



# Sun™ Control Station 2.2 Health Monitoring Module

---

Sun Microsystems, Inc.  
[www.sun.com](http://www.sun.com)

Part No. 819-0443-10  
December 2004 Revision A

Submit comments about this document at: <http://www.sun.com/hwdocs/feedback>

Copyright 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, JavaServer Pages, JSP, JumpStart, Netra, Solaris, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube, Sun Fire and Ultra are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

Netscape and Mozilla are trademarks or registered trademarks of Netscape Communications Corporation in the United States and other countries.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, États-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatants à la technologie qui est décrite dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les États-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, JavaServer Pages, JSP, JumpStart, Netra, Solaris, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube, Sun Fire et Ultra sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Netscape et Mozilla sont des marques de Netscape Communications Corporation aux États-Unis et dans d'autres pays.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciées de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE «EN L'ÉTAT» ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISÉE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.

# Contents

---

<b>Health Monitoring Module</b>	<b>1</b>
How Managed Hosts Are Monitored	2
Health Monitor Alerts	2
Known Issues	3
Conflicting Settings	3
Unexpected LOM Information Within Health Monitor	3
Health Monitor Screen	4
Health Summary	4
Viewing the Health Monitor Data	5
Critical Events Refresh Button	6
Services Monitored on Managed Hosts	6
Clearing Critical Events	6
Updating Health Status Data	7
Viewing the Health Summary of All Hosts	8
Refreshing the UI	9
Settings	9
Alive Polling	9
Status Polling	10
Alive and Status Polling Settings	10

Health Monitor Settings You Can Configure	10
Configuring Health Monitoring Settings	11
Scheduling an Alive Polling Task	12
Scheduling a Status Polling Task	13
Adding New Services to the Health Monitoring Module	13
Format of the Configuration File	14
Creating a New Health Monitor Service	15

# Health Monitoring Module

---

The Health Monitoring control module of the Sun™ Control Station software enables you to monitor the status of various parameters of your managed hosts. This document explains the features and services available through the Health Monitoring control module. These include:

- Viewing a summary of the health status data for a host or group of hosts
- Retrieving the most recent health status data from the managed hosts
- Scheduling polling of managed hosts to obtain health status data
- Verifying that you can reach the agent on a managed host and that the host can be accessed over the network
- Forcing the Control Station to retrieve immediately the most recent health status data from an individual host
- Configuring the parameters for the Health Monitoring module
- Entering an email address to receive alerts from the Health Monitoring module when there are critical system events (a yellow circle with an exclamation mark or a red circle with an “X”)

---

**Note** – This manual assumes that you understand the basic operation of Sun Control Station software. For an introduction to basic Sun Control Station features like status icons, the selector window, the Scheduler, and the Task Progress dialog, see the *Sun Control Station 2.2 Administrator Manual*.

---

---

# How Managed Hosts Are Monitored

Monitoring in the Health Monitoring module is based on polling and events. This means that health status data is acquired either by the Control Station initiating a poll to read the client-state information from each host, or by the managed host informing the Control Station immediately upon encountering a problem (an *event*).

FIGURE 1 shows the Critical Events and the Managed Host Group Status tables.



The screenshot displays a user interface for health monitoring. At the top, there are two buttons: "Refresh" and "Clear Critical Events". Below these are two tables. The first table, "Critical Events", has columns for Status, IP, Date/Time, and Action. It lists three events with a red 'X' status icon, all occurring on Friday, September 5, 2003. The second table, "Managed Host Group Status", has columns for Status, Group Name, Number of Hosts, and Action. It lists three groups: "Raq 550" (red 'X' status, 22 hosts), "Qube 3" (red 'X' status, 26 hosts), and "New Group" (green checkmark status, 3 hosts).

Status	IP	Date/Time	Action
✖	10.6.73.46	Fri, 5 Sep 2003 01:53:16	🔍 🔄
✖	10.6.73.48	Fri, 5 Sep 2003 01:54:06	🔍 🔄
✖	10.6.75.170	Fri, 5 Sep 2003 01:54:32	🔍 🔄

  

Status	Group Name	Number of Hosts	Action
✖	Raq 550	22	🔍
✖	Qube 3	26	🔍
✔	New Group	3	🔍

FIGURE 1 Health Monitor Tables

The time stamp given for an event in the Health Monitor tables reflects the time of its last change in status, for instance from yellow to red.

