Sun Fire™ Midframe Server Best Practices for Administration

By James Hsieh - Customer Problem Resolution (CPR) Engineering - Americas (formerly HES-CTE)

Sun BluePrints™ OnLine - October 2001

http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 816-2201-10
Revision 1.0, 10/01/01
Edition: October 2001

Please
Recycle

Sun Fire™ Midframe Server Best Practices for Administration

Sun Fire™ 3800, 4800, 4810, and 6800 Midframe servers provide new functionality to monitor, diagnose, and administer the system which can increase overall system Reliability, Availability, and Serviceability (RAS). Much of the new functionality is available through the Sun Fire System Controller (SC) which is a central part of the Sun Fire Midframe server. The emphasis of this article is to introduce “Best Practices” that take advantage of the new functionality provided by the SC and to configure the appropriate external support resources such as a Midframe Service Processor to prepare a Sun Fire system for mission critical service.

Specifically, this article covers the following topics:

- Configuring the SC
- SC administration philosophy for the Sun Fire Midframe server
- Midframe Service Processor (MSP) configuration
- Basic platform security
- Error analysis and diagnosis

While many recommendations made here apply to the majority of cases, not all recommendations may apply to every circumstance.

System Controller Configuration

Overview:

- RS-232 Port should be accessible during the initial setup
- Use a 100BaseT Ethernet connection
- Put the SC on a switched, private network

The first step in the administration of the Sun Fire Midframe server is to configure the Sun Fire SC. The Sun Fire SC can be accessed two ways—through the built-in RS-232 serial port, or through its 10/100 Ethernet port. Be sure that access to the serial port is available during the initial setup of the SC as this is the only connection where SC Power On Self Test (SCPOST) output can be viewed. The serial port can be accessed using a network terminal server or the serial port on a Midframe Service Processor (MSP). The port settings should be 9600 bps, 8 bits, no parity, 1 stop bit (9600-8-N-1).

Once the Ethernet port has been configured, it should be the primary access path to the SC. A `telnet` session is used to connect to the Sun Fire SC from the network. Access through the Ethernet port is faster than the serial port, and allows for multiple simultaneous connections to the SC. A 100BaseT link is strongly recommended for the SC Ethernet connection and required for use with Sun™ Management Center (Sun MC) software. When in service, access to the serial port should be available to provide an alternate access path to the SC in the event of a network problem, or if the SC is rebooted or reset. Serial port access is also required to monitor certain SC and platform related errors as this is where these errors will be displayed. However, if only one connection is possible, the Ethernet port should be chosen as the primary connection path for the speed, multi-session access, and logging capabilities it provides.

For best performance, the SC should be configured on a switched, private network. If configuring two SCs for the network, assign each SC a separate IP address so they do not conflict with each other on the network. FIGURE 1 illustrates a simplified network topology.

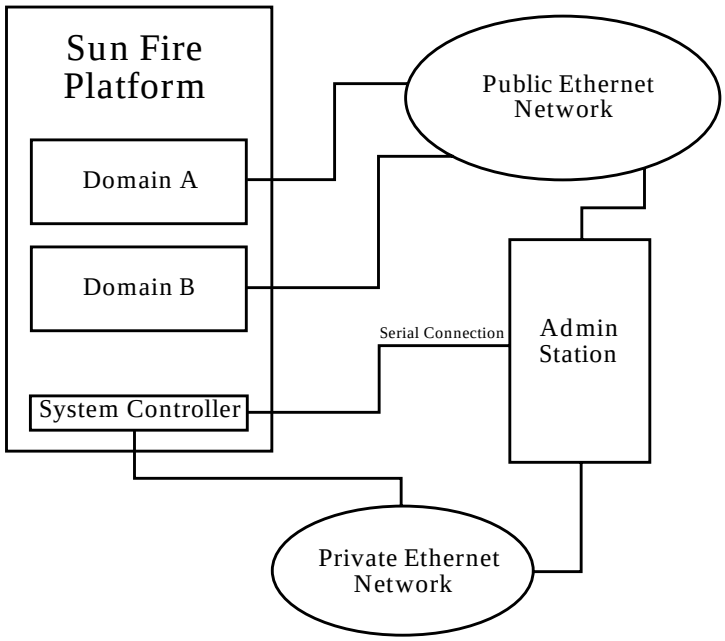

FIGURE 1 Simplified Network Topology

System Controller Administration Philosophy

The Sun Fire SC has a management scheme where operations affecting the entire system are managed through a “platform” shell and separate domain functionality is managed by a “domain” shell.

