

Sun Cobalt™ Control Station

Health Monitoring Module



Copyright © 1997-2002 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 embodied in the product 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 other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution and decompilation, and are for use only with this product. 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, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube and the Sun Cobalt logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communication Corporation in the United States and other countries.

PostScript is a trademark or registered trademark of Adobe Systems, Incorporated, which may be registered in certain jurisdictions.

Linux is a trademark of Linus Torvalds.

Federal Acquisitions: Commercial Software - Government Users Subject to Standard License Terms and Conditions.

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 © 1997-2002 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient des droits de propriété intellectuelle sur la technologie réunie dans le produit qui est décrit par ce document. Ces droits de propriété intellectuelle peuvent s'appliquer en particulier, sans toutefois s'y limiter, à un ou plusieurs des brevets américains répertoriés à l'adresse <http://www.sun.com/patents> et à un ou plusieurs brevets supplémentaires ou brevets en instance aux Etats-Unis et dans d'autres pays.

Ce produit ou document est 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 Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, JavaScript, JDK, Sun Cobalt, Sun Cobalt RaQ, Sun Cobalt CacheRaQ, Sun Cobalt Qube et le logo Sun Cobalt sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Netscape et Netscape Navigator sont des marques de fabrique ou des marques déposées de Netscape Communication Corporation aux Etats-Unis et dans d'autres pays.

PostScript est une marque de fabrique d'Adobe Systems, Incorporated, laquelle pourrait être déposée dans certaines juridictions.

Linux est une marque de fabrique de Linus Torvalds.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

Part Number / Numéro de pièce : 816-3095-12 Rev A

Contents

1 Health Monitoring Module	1-1
Monitoring model	1-1
Active Monitor	1-2
Status colors	1-2
Health Monitor icon	1-3
Health Monitor screen	1-3
Summary	1-3
Link to Administration screen of a managed server	1-4
Viewing the health-monitoring data	1-4
Services monitored on Sun Cobalt server appliances	1-6
Services monitored on Sun Cobalt general-purpose servers	1-6
Clearing a critical event	1-7
Updating the health-status data	1-7
View all devices	1-8
Settings	1-9
Health Status polling	1-9
“I am alive” polling	1-9
Configuring the settings	1-10
Adding new services to the Health Monitoring module	1-12
Format of the configuration file	1-12
Creating a new service	1-13

Health Monitoring Module

The Health Monitoring control module on the Sun Cobalt™ Control Station allows you to monitor the health status of your managed servers according to various parameters. This document explains the features and services available through the Health Monitoring control module.

This module allows you to:

- view a summary of the health-status data for a server or group of servers
- retrieve the most recent health-status data from the managed servers
- verify that you can reach the agent on a managed server and that the server can be accessed over the network
- force the control station to retrieve immediately the most recent health-status data from an individual server.
- configure the parameters for the Health Monitoring module.
- enter an email address to receive alerts from the Health Monitoring module when there are critical system events (red circle).



Note: In most of the short procedures in this chapter, the first step is to click the **Control Modules** tab in the top menu bar and the second step is to click on a selection from the left menu bar.

To reduce the number of steps in each procedure, the menu commands are grouped together and shown in **bold** type face. Right angle brackets separate the individual items.

For example, select **Control Modules > Health Monitor > Summary** means to click the **Control Modules** tab in the top menu bar, click the **Health Monitor** menu category in the left menu bar and finally click the **Summary** sub-menu item.

Monitoring model

The model implemented for 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 polling interval or by the the managed server informing the control station when it has a problem (an “event”).

The event model allows for immediate notification when a problem is detected.



















Figure 1 shows the “Health Monitor” tables.









Note: The poller reads the Active Monitor information from each server. For more information, see “Active Monitor” in the PDF *Administrator Manual*.