---

## Health Monitor Alerts

If a critical event is present on the Control Station, a Status Alert is indicated in the top left corner of the user interface (UI). A critical event results when a transition to a “warning” or “critical” event is detected or generated (meaning that a yellow or red state is returned during health polling).

A critical event can involve any of the services or hardware components on a managed host.

---

## Known Issues

This section alerts you to some difficulties you might encounter using the Health Monitoring module. These difficulties tend to arise when a particular host is managed by more than one Control Station.

### Conflicting Settings

The Health Monitor settings (for example, the CPU alarm thresholds) can be changed from any Control Station. When the settings are changed on a Control Station, the new values are propagated to all of that Control Station's managed hosts.

The values from the most recent settings changes overwrite any earlier values on the managed host. However, the settings that appear in the interfaces of the other Control Stations do not update to reflect the most recent settings changes.

For best practice, if more than one Control Station manages a given host, ensure that the Health Monitor settings on each of these Control Stations are set to the same values.

### Unexpected LOM Information Within Health Monitor

This problem arises when a single host is being managed by two (or more) Control Stations, *and*:

- The Lights Out Management (LOM) control module is installed on one of the Control Stations but not the others
- The LOM control module client software has been installed on the managed host

Since the Health Monitoring control module is designed to receive LOM information when it is available, the Health Monitor tables on all Control Stations will display this LOM information, even though the LOM control module has not been installed on all Control Stations.

This is not a bug or a malfunction. It just means that you may see LOM information displayed in the Health Monitor tables when you would not expect to see it.

---

# Health Monitor Screen

When you click the Health Monitor menu item, the submenu items allow you to view the current status or update the status of the services and hardware components for managed hosts.

The submenu items are:

- Health Summary (see “Health Summary” on page 4)
- View Hosts (see “Viewing the Health Summary of All Hosts” on page 8)
- Settings (see “Settings” on page 9)

## Health Summary

The Health Summary submenu item displays a summary of the health status data for the managed hosts.

When you click on the Health Summary submenu item, the Critical Events and Managed Host Group Status tables appear; see FIGURE 1.

- The Critical Events table displays events that the Administrator should address immediately.
- The Managed Host Group Status table displays the general status of the groups of hosts on the Control Station.

When you click a *magnifying glass* icon to see more detailed information for a host, three tables appear:

- The Base System Components table displays information on: CPU, Disk, Memory and Network.
- The Base Services table displays information on the various services that are running on that particular host, for example, FTP server, Telnet server, Email server, or DNS server. These items can vary depending on the type of host you are viewing.
- The Other System Services table displays information on third-party or customized services that the Administrator has added to a host.

---

**Note** – To add a new Health Monitoring service, see “Adding New Services to the Health Monitoring Module” on page 13.

---



## Viewing the Health Monitor Data

To view a summary of the health monitor data on a managed host:

1. **Select Health Monitor → Health Summary.**

The Critical Events and Managed Host Group Status tables appear.

2. **To view more detailed information for a critical event, click the *magnifying glass* icon next to the item in the Action column.**

The following information tables appear (see FIGURE 2).



The screenshot displays a web interface for monitoring system health. At the top, there is an 'Update Now' button. Below it, the main title is 'Health Monitor - Base System Components-10.6.75.154'. The interface is divided into three sections, each with a table of data.

Status	Service	Vendor	Date/Time
✓	CPU	Sun	Thu, 4 Sep 2003 14:38:20
!	Memory	Sun	Thu, 4 Sep 2003 14:38:20
✓	Network	Sun	Thu, 4 Sep 2003 14:38:20
✗	Disk	Sun	Fri, 5 Sep 2003 02:44:35

  

Status	Service	Vendor	Date/Time
...	DNS Server	Sun	Thu, 4 Sep 2003 14:38:20
✓	Email Server	Sun	Thu, 4 Sep 2003 14:38:20
✓	FTP Server	Sun	Thu, 4 Sep 2003 14:38:20
✓	SNMP Server	Sun	Thu, 4 Sep 2003 14:38:20
✓	Telnet Server	Sun	Thu, 4 Sep 2003 14:38:20
...	Web Server	Sun	Thu, 4 Sep 2003 14:38:20

  

Status	Service	Vendor	Date/Time
There is currently no data			

FIGURE 2 Detailed Information Tables

- Base System Components
- Base Services
- Other System Services

Click the *up arrow* icon in the top right corner to return to the previous screen.