Multiple platform shells may be accessed simultaneously, and the platform shell has the ability to view status of any component within the system and can also control their allocation. One example of how the platform shell is used to manage the entire system is through the ability of the platform shell to set Access Control Lists (ACLs). The ACLs can be set up using the `setupplatform -p acl` command and can be used to restrict what resources a particular domain has access to. The domain shell can only access resources specified in the ACL set up for it by the platform.

While the platform shell manages and administers overall system resources, operations such as turning on the virtual keyswitch for each domain are controlled exclusively by the domain shell. Only one shell per domain can be active at any time. In addition, the ACL restricts the domain shell to only be able to view resources that the domain is currently using, resources that are allocated to the domain, or any resources that are unassigned on the platform, which are available to the domain according to the ACL.

The advantages to this setup are that access to the platform (and administration of overall system resources) can be restricted to a group of administrators separate from the domains. Access to platform and domain shells can be controlled using passwords which can be set and changed using the `password` command on the SC. From the platform shell, one has the ability to set or change the platform and domain shell passwords. From a domain shell, one can only change the password of the particular domain. Since the platform has additional privileges, its password should be different from those selected for the domains.

Monitoring Through Serial Port, `syslog`, and SNMP

Overview:

- Keep serial and Ethernet ports available
- Use the Ethernet interface for routine tasks
- Monitor the platform and all domain consoles
- Set up `syslog`
- Set up SNMP for Sun MC software

Administration of a Sun Fire server is designed to be performed primarily through the Sun Fire SC, and can be accessed in two ways—through the built-in RS-232 serial port or through its 10/100 Ethernet interface. While the Ethernet interface is the preferred means of accessing the SC, the serial port performs important roles in the administration of the Sun Fire server after the initial platform setup. First, the serial port is a second point of accessibility to the system in the event of a network outage. Second, it is also where the system will output platform and SC error messages. While output is buffered (up to 4K) and can also be directed to a `syslog` host if a network is configured, it is best to continuously monitor the serial port output either with a logging terminal server, or by connecting the serial port to an MSP which can capture the terminal output with a mechanism such as “script” under the Solaris™ Operating Environment (Solaris OE). This provides additional error detection and information in the event of a failure.

The Ethernet interface of the SC, in addition to providing multiple high speed shell connections, also allows for `syslog` and SNMP messages to be sent to a designated administration platform. The Ethernet interface is also required for performing firmware updates on the system, and for saving and restoring SC configuration information. Both `syslog` and SNMP facilities should be enabled and configured; however, system consoles should also be recorded using a mechanism such as "script" because not all messages can be logged with `syslog` or SNMP.

The setup of information recording and logging should be done during the initial platform setup, although it is also possible to make these changes at other times. At an absolute minimum, `syslog` should be set up to log to a central location because messages will be permanently lost if the SC message buffer fills and buffer contents are overwritten. In addition, because the SC message buffer is in volatile memory, messages can also be lost if the SC loses power. The SC maintains a 4K ring buffer for messages from each domain and the platform. A centralized mechanism for analyzing log information is also important in order to quickly locate the desired information.

When setting up the platform or domain (using `setupplatform` or `setupdomain` respectively), you will be prompted for a `syslog` log host. You can supply a `syslog` log host (using an IP address or hostname) as well as a facility level. The syntax for this is `hostname:facility` (for example, `mysysloghost:local0`). A typical setup may look as follows:

```
heslab-16:A> setupdomain -p loghost

Loghosts
--------
Loghost [129.146.63.251]: 129.146.63.251:local1

heslab-16:A>
```

Corresponding changes need to be made to the `/etc/syslog.conf` file on the `syslog` log host or MSP. Further information on the configuration of `syslog` can be found in the *Solaris Systems Administration Guides*.

Based on the number of systems and `syslog` devices that a single `syslog` log host will be monitoring, establish a convention to maximize use of the limited number of `syslog` facilities available. There are only eight `syslog` facilities available for user use in the Solaris OE, so it is likely that an administrator will quickly run out of unique `syslog` facilities. Organization of message logging is important to allow the administrator to quickly find the desired information. A good way to organize `syslog` logging is to assign `local0` to all platform messages, and then assign `local1-4` to domains A-D, respectively. `syslog` under the Solaris 8 OE identifies each `syslog` entry with the originating host name and `syslog` facility used. This makes it easy to quickly separate messages coming from different hosts.