Figure 1. Health Monitor tables

Clear Critical Events

Critical Events			
			6 Entries
	Device	Time/Date	Action
	10.9.33.238	Thu, 20 Sep 2001 00:10:30	 
	10.9.33.17	Fri, 21 Sep 2001 00:25:50	 
	ranga.1	Thu, 20 Sep 2001 00:17:05	 
	10.9.33.101	Thu, 20 Sep 2001 00:17:56	 
	10.9.60.3	Thu, 20 Sep 2001 00:19:44	 
	10.9.23.216	Thu, 20 Sep 2001 00:23:04	 

Device Group Status			
			3 Entries
	Group Name	Number of Appliances	Action
	Bldg_32	8	
	Bldg_33	8	
	Bldg_31	12	

Key:

-  No Information Available or Monitoring Not Enabled
-  Normal
-  Problem
-  Severe Problem

Active Monitor

Active Monitor is a utility that runs on a Sun Cobalt server appliance and updates key system and service status every 15 minutes.

The Health Monitoring Module reads portions of this information from each server and uses this information to determine the state of the server.

Status colors

The status of each service or hardware component is indicated by a grey, green, yellow or red circle beside each item. The colors have the following significance:

- **Grey**—No information is available, or the service or the monitoring feature is not enabled on the server.
- **Green**—The services and components are functioning normally.
- **Yellow**—There is moderate use on the server or a component is recovering.
- **Red**—There is heavy use on the server or a failure.

Health Monitor icon



The Health Monitor icon in the top right corner flashes red if a “critical” event is present. A critical event is generated when a transition to a “warning” or “critical” event is detected or generated through a polling interval.

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

Health Monitor screen

When you click the **Health Monitor** menu item on the left, the sub-menu items allow you to view the current status or update the status of the services and hardware components for managed servers.

The sub-menu items are:

- Summary (see “Summary” on page 1-3)
- View all devices (see “View all devices” on page 1-8)
- Settings (see “Settings” on page 1-9)

Summary

The **Summary** sub-menu item displays a summary of the health-status data for the managed servers.

When you click on the **Summary** sub-menu item, the “Critical Events” and “Device Group Status” tables appear; see Figure 1.

- The “Critical Events” table displays events that the Administrator should address immediately.
- The “Device Group Status” table displays the general status of the groups of servers on the control station.

When you click a green *magnifying-glass* icon to see more detailed information for a server, 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 server, for example, FTP server, telnet server, Email server or DNS server. These items can vary depending on the type of server you are viewing.
- The “Other System Services” table displays information on third-party or customized services that the administrator has added to a server.



Note: To add a new Health Monitoring service, see “Adding new services to the Health Monitoring module” on page 1-12.

Link to Administration screen of a managed server

In the information tables, the host name or IP address of an individual server appears as a hypertext link. If you click on a link, a new browser window opens to the Administration screen of that server.



Note: You must provide the user name and password of the administrator to access this server.

Viewing the health-monitoring data

To view a summary of the health-monitoring data on a managed server:

1. Select **Control Modules > Health Monitor > Summary**. The “Critical Events” and “Device Group Status” tables appear.
2. To view more detailed information on a server or a group, click the green *magnifying-glass* icon next to the item in the Action column. More detailed tables of information appear; see Figure 2.
3. If you view the details for a critical event, the following information tables appear:
 - Base System Components
 - Base Services
 - Other System Services

Click **Back** to return to the previous screen.





4. If you view the details for a device group, the table listing the servers belonging to that group appears.











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

Click **Back** to return to the previous screen.

Figure 2. Detailed information tables





Update Now

Base System Components - 10.9.33.17 (10.9.33.17)			
4 Entries			
	Service	Vendor	Time/Date
	CPU	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	Disk	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	Memory	Sun Cobalt	Wed, 19 Sep 2001 15:50:01
	Network	Sun Cobalt	Fri, 21 Sep 2001 00:25:50

Base Services - 10.9.33.17 (10.9.33.17)			
10 Entries			
	Service	Vendor	Time/Date
	Appleshare	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	DHCP Server	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	DNS Server	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	Email Servers	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	FTP Server	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	SNMP Server	Sun Cobalt	Wed, 19 Sep 2001 15:50:01
	Serverfisktop	Sun Cobalt	Wed, 19 Sep 2001 15:45:02
	Telnet Server	Sun Cobalt	Wed, 19 Sep 2001 15:50:01
	Web Server	Sun Cobalt	Wed, 19 Sep 2001 15:50:01
	Windows File Sharing Server	Sun Cobalt	Wed, 19 Sep 2001 15:50:01

Other System Services - 10.9.33.17 (10.9.33.17)			
0 Entries			
No data is currently available.			