**3. If you view the details for a group of managed hosts, the Managed Hosts State table appears, listing the hosts belonging to that group.**

You can click on the *magnifying glass* icon next to the host in the Action column. The same three information tables then appear.

Click the *up arrow* icon in the top right corner to return to the previous screen.

## Critical Events Refresh Button

Above the Critical Events table is a Refresh button. This button causes the UI frame to update immediately to reflect the most current data in the database.

This button does not update the database with new information from the managed hosts. To update the information in the database, see “Updating Health Status Data” on page 7.

## Services Monitored on Managed Hosts

The services monitored on managed hosts include:

- DNS Server
- Email Server
- FTP Server
- MySQL Server
- SSH Server
- Telnet Server
- Web Server

## Clearing Critical Events

When a critical event occurs on a managed host, the event appears in the Critical Events table. If you decide not to deal with a given critical event, you can clear this event from the table. The problem is still present on the managed host, but there will be no further notification concerning this critical event in the Critical Events table.

---

**Note** – If a critical event for a different problem occurs on this same managed host, a new critical event displays in the table.

---

To clear a particular critical event from the Critical Events table or to clear all critical events:

**1. Select Health Monitor → Health Summary.**

The Critical Events and Managed Host Group Status tables appear.

2. **To clear a particular critical event from the table, click the *delete* icon next to the event in the Action column.**

The Critical Events table refreshes with that critical event removed from the table.

3. **To clear all critical events from the table, click Clear Critical Events above the table.**

The Critical Events table refreshes with no entries.

## Updating Health Status Data

You can refresh the health status data for each host. This feature causes the Control Station to retrieve immediately the most recent health status data from a host.

The Update Now button appears in the UI when you are viewing the detailed information tables for an individual host. To refresh the health status data on a managed host:

1. **Select Health Monitor → Health Summary.**

The Critical Events and Managed Host Group Status tables appear.

2. **Click the *magnifying glass* icon next to the item in the Action column.**

The detailed tables of information appear.

3. **If you view the details for a critical event, the following information tables appear:**

- Base System Components
- Base Services
- Other System Services

4. **If you view the details for a group of managed hosts, the Managed Hosts State table appears, listing the hosts belonging to that group.**

You can click on the *magnifying glass* icon next to the host in the Action column. The same three information tables then appear.

5. **On the screen showing the detailed information tables for a host, click Update Now above the table.**

This forces the Control Station to retrieve immediately the health data from the managed host.

The Task Progress dialog appears.

6. **Click the *up arrow* icon in the top right corner to return to the previous screens.**

## Viewing the Health Summary of All Hosts

To view the overall health for each of the managed hosts in one table:

### 1. Select Health Monitor → View Hosts.

The Managed Hosts State table appears, displaying the list of managed hosts (see FIGURE 3).



Status	IP	Date/Time	Action
✓	10.6.73.44	Tue, 2 Sep 2003 17:32:37	🔍
✗	10.6.73.46	Fri, 5 Sep 2003 01:53:16	🔍
✗	10.6.73.48	Fri, 5 Sep 2003 01:54:06	🔍
✗	10.6.73.49	Fri, 5 Sep 2003 01:57:52	🔍
✗	10.6.74.69	Fri, 5 Sep 2003 01:59:55	🔍
✓	10.6.73.109	Tue, 2 Sep 2003 18:08:05	🔍
✓	10.6.73.50	Tue, 2 Sep 2003 18:11:10	🔍
✓	10.6.73.54	Tue, 2 Sep 2003 18:24:08	🔍
✓	10.6.73.56	Tue, 2 Sep 2003 18:24:53	🔍
✗	10.6.74.129	Fri, 5 Sep 2003 01:53:56	🔍

FIGURE 3 Managed Hosts State Table

---

**Note** – If there are more than 10 entries in the Managed Hosts State table, the table lists the first 10 entries. There are buttons at the bottom of the table with which to choose different ranges of entries.