When setting up the platform, one can configure the Sun Fire SC to interface with the latest versions of Sun MC software through SNMP. To increase the monitoring capability of the platform, users should enable SNMP with Sun MC software. 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, however, 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 platform (with `setupplatform`) before SNMP can be enabled on any of the domains. The session may look similar to the following:

```
heslab-16:SC> setupplatform -p snmp

SNMP
----
Platform Description [Sun Fire 3800]:
Platform Contact [james.hsieh@east]:
Platform Location [Lab]:
Enable SNMP Agent? [no]: yes
Trap Hosts [ ]: 129.154.221.11
Public Community String []: P-public
Private Community String []: P-private

heslab-16:SC> console a

Connected to Domain A

Domain Shell for Domain A

heslab-16:A> setupdomain -p snmp

SNMP
----
Domain Description [test]:
Domain Contact [james.hsieh@east]:
Trap Hosts [ ]: 129.154.221.11
Public Community String [ ]: A-public
Private Community String [ ]: A-private

heslab-16:A>
```

To find additional information on configuring Sun MC software, please refer to the Sun MC section on Sun Fire documentation and the main Sun MC documentation.

In addition to setting up `syslog` and SNMP, domain console sessions should be monitored in a manner similar to that described for the platform and the serial port connection. While the SC has a buffer for each domain's messages, the SC will not send domain console messages or error messages generated by the Solaris OE (such as panic strings) to an external log host. Therefore, if a domain console is not constantly monitored, critical messages and valuable diagnostic information could be lost in the event of a failure. Since there are multiple domains to monitor, domain shells should be accessed through the Ethernet port because it allows multiple connections. (The user should be aware, however, that the number of simultaneous connections via `telnet` is not unlimited.)

POST levels and Other Settings

Overview:

- Set domain post values to maximum (default)
- Set other parameters for system recovery

To provide thorough testing of all components, the POST level for both the SC and domains should be set to maximum. (Maximum is the “default” level for all domains.) If it is not always possible to run maximum POST levels at all times, it is advisable that on initial setup, maximum level POST be used to identify any components which may have failed during transit. Maximum level POST should also be used in other circumstances such as hardware being replaced or moved, after an unexpected system or power failure, or when hardware is suspected of causing system problems.

For the SC, confirm SCPOST values using the `showplatform -p sc` command as follows:

```
heslab-12:SC> showplatform -p sc

SC POST diag level: max

heslab-12:SC>
```

For each domain, confirm POST values using the `showdomain -p bootparams` command as follows:

```
heslab-12:B> showdomain -p bootparams

diag-level = max
verbosity-level = off
error-level = max
interleave-scope = within-board
interleave-mode = optimal
reboot-on-error = true
OBP.use-nvramrc? = true
OBP.auto-boot? = true
OBP.error-reset-recovery = sync

heslab-12:B>
```

Note – “default” is also equal to “max” in the case of domain diag-level.

In addition, on each domain, other recommended Domain Boot Parameters are as follows:

```
heslab-12:B> showdomain -p bootparams

diag-level = max
verbosity-level = off
error-level = max
interleave-scope = within-board
interleave-mode = optimal
reboot-on-error = true
OBP.use-nvramrc? = true
OBP.auto-boot? = true
OBP.error-reset-recovery = sync

heslab-12:B>
```

Maintenance Functions

Overview:

- Perform regular backups of the SC(s)
- Perform firmware updates as new firmware is released

In the event of an SC failure, it may become necessary to manually restore the SC's configuration information. Once the configuration of the platform has been completed, (this includes setting up domains and segments), create a backup of your SC configuration so that in the event of an SC failure, a quick restoration will be possible. To do this, use the `dumpconfig` command as follows from the SC platform shell:

```
heslab-12:B> dumpconfig -f ftp://me:passw0rd@heslab-05/dumps
```

To restore an SC configuration, use the `restoreconfig` command as follows from the SC platform shell:

```
heslab-12:B> restoreconfig -f ftp://me:passw0rd@heslab-05/dumps
```

Perform a `dumpconfig` of the Sun Fire SC on a routine basis to ensure the dump file is up to date. To help with a quick recovery in the event of a primary SC failure, make sure that the second SC has the same configuration information as the primary SC after all domain configuration has been completed.

