `/var/log/sunfire` are in Table 2.

TABLE 2 `sclogger` Naming Convention for Log Files

File Name	Description
`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 Management Center Software

Sun Management Center software is an element management system for monitoring and managing the Sun environment. It also integrates with the leading enterprise management systems. The software provides hardware monitoring with the capability to logically group domains and the system controller into a single, manageable object to simplify operations. And, once configured, the software is also the recipient of Simple Network Management Protocol (SNMP) traps and events.

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

The Sun Management Center 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 Management Center software server that is tasked with monitoring the entire network. This configuration provides additional monitoring capabilities in case the system containing the Sun Management Center software server becomes unavailable. It also provides flexibility in the MSP and security configuration.

Sun Management Center 3.0 Platform Update 1, or higher is required to monitor SNMP traps generated by the SC. This version of Sun Management Center software is available with the Solaris 8 OS 04/01 release. Currently, the Sun Management Center software is the only package that can understand the SNMP traps generated by the SC. There are no publicly available MIBs (Management Information Base).

Note – The SC does not support a secure version of the SNMP protocol. Do not enable SNMP unless a Sun Management Center server is configured to support the system.

When configuring the SC for SNMP, it is strongly recommended that the default community strings be changed during installation for security reasons. A SNMP community string is a user name or password that accesses the statistics of a router or other device when sending SNMP traps. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond. The default community string that provides monitoring or read capability is *public*. The default management or write community string is *private*. 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
```

For SNMP clients such as the Sun Management Center software to access the system controller using SNMP, their community strings should be set to the same value as the value entered in `setupplatform`.

SNMP must be enabled on the 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 are `<domain>-public/private`.

```
sun-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

sun-sf4800-sc0:SC>
```

The port for the `Trap Hosts` value can be entered in the form of `hostname:port` in firmware 5.13.0, or higher. The SNMP agent sends traps to the trap host on an SNMP default port number (162). Do not change the port setting unless specifically instructed to do so for the installation of other software on the trap host.

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 site listed in the *References* section of this article.

In addition to setting up `syslog`(3) and SNMP, it is advisable to 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 does not send domain console messages or error messages generated by the Solaris OS (such as panic strings and watchdog reset information) to an external log host. Therefore, if the domain consoles are not constantly monitored, critical messages and valuable diagnostic information could be lost in the event of a failure. Multiple domains can be monitored and accessed via the domain shells through the Ethernet port.

Configuring the MSP as a Firmware Update Server

In order to perform firmware updates to the SC, an FTP or HTTP service must be set up on the MSP. The administrator can set up an anonymous FTP server by following the instructions in the `ftpd`(1M) man page, or use normal `ftp` by specifying a user and password in the `ftp` URL. If the MSP uses the Solaris 8 OS or higher, a version of the Apache Web server is provided with the Solaris OS, which can be used to provide HTTP services. Because the HTTP service is more configurable than the FTP service and because it can be restricted to listen-only on certain network interfaces, HTTP is more secure than FTP. A typical `flashupdate` command on the main SC might look like this:

```
ita-sf6800a-sc1:SC>flashupdate -f ftp://anonymous:ftp-
user@10.1.9.12//pub/114525-01 all rtos
```

For more information on setting up a firmware server see the *Sun Fire Midrange Systems Platform Administration Manual, Firmware Release 5.18.0*.

Sun Explorer Software

After completing the initial installation of a Sun Fire server, the Sun Explorer software should be installed on both the server and the MSP. Sun Explorer is a data collection tool comprised of shell scripts and a few binary executables. Information is gathered and transmitted to Sun and stored to enable faster, more effective diagnosis and support. The data is also reviewed in the aggregate without reference to individual customers as a tool for planning future offerings and enhancements. It should be configured to periodically collect system configuration information and error messages. Check the following site regularly for updates to the Sun Explorer software:

http://sunsolve.sun.com

It is strongly suggested that the latest version of Sun Explorer software be run, as it is continually enhanced.

If possible, the output from Sun Explorer software should be automatically submitted to the Sun Explorer software proactive database at the email address specified when the software is set up.

The following command is executed on the MSP and gathers information from the SC. The command assumes the Sun Explorer software is installed on the system in the default location: `/opt/SUNWexplo`.

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

If this command is executed on the MSP, Sun Explorer software collects data from both the MSP and the SC. To collect data from the SC, the Sun Explorer software uses a telnet connection. Therefore, the MSP must be able to establish a telnet session on the SC. With firmware 5.16.0 on the Sun Fire 3800/4800/4810/6800 servers, the SC is capable of using SSH to gather the SC extended data. On system controllers running SSH, Sun Explorer software version 4.3 or higher must be used.

The above example executes Sun Explorer software from an interactive session and the `scextended` option prompts the user for a hostname and password for each SC. To automate the process, so that Sun Explorer software can be run non-interactively through `crontab`(1) and forwarded to Sun, the user can put the login information into a file named `/etc/opt/SUNWexplo/scinput.txt`. The format for the `scinput.txt` file is:

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

If security considerations prevent automatic transmission of the Sun Explorer software results to the Sun Explorer software database, the Sun Explorer software should still be installed 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 Sun Explorer software on the MSP also collect this data. To automate this process, a line can be added to the `/opt/SUNWexplo/tools/messages` file in Sun Explorer software to include the `/var/log/sunfire` directory in the list of files the software collects. An example is shown below:

```
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
```

With Sun Explorer software 5.0 or greater, this change is not required as the software automatically gathers this data.

Monitoring Domain Consoles

It is also advantageous to continue monitoring the consoles of active domains in order to make sure messages sent to the domain consoles are not lost. Since simultaneous, multiple domain console access needs to be executed 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 publicly distributed software available at:

http://www.conserver.com

Conserver is an application that allows multiple users to watch a serial console at the same time. It logs all serial traffic, enabling the user to go back and review system crashes, see changes (if performed on the console), or input the console logs into a monitoring system. 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 domains A-D, telnet to ports 5001-5004 respectively. SSH does not allow the ability to directly telnet to a console port, 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 is to open up multiple terminal windows running the UNIX® `script` command through the `nohup` command, which allows for recording of console messages even if the terminal window is disconnected. However, this solution interrupts console logging when connecting to the domain console.

Other Functions for the MSP

The operating system for individual domains can be installed either from an attached DVD-ROM driver or over the network from a Solaris JumpStart™ software server. The function of a Solaris JumpStart software server can also be well suited for an MSP. Detailed instructions for setting up a Solaris JumpStart software server can be found in the *Solaris Operating System Administration Guides*.

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 SSH
- Keyswitch settings

Because the Sun Fire domains run the same Solaris Operating System as other systems, basic security practices that apply to any Solaris OS 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 OS, 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 protecting the SC is really protecting the whole platform.

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

Recommendations for User Authorization

The 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.

It is possible to access multiple platform shells simultaneously. The 5 SSH connections and 12 telnet connections mentioned earlier in this article 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 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.

While the platform shell manages and administers overall system resources, domain specific operations, such as the turning of the virtual keyswitch, are controlled by the domain shell. The domain shell can only access resources specified in the ACL set up for it by the platform shell, and 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. To help deter unauthorized access, passwords should be set on the SC platform and domain shells. Access to platform and domain shells can be controlled by using passwords that can be set and changed by using the `password` command on the SC. From the platform shell, the platform and domain shell passwords can be changed. From a domain shell, only the password of that particular domain can be changed.

The SC does not enforce any password standards, nor does it maintain 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 suggested policy encourages the use of pass-phrases of 16 characters as a minimum, with mixed characters, numbers and punctuation marks. 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, so 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 MSP where access can be monitored and logged.

Telnet and SSH

Prior to firmware version 5.16.0, there was no facility for an encrypted network session between a management host and the system controller. With 5.16.0, the administrator has a choice between telnet or SSH. Each option has advantages and disadvantages.

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). If the telnet protocol is chosen, it is strongly recommended that the MSP and the SCs be placed on a private, switched, non-routed network. The MSP should be the only way to access the SCs, and access to the MSP should be carefully secured, monitored, and encrypted if possible.

The SSH option is much more secure, as the traffic goes across the network in an encrypted format, and is unreadable by utilities such as snoop(1M). SSH does have some disadvantages. The number of SSH connections is limited to five overall connections. This enables a fully configured Sun Fire 6800/6900 server to have one session for each of the domains, and one for a platform shell, which might be an issue in environments with many administrators. Because of this limit, an `Idle connection timeout` value can be set

when setting up the remote access type in `setupplatform`. The idle connection timeout option is also available in telnet, as a security precaution. The following shows an example of how to set up SSH access.

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

Network Configuration
---------------------
Is the system controller on a network? [yes]:
Use DHCP or static network settings? [static]:
Hostname [sun-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]:

sun-sf4800-sc0:SC>
```

The first time SSH is enabled, the SC automatically runs ssh-keygen and generates an SSH host key that must be accepted the first time a connection is initiated. A host key is a large number that functions as a way of identifying a given system to another system. It is the primary way that one system authenticates another as being the system it claims to be. Only after the system's identity is assured can the encryption for the primary datastream be established. If in the future the host key needs to be changed, `ssh-keygen` can be executed again and the SC rebooted to use the new host key.