---

### 2. To view more details for an individual host, click the *magnifying glass* icon next to the host in the Action column.

The following information tables appear:

- Base System Components
- Base Services
- Other System Services

Click the *up arrow* icon in the top right corner to return to the previous screen.

3. **On the screen showing the detailed information tables for a host, click Update Now.**

This forces the Control Station to retrieve immediately the health data from the managed host.

The Task Progress dialog appears.

4. **Click the *up arrow* icon in the top right corner to return to the previous screen.**

## Refreshing the UI

- **Click the Refresh button.**

This button, located above the Managed Hosts State table, causes the interface to update immediately to reflect the most current data in the database.

This button does not update the database with new information from the managed hosts.

## Settings

### Alive Polling

This feature allows the Control Station to verify that the agent is running on a managed host, and that the host can be accessed over the network. It works in the following way:

1. The Control Station sends a simple agent request.

If this request is successful, the agent is functioning normally and the host can be accessed over the network. The status of the network component in the Base System Components table is green.

If this agent request is not successful, the status of the network component changes to red; see FIGURE 2 for an example.

2. The host with the “failed” agent is then pinged through an Internet Control Message Protocol (ICMP) ping to verify network connectivity.

If this ICMP ping is successful, the health-monitoring information table in the database records that the Control Station cannot access the agent on the host *IP address*.

If this ICMP ping is not successful, the table records that the Control Station cannot access the host *IP address* over the network.

## Status Polling

The Status Polling Interval indicates when a polling cycle begins (for example, every four hours) for retrieving the health data from the managed hosts.

When setting this interval, you need to take into account the number of hosts managed by the Control Station. The managed hosts are polled serially. When the Control Station encounters an unreachable host (including Sun Control Station agent failures), the time-out period for polling this host is 10 minutes.

If the Control Station encounters a number of unreachable hosts during a polling cycle, a given cycle may not complete before the start of the following polling cycle.

The minimum Status Polling Interval is one hour. If a Sun Control Station is managing many hosts, you should set a longer interval.

## Alive and Status Polling Settings

Alive and Status Polling settings you can configure include:

- **Run Interval.** Set the interval at which the Control Station attempts to communicate with the managed hosts. For example, every 6 hours.
- **Run Minute(s).** Select the minute(s) past the hour that you want the Alive Polling task to run. Highlight the minute(s) and use the arrow keys to move them between the scrolling windows.
- **Email Address.** Enter an email address of the person who will be notified when the Alive Polling task runs.
- **Notify When Starting.** Check the box to notify the person when the task is starting.
- **Notify When Finished.** Check the box to notify the person when the task has completed.

## Health Monitor Settings You Can Configure

You can configure the following parameters:

- **Enable Event.** If you enable the check box, all of the managed hosts send to the Control Station any events that are generated on the hosts. If you do not enable the check box, events are not sent to the Control Station.  
Events come into the Control Station on port 80.  
This feature does not affect the events that are detected during a polling interval.
- **Notification Email Address.** This email address receives alerts from the Health Monitoring module when there are critical system events (red circle).  
You can enter only one email address in this field.

---

**Note** – If you enter an email address for a host’s Administrator when adding the host to the Control Station, that email address also receives from the Health Monitoring module the notifications for that particular host.