Periodically, updates to the SC firmware and Real Time Operating System (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. Before applying a firmware update using the `flashupdate` command, carefully read any README files which may be contained in the patch package before proceeding with the update. Backing up the SC configuration before updating is also recommended. The firmware updates can be retrieved from SunSolve[SM] Web site (`http://sunsolve.sun.com`). For Sun Fire systems which have two SCs, remember to update the firmware on both SCs.

Refer to the *Sun Fire 6800/4810/4800/3800 SC Commands Reference Manual* for more information on the commands discussed here and also for other SC commands.

Midframe Service Processor Configuration

Overview:

- Change `syslog.conf`, set up log files, and test logging
- Set up Sun MC proxy and server agents on separate systems
- Set up `ftp` and/or `http` servers to provide firmware updates

By this time, it should be apparent that there is a need for an external administration system to help with the administration of Sun Fire servers because a number of features of the Sun Fire SC attempt to log messages to an external host (SNMP, `syslog`), or require monitoring on a regular basis (console outputs, SC platform messages). The Midframe Service Processor (MSP) provides a centralized and secured access point for logging these messages and provides support services that the SC cannot provide.

While the Sun Fire platform is theoretically self-contained, for ease of problem diagnosis, accessibility to platform information, and performing system firmware and software updates, an MSP is strongly recommended to provide a centralized location for these functions.

This article does not recommend any particular type of MSP, because each individual site's needs (number of systems to monitor, requirement for Sun MC software, etc.), generally differ greatly. In addition, many individual sites' requirements may conflict. For example, `syslog` does not require as much system resource as Sun MC software to monitor hosts, but because of the limited number of `syslog` logging facilities available per host, it may not be possible to monitor as many systems as a single, larger Sun MC server is capable of, without generating large, unmanageable log files.

To be able to the log messages sent with `syslog` from a Sun Fire SC, additions to the default `/etc/syslog.conf` file need to be made on the `syslog` log host, which correspond to the settings made on the Sun Fire platform. Examples of the changes to the `syslog.conf` file are as follows:

```
local0.notice   /var/log/messages.platform
local1.notice   /var/log/messages.domain-A
local2.notice   /var/log/messages.domain-B
local3.notice   /var/log/messages.domain-C
local4.notice   /var/log/messages.domain-D
```

(The above entries should be separated by tabs, `syslogd` fails otherwise.)

After making these changes to the `syslog.conf` file, create the log files before restarting `syslog`, by entering the following commands. Be sure the files have appropriate permissions.

```
nerm# touch /var/log/messages.platform
nerm# touch /var/log/messages.domain-A
nerm# touch /var/log/messages.domain-B
nerm# touch /var/log/messages.domain-C
nerm# touch /var/log/messages.domain-D
```

After restarting `syslog` or rebooting the MSP, verify that `syslog` is working correctly. Do this using the `logger` command as follows:

```
nerm# logger -p local0.notice "Platform test message"
nerm# logger -p local1.notice "Domain A test message"
nerm# logger -p local2.notice "Domain B test message"
nerm# logger -p local3.notice "Domain C test message"
nerm# logger -p local4.notice "Domain D test message"
```

Verify that the “test message” is logged in the appropriate log file. Then, verify that the SC is logging properly by entering the `setkeyswitch off` and `setkeyswitch on` commands, and verifying that POST results are sent to the log files.

Periodically, the log files will need to be rotated to prevent them from growing too large in size. This can be done by setting up additional scripts such as `/usr/lib/newsyslog` to run on a regular basis, which modifies the contents of the additional scripts to rotate the specified log files. Rotate the files on at least a monthly basis, and keep archived copies of the information for at least two months.

As mentioned previously, `syslog` facilities available for use are limited, so plan ahead and organize how the limited number of resources are used to effectively enable the administrator to quickly locate data. In addition, it is also useful to set up

scripts to parse and sort the incoming information on a regular basis and notify the administrator with an email of the changes. Further information on the configuration of `syslog` can be found in the *Solaris Systems Administration Guides*.

A Sun MC server normally requires a higher level of system resources, such as a correctly configured dual processor system capable of having 1 GB of RAM or more. However, a Sun MC server has a greater capability to monitor and administer a large number of systems. Whether or not the Sun MC proxy agent is running on the same host as the server agent, may influence a Sun MC server configuration. Sun MC software should be implemented with two systems, where one small system acts as a proxy agent for one or more Sun Fire platforms, and the second system is the larger Sun MC server tasked with monitoring an entire network. This configuration provides additional monitoring capabilities in case the system containing the Sun MC server becomes unavailable, and provides flexibility in MSP and security configuration.