Keyswitch Settings

Each domain has a virtual keyswitch. There are five keyswitch positions: off (default), standby, on, diag, and secure. The virtual keyswitch replaces the need for a physical keyswitch for each domain. During normal operations, it is recommended that the virtual domain keyswitch be set to secure by using the following command:

```
sun-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 OS. 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.

Error Analysis, Diagnosis, and Recovery

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

It is important to run Sun Explorer software immediately after a failure. The storage area on the system controllers is limited, and other new errors can overwrite the original error that caused the outage. The error logs are also reset on system controller reboots, so the errors can be lost in a platform power cycle or SC reboot. SC v2 system controllers maintain the errors across reboots, allowing persistent logging. SC v2 also has additional storage for more errors, but the space is not unlimited, and a quick Sun Explorer software run 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 Diagnosis Engine (ADE) is capable of acting on the diagnosis, and disabling hardware to increase the availability of the system. For more information, refer to Sun BluePrint *Sunfire Midrange Server Auto Diagnosis and Recovery.*

After the appropriate error messages are analyzed, isolate the source of the error. Based on the results, 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 is determined, man components in the platform can be replaced with a running domain. This is accomplished through the use of Dynamic Reconfiguration (DR). Refer to Sun BluePrint *Sun Fire 3800-6800 Server Dynamic Reconfiguration* for more information about DR.

Maintenance Functions

There are serveral maintenance functions that need to be performed on a regular basis. The following functions are described in this section:

- Updating the firmware and Real Time Operating System
- Restoring the Sun Fire SC configuration
- Removing the SC from platform use

Updating the Firmware and Real Time Operating System

Periodically, updates to the system controller firmware and RTOS are 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.

Instructions for upgrading firmware are provided in the `Install.info` file included with the firmware release. The `Install.info` file also contains instructions for downgrading to an earlier version of the firmware.

The `flashupdate` command updates the firmware in the system controller and the system boards. This command is available in the platform shell only.

Before applying a firmware update using the `flashupdate` command, carefully read the release notes and `Install.info` files in the patch package before proceeding with the update to become familiar with the procedures. Creating a backup of the SC configuration before performing the update is strongly recommended.

It is also necessary to 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`. Refer to the *Sun Fire 6800/4810/4800/3800 System Controller Command Reference Manual* for more information on these commands.

It is important to perform firmware updates regularly, and for Sun Fire systems that have two SCs, to update the firmware on both SCs.

Caution – It is very important to follow the instructions in the `Install.info` file, included with each patch release, to help 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 might require that the upgrade to the SCs be performed in a specific order (e.g., spare SC upgraded first in a redundant SC configuration). It is important to read and follow the instructions carefully to avoid omitting steps, such as the `setkeyswitch` commands, that are critical to a successful upgrade of the firmware.

Firmware updates can be downloaded from the SunSolve℠ program site:
http://sunsolve.sun.com

Restoring the Sun Fire SC Configuration

If an SC fails, it might be necessary to manually restore the SC configuration information. After the configuration of the platform is completed, including setting up domains and segments, create a backup of the SC configuration so that a quick restoration is possible.

The following shows an example of how to create a backup of the Sun Fire SC configuration on the MSP using the `dumpconfig` command.

```
sun-sf4800-sc0:SC>dumpconfig -f ftp://<ftpusr>:<ftpuser
pswrd>@msp/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 MSP.

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

Removing the SC from Platform Use

If a SC needs to be removed for maintenance purposes, follow the instructions for SC replacement that are specific for the version of firmware on the SCs. For specific instructions, refer to the *Sun Fire 6800/4810/4800/3800 Systems Platform Administration Manual* for the applicable version of firmware.

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.

Summary

The Sun Fire midrange family of servers is extremely powerful and flexible, with many capabilities to enhance reliability, availability, serviceability, and security. The best practices detailed in this article are intended to help system administrators take advantage of these capabilities to develop a well planned and efficient Sun Fire server environment.

About the Authors

Ken Kambic is a member of Sun's PTS Americas Midrange Server Group where he is currently focused on resolving issues with Sun's midrange servers. Prior to his current role with PTS Engineering, Ken worked for Sun Enterprise Services in various System Support Engineer roles for the last 11 years, and before that as a systems administrator for a variety of UNIX® systems.

James Hsieh is a member Sun's PTS Americas Strategic Support Group (SSG) where he currently focuses on resolving issues with Sun's midrange servers Prior to his current role with PTS Engineering, James worked for Sun Enterprise Services supporting mission critical customers. Prior to Sun, James worked for over thirteen years with UNIX and Sun systems as a software engineer and as a Systems Administrator for large groups of UNIX systems.

References

The following sources are referenced in this article:

- *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
- *Sun Fire Midrange Server Auto Diagnosis and Recovery*
- *Sun Fire 3800-6800 Server Dynamic Reconfiguration*
- Sun Explorer software at: *http://sunsolve.sun.com*
- Solaris Security Toolkit (formerly known as jass) at: *http://www.sun.com*
- Sun Fire System Controller Logger is available at: *http://wwws.sun.com/software/download/products/4068a5fd.html*

Ordering Sun Documents

The SunDocs[SM] program provides more than 250 manuals from Sun Microsystems, Inc. If you live in the United States, Canada, Europe, or Japan, you can purchase documentation sets or individual manuals through this program.

Accessing Sun Documentation Online

The `docs.sun.com` Web site enables you to access Sun technical documentation online. You can browse the `docs.sun.com` archive or search for a specific book title or subject. The URL is `http://docs.sun.com/`

To reference Sun BluePrints OnLine articles, visit the Sun BluePrints OnLine Web site at: `http://www.sun.com/blueprints/online.html`