---

- **CPU Yellow Alarm.** Enter the threshold at which a yellow alarm is generated. This value represents the average load of the CPU. The default value is 3; the recommended maximum is 7.
- **CPU Red Alarm.** Enter the threshold at which a red alarm is generated. This value represents the average load of the CPU. The default value is 6; the recommended maximum is 15.
- **Disk Yellow Alarm.** Enter the threshold at which a yellow alarm is generated. This value represents a percentage of hard disk drive usage. The default value is 80; the recommended maximum is 90.  
For example, a value of 80 means that a yellow alarm is generated when 80% of the capacity of the hard disk drive is used.
- **Disk Red Alarm.** Enter the threshold at which a red alarm is generated. This value represents a percentage of hard disk drive usage. The default value is 90; the recommended maximum is 95.  
For example, a value of 90 means that a red alarm is generated when 90% of the capacity of the hard disk drive is used.
- **Memory Yellow Alarm.** Enter the threshold at which a yellow alarm is generated. This value represents a percentage of memory usage. The default value is 50; the recommended maximum is 75.  
For example, a value of 50 means that a yellow alarm is generated when 50% of the memory is in use.
- **Memory Red Alarm.** Enter the threshold at which a red alarm is generated. This value represents a percentage of memory usage. The default value is 75; the recommended maximum is 90.  
For example, a value of 75 means that a red alarm is generated when 75% of the memory is in use.

## Configuring Health Monitoring Settings

To configure the settings for the Health Monitoring control module:

1. **Select Health Monitor → Settings.**

The Health Monitor Properties table appears (see FIGURE 4).

Health Monitor Properties	
Enable Events	<input checked="" type="checkbox"/>
Notification Email Address	<input type="text"/>
CPU Yellow Alarm	<input type="text" value="3"/>
CPU Red Alarm	<input type="text" value="6"/>
Disk Yellow Alarm	<input type="text" value="80"/>
Disk Red Alarm	<input type="text" value="90"/>
Memory Yellow Alarm	<input type="text" value="50"/>
Memory Red Alarm	<input type="text" value="75"/>

**FIGURE 4** Health Monitor Properties Table

**2. Configure settings.**

For a list of settings you can change, see “Health Monitor Settings You Can Configure” on page 10.

**3. Click Save.**

The Health Monitor Properties table is refreshed.

## Scheduling an Alive Polling Task

To schedule a new Alive Polling task:

**1. Select Health Monitor → Settings.**

The Health Monitor Properties table appears.

**2. Click Schedule New Alive Polling.**

This button is located above the table. The Schedule Settings For Alive Polling table appears.

**3. Configure settings.**

For a list of Alive Polling settings, see “Alive and Status Polling Settings” on page 10.

**4. Click Save or Cancel.**

- *If you click Cancel*, the scheduled task is not saved. The Scheduled Tasks table appears, but without the task you just cancelled.
- *If you click Save*, the scheduled task is added to the list of scheduled tasks. The Scheduled Tasks table appears with the new task.



5. **In the Scheduled Tasks table, you can view details for, modify, or delete a scheduled task.**
  - To view the details of a scheduled task, click the *magnifying glass* icon.
  - To modify a scheduled task, click the *pencil* icon.
  - To delete a scheduled task, click the *delete* icon.

## Scheduling a Status Polling Task

To schedule a new Status Polling task:

1. **Select Health Monitor → Settings.**

The Health Monitor Properties table appears.
2. **Click Schedule New Status Polling.**

This button is located above the table. The Schedule Settings For Status Polling table appears.
3. **Configure settings.**

For a list of settings you can change, see “Alive and Status Polling Settings” on page 10.
4. **Click Save or Cancel.**
  - *If you click Cancel*, the scheduled task is not saved. The Scheduled Tasks table appears, but without the task you just cancelled.
  - *If you click Save*, the scheduled task is added to the list of scheduled tasks. The Scheduled Tasks table appears with the new task.
5. **In the Scheduled Tasks table, view details for, modify, or delete a scheduled task.**

---

# Adding New Services to the Health Monitoring Module

The Health Monitoring module allows you to incorporate customized scripts to execute and monitor. A script is executed and, based on the results, may send an event that causes an alarm or critical event on the Sun Control Station. The specific information associated with the event is presented in the Other Services table in the detailed information screen. Clearing the Critical Event table resets the alarms.

To make it easy to customize the Health Monitoring module, the module uses a configuration file to specify details on the customized scripts. From this configuration file, the Health Monitoring daemon acquires the name of the monitor, description, program to run, and the text for each of the states that the program will supply.