To be able to monitor SNMP traps generated by the Sun Fire SC, the Sun MC 3.0 Platform Update 1 (available with the Solaris 8 OE 04/01 software release) must be installed. Currently, Sun MC software is the only package that can understand the SNMP traps generated by the Sun Fire SC—no MIBS are publicly available. Refer to the Sun MC 3.0 Software Supplement for Sun Fire 6800/4810/4800/3800 systems documents for additional installation and setup information.

For purposes of firmware updates to the Sun Fire SC, it is necessary to set up an `ftp` or `http` service on the MSP. An anonymous `ftp` server can be set up by following the instructions in the `ftpd` man page under the Solaris OE, or it is possible to use normal `ftp` by specifying a user and password in the ftp URL. If the MSP uses the Solaris 8 OE, a version of the Apache Web server is provided with the Solaris 8 OE software and may be used to provide `http` services. Because the `http` service is more configurable than the `ftp` service and may be restricted to listen only on certain network interfaces, `http` can have less of a security impact than `ftp`. Refer to the Sun BluePrints™ OnLine article published September 2001, "*Securing the Sun Fire™ Midframe System Controller*" (available from `http://www.sun.com/blueprints/0901/sunfire-msp-sc.pdf`) for additional configuration information.

The operating system for Sun Fire server domains can be installed either with an attached DVD-ROM drive or over the network from a Solaris JumpStart™ server. The function of a JumpStart server may also be well suited for an MSP. Detailed instructions for setting up a Solaris 8 OE JumpStart™ server can be found in the *Solaris Systems Administration Guides*.

When choosing a proper MSP (or MSPs), some additional capabilities need to be considered, such as accessing the serial ports on multiple Sun Fire SCs, and how many devices need to be monitored on the same system. For example, the Sun StorEdge™ T3 array may also need to be monitored by the same MSP.

General System Administration and Management

Overview:

- Set up and run Explorer Version 3.5 or higher
- Set up Explorer to run periodically

After completing the initial installation of a Sun Fire server, the Explorer utility should be installed on both the server and MSP, and set up to run periodically to collect system configuration information and error messages. If possible, the output from Explorer should be automatically emailed to the Explorer database at the email address specified when setting up Explorer. Version 3.5 or higher of Explorer should be used because it has the capability to gather data from the Sun Fire SC.

The following command gathers information from the SC, and should be executed on the MSP. In addition, the following command assumes that Explorer has already been installed on the system in the default `/opt/SUNWexplo` location.

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

If the previous command is executed from a Sun Fire domain, Explorer will collect data from both the SC and the domain.

Explorer is available from `http://sunsolve.sun.com`.

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

The initial installation is also a good time to record and check the system serial number, `hostid` information, and MAC address information provided with the system and to become familiar with how these values are reported by the SC `showplatform -v` command. This information should be kept where it can be easily accessed should an SC replacement be required.

Basic platform Security

Overview:

- General Solaris OE security practices always apply
- Choose “good” passwords for your system
- Control and restrict access to the SC serial port
- Only access the SC from the MSP
- Secure the MSP

System security is important for any computing system, and the Sun Fire server is no exception. Since the Sun Fire server runs the same Solaris OE as other Sun systems, basic security practices that apply to any Solaris OE system also apply to the Sun Fire servers. This includes basic suggestions such as regular patch maintenance, stopping unnecessary network services, and choosing good passwords to prevent account abuse. However, the architecture of the Sun Fire server with the SC, results in additional security considerations. In addition, because the SC is key to the administration and operation of a Sun Fire server, the security capabilities of the Sun Fire SC are more limited.

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. Refer to the Sun BluePrints OnLine article, “*Securing the Sun Fire™ Midframe System Controller*” for a more detailed discussion of this topic. Some general recommendations of user authorization are presented in this section.

To help deter unauthorized access, passwords should be set on the Sun Fire SC platform and domain shells. These can all be set using the `password` command from either the SC platform or domain shells. The `password` command, issued from the platform shell, can be used to change the platform shell password, or any domain shell password through the use of the `-d <domain>` option. The `password` command issued from a domain shell, can only be used to change the password for the particular domain. The SC does not enforce any password standards and the SC also maintains no records of failed login attempts or the source of the login attempts. Given the importance of these passwords in terms of restricting access to critical system resources, good passwords should be chosen that cannot be easily guessed or discovered using a brute-force attack. Passwords for the SC can and should be longer than eight characters. It is strongly recommended that passwords for platform access and root user access on the domains be different.