Key:

-  No Information Available or Monitoring Not Enabled
-  Normal
-  Problem
-  Severe Problem

Back

Services monitored on Sun Cobalt server appliances

The services monitored on Sun Cobalt server appliances can include:



Note: Not all of these services are available on each type of Sun Cobalt server appliance.

- Active Server Pages (ASP)
- Appleshare
- Buffer Overflow Protection
- DHCP Server
- DNS Server
- Email Servers (POP / IMAP / SMTP)
- FTP Server
- JavaServer Pages (JSP) and Servlets
- Scan Detection
- Server Desktop
- SNMP Server
- Telnet Server
- Web Server
- Windows File Sharing Server

Services monitored on Sun Cobalt general-purpose servers

The services monitored on Sun Cobalt general-purpose servers (such as the Sun LX50 server) include:

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

Clearing a critical event

If you clear a critical event generated by a managed server, the control station ignores that server until the critical event or events are cleared from the server.

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

1. Select **Control Modules > Health Monitor > Summary**. The “Critical Events” and “Device Group Status” tables appear.
2. To clear a particular critical event from the table, click the red *trashcan* 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** at the top of the table.
A confirmation box appears to confirm your selection.
4. Click **OK**. The “Critical Events” table reappears with no entries.

Updating the health-status data

You can refresh the health-status data for each server; this feature causes the control station to retrieve immediately the most recent health-status data from a server.

The Update button appears in the UI when you are viewing the detailed information tables for an individual server.

To refresh the health-status data on a managed server:

1. Select **Control Modules > Health Monitor > Summary**. The “Critical Events” and “Device Group Status” tables appear.
2. Click the green *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 device group, the table listing the servers belonging to that group appears.
You can then click on the green *magnifying-glass* icon next to the server in the Action column. The same tables appear.
5. On the screen showing the detailed information tables for a server, click **Update Now** above the table. This forces the control station to retrieve immediately the health data from the managed server.
A confirmation box appears, asking if you want to update the current information.
6. Click **OK**. After a few moments, the screen refreshes with the updated information.
7. Click **Back** to return to the previous screen.

View all devices

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

1. Select **Control Modules > Health Monitor > View All Devices**. The “Managed Devices State – All” table appears, displaying the list of managed servers; see Figure 3.



Note: If there are more than 25 entries in the “Managed Devices State - All” table, the table lists the first 25 entries.

At the top or bottom of the table, you can use a pull-down menu to choose the range of entries that you want to view.

2. To access the Administration screen of a particular server, click the host name or IP address of the server (displayed as a hypertext link). You must provide the user name and password of the administrator.

The Administration screen of that server opens in a new browser window. .

3. To view more details on an individual server, click the green *magnifying-glass* icon next to the server in the Action column. The following information tables appear:

- Base System Components
- Base Services
- Other System Services

Click **Back** to return to the previous screen.

4. On the screen showing the detailed information tables for a server, you can click **Update Now** above the table. This forces the managed server to send its current health data to the control station.

A confirmation box appears, asking if you want to update the current information.

5. Click **OK**. After a few moments, the screen refreshes with the updated information.

Figure 3. View all devices table

Managed Devices State - All			9 Entries
	Device	Time/Date	Action
	lease19	Sun, 21 Apr 2002 23:47:02	
	lease20	Tue, 16 Apr 2002 16:16:35	
	10.9.32.132	Tue, 16 Apr 2002 16:36:36	
	10.9.32.134	Tue, 16 Apr 2002 16:41:02	
	bmula5	Mon, 22 Apr 2002 19:50:00	
	10.9.32.137	Sun, 21 Apr 2002 23:29:53	
	10.9.32.139	Tue, 16 Apr 2002 18:40:58	
	10.9.32.140	Tue, 30 Apr 2002 12:46:37	
	10.9.32.141	Wed, 01 May 2002 05:39:30	

- Key:
- No Information Available or Monitoring Not Enabled
 - Normal
 - Problem
 - Severe Problem

Settings

Health Status polling

The Health Status Polling Interval indicates when a polling cycle begins (for example, every four hours) for pulling the Active Monitor health data from the managed servers. However, if a polling cycle is still in progress, a second polling cycle does not begin until the first cycle has finished.