The states are 0, 1, 2 or 3; they correspond to the criticality of the problem and thus to the color and icon of the state presented in the Health Monitoring tables. The states are defined as:

- State 0 = Unavailable service (grey with dotted line)
- State 1 = Service is functioning normally (green with checkmark)
- State 2 = Warning state (yellow with exclamation mark)
- State 3 = Critical state (red with X)

## Format of the Configuration File

The format of the configuration file is as follows:

- **version.** The version of the configuration file or monitor script  
Example: version 1.0
- **Program.** The full path name of the script to be run at each interval  
Example: /usr/mgmt/bin/cobalt\_db.pl
- **vendor.** A string that specifies the vendor or owner of the monitor  
Example: Vendor Test
- **interval.** The interval at which the monitor runs, in minutes  
Example: 10
- **name.** A string specifying the name of the monitor  
Example: Database Check
- **description.** A string specifying a brief description of the monitor  
Example: Monitors the database
- **state0msg.** The string specifying the message to send with an event when the state is “unavailable” (gray circle)  
Example: The database server is not monitored/state unavailable.
- **state1msg.** The string specifying the message to send with an event when the state is “good” (green circle)  
Example: The database server is online.

- **state2msg.** The string specifying the message to send with an event when the state is “warning” (yellow circle)

Example: The database server is in limbo.

- **state3msg.** The string specifying the message to send with an event when the state is “critical” (red circle)

Example: The database server is offline.

The program specified in the configuration file is required to return a numeric value of 0, 1, 2 or 3. When the Health Monitoring daemon runs a polling pass (approximately every 10 minutes), the program specified in the configuration file is executed.

The results (a value of 0, 1, 2 or 3) are captured and stored after the program is executed for the first time. From that point on, each time the Health Monitoring daemon runs, the results are compared to the previous results. If the results are different, an event is generated and sent to the Control Station. The event contains the state, message associated with the state, name, version, and description of the service. If a yellow or red state is returned, a critical event is generated on the Control Station and a Status Alert is generated in the top left corner of the UI.

The configuration file must be placed in the `/usr/mgmt/etc/hmd` directory and the monitor script in the `/usr/mgmt/bin` directory.

Include these steps in the install script so that, during installation, the files are placed in the correct directories and the daemon is restarted.

## Creating a New Health Monitor Service

To create a new Health Monitor service:

### 1. Create the configuration file with the various settings for the new service.

Name the configuration *filename.conf* (for example, `monitor_db.conf`). All of the configuration files are placed in the `/usr/mgmt/etc/hmd` directory.

This is what a sample configuration file would look like:

```
version 1.0
program /usr/mgmt/bin/monitor_db.pl
vendor Sun
interval 10
name Database
description Monitors the database.
state0msg The database server is not monitored/state unavailable.
state1msg The database server is running.
```

```
state2msg The database server is in limbo.
state3msg The database server is not running.
```

**2. Create a script to monitor the new service (the *program* setting in the configuration file).**

All of these monitor scripts are placed in the `/usr/mgmt/bin` directory.

For example, the monitor script for the service Database Check (`monitor_db.pl`) would look like:

```
#!/usr/bin/perl -w
# This script return whether mysql db is running
#
# return values:
#   Disabled/No info: 0
#   Running:          1
#   Not Running:     3
use strict;
use lib '/scs/lib/perl5';
use SysCmd;

if (system("/bin/ps -ef | /bin/grep mysqld | /bin/grep -v grep"))
{
    exit(3);
}
else {
    exit(1);
}
```

**3. In the install script, include the following directive specifically for the new Health Monitor service.**

Copy the configuration file and the monitor script to the correct locations.

```
echo "Copying script to /usr/mgmt/bin " >> $LOG
cp /YourDirectory/patches/monitor_db.pl /usr/mgmt/bin/
echo "Copying configfile to /usr/mgmt/etc/hmd " >> $LOG
cp /YourDirectory /patches/monitor_db.conf /usr/mgmt/etc/hmd/
```

**4. Create a package file for each type of host on which you want to install this new Health Monitor service.**

**5. Upload the package to the Control Station using the Software Installer module. Use Software Installer module either to publish the package or to install it on selected hosts.**

For more information, refer to the PDF *Sun Control Station 2.2 Software Installer Module*.