It is extremely important to carefully control access to the Sun Fire SC serial port. Since 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. Access to the serial port could result in the compromise of the application that runs on the SC. Since that application controls the entire Sun Fire system, improper access could

result in undesired changes to critical settings or system outages. Attach the serial port connection of the Sun Fire SC to a password controlled terminal server or directly to the MSP where access can be monitored and logged.

There is no current capability for session encryption between a host and the SC through the Ethernet interface. Since `telnet` sessions are used to make connections to the SC, maintaining a secure network is of the utmost importance. It is strongly recommended that the MSP and the Sun Fire SCs be placed on a private, switched, non-routed network. The MSP should be the only way to access the Sun Fire SCs, and access to the MSP should be carefully secured, monitored, and encrypted if possible. This includes the use of a terminal server which supports encryption (i.e. SSH) if possible. If the terminal server does not support encryption, be sure to place the terminal server on the private network and not on the public network.

In cases where corporate security policy dictates the use of encrypted sessions on all networks, one suggestion is to connect the Ethernet interface on the SC directly to a secured workstation with an Ethernet cross-over cable, and then require encrypted sessions between other hosts and the secured workstation. To further enhance the security of the MSP, a tool such as the Solaris™ Security Toolkit software, formerly known as `JASS` (`http://www.sun.com/blueprints/tools`), should be used to install and improve the security profile of the MSP. Due diligence should also be exercised to keep the MSP and SC up to date in terms of patches.

While it is advantageous to set up a Web (`httpd`) server and/or an anonymous `ftp` server on the MSP to facilitate firmware updates to the Sun Fire SC, both of these network services have traditionally been common sources for security issues. Since a compromised MSP could also compromise the SC and the entire Sun Fire platform, it is important to pay close attention to the setup of these services, security patches applied for these services, and access to the MSP be carefully configured.

Error Analysis and Diagnosis

Overview:

- Use Explorer to gather data
- Carefully analyze any errors
- Isolate failure through software reconfiguration before swapping boards

Sun Fire servers have been designed with significantly enhanced diagnostics capabilities. In the event of a system fault, the system should provide data for both software and hardware failures which can be used to help determine the source of the fault. Errors can be generated and logged to several places, depending on the type of error. A utility such as Explorer is recommended to gather data from the system so that all error messages can be collected in a central location for analysis.

After the appropriate error messages have been located, use the *Sun Fire 6800/4810/4800/3800 Systems Troubleshooting Manual* and the flow charts contained within to isolate the source of the error as far as possible. Based on the results, attempt to verify the failure using component blacklisting, segmenting, or other reconfiguration before attempting to remove or replace components (in the case of a suspected hardware problem).

Summary

This article has described the configuration and setup of the various parts of the Sun Fire Midframe to take advantage of many of the new features available to help administer and service the system. Proper configuration of the Sun Fire Midframe server provides increased RAS through the availability of additional monitoring and logging functionality while maintaining security over the system's resources.

References

- *Sun Fire 6800/4810/4800/3800 System Controller Command Reference Manual* (Sun Document # 805-7372)
- *Sun Fire 6800/4810/4800/3800 Systems Service Manual* (Sun Document #805-7363)
- *Sun Management Center 3.0 Software Installation Guide* (Sun Document #806-5943)
- *Sun Management Center 3.0 Software Supplement For Sun Fire 6800/4810/4800/3800 Systems* (Sun Document #806-5948)
- *Securing the Sun Fire™ Midframe System Controller* (Sun Blueprints OnLine September 2001)
- *Sun Field Engineer Handbook*
- Global Knowledge Engineering Explorer Tool at `http://sunsolve.sun.com`
- Solaris Security Toolkit (formerly known as JASS) available at `http://www.sun.com/blueprints/tools`

Author's Bio: James Hsieh

James Hsieh is a member of the Sun CPR Engineering Americas (formerly HES-CTE) group and is part of the team responsible for providing engineering support of Sun's midrange server line. Prior to his current role with CPR Engineering, James worked for Sun Enterprise Services supporting Mission Critical customers.

Prior to Sun, James worked for over ten years with UNIX® and Sun systems as a software engineer and as a systems administrator for large groups of UNIX systems.