For example, if, due to the number of managed servers, a complete polling cycle takes one hour and you set the poller interval to 20 minutes, the second polling cycle does not begin until the first cycle has finished after one hour.

“I am alive” polling

This feature allows the control station to verify that the agent is still running on a managed server and that the server can be accessed over the network. It works in the following way:

- a. The control station sends a simple agent request.

If this request is successful, the agent is functioning normally and the server 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 a sample.

- b. The server 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 states that the control station cannot access the agent on the server <IP address>.

If this ICMP ping is not successful, the health-monitoring information table states that the control station cannot access the server <IP address> over the network.

Configuring the settings

To configure the settings for the Health Monitoring control module:

1. Select **Control Modules > Health Monitor > Settings**. The “Health Monitor Properties” table appears; see Figure 4.
2. You can configure the following parameters:
 - **Enable Event.** If you enable the check box, all of the managed servers send to the control station any events that are generated on the servers. 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. You may want to disable this feature in order to reduce network traffic. This feature does not affect the events that are detected during a polling interval.
 - **“I am alive” Polling Interval.** Set the interval at which the control station attempts to communicate with the managed appliance(s). Use the pull-down menu to select a value or to disable this feature.
 - **Health Status Polling Interval.** Set the interval at which the control station requests the health data from the managed servers. Use the pull-down menu to select a value or to diable this feature.
 - **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 server’s administrator when adding the server to the control station, that email address also receives from the Health Monitoring Module the notifications for that particular server.

- **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; a 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; a 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; a recommended maximum is 90. For example, a value of 80 means that a yellow alarm is generated when the 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; a recommended maximum is 95. For example, a value of 90 means that a red alarm is generated when the 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; a recommended maximum is 75. For example, a value of 50 means that a yellow alarm is generated when the 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, a recommended maximum is 90. For example, a value of 75 means that a red alarm is generated when the 75% of the memory is in use.
3. Click **Save**. The “Health Monitor Properties” table refreshes.

Figure 4. Health Monitor Properties table

Health Monitor Properties	
Enable Event	<input checked="" type="checkbox"/>
I am alive Polling Interval	every 5 minutes
Health Status Polling Interval	every 60 minutes
Notification Email Address <i>(optional)</i>	<input type="text"/>
Base Service Threshold Defaults	
CPU Yellow Alarm	3
CPU Red Alarm	6
Disk Yellow Alarm	85
Disk Red Alarm	90
Memory Yellow Alarm	50
Memory Red Alarm	75

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 Cobalt 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 (meaning that the Health Monitoring icon returns to normal).

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 of the state presented in the Health Monitoring tables. The states are defined as:

- State 0 = Unavailable service (gray circle)
- State 1 = Service is functioning normally (green circle)
- State 2 = Warning state (yellow circle)
- State 3 = Critical state (red circle)

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 15 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 the Health Monitor icon in the top-right corner begins to flash.

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 service

To create a new Health Monitoring service:

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

Name the configuration `filename.conf` (for example, `cobalt_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/cobalt_db.pl
vendor Vendor Test
interval 10
name Database Check
description DB Monitor
state0msg The database server is not monitored/state unavailable.
state1msg The database server is online.
state2msg The database server is in limbo.
state3msg The database server is offline.
```

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 (`cobalt_db.pl`) would look like:

```
#!/usr/bin/perl
use Cobalt::Meta;

$PGDATABASE = "cobalt";
$PGPORT      = 5583;
$PGUSER      = "admin";

## Check whether you can connect to the database
$dbc = Cobalt::Meta::connect($PGDATABASE, $PGUSER, $PGPORT);
if ($dbc && $dbc->status eq Pg::PGRES_CONNECTION_OK) {
    print "connection to db is successful.. \n";
    Cobalt::Meta::db_reset($dbc);
    exit 1;
}
else {
    print "error connecting to db.. \n";
    exit 3;
}
```

In this case, there are only two possible states: the database is either online or offline. The only two states required are 1 and 3. The configuration file could have just two state messages:

```
state1msg The database server is online.
state3msg The database server is offline.
```

3. In the install script, include the following directive specifically for the new Health Monitoring service.
 - Copy the configuration file and the monitor script to the correct locations.
4. Create a package file for each type of server on which you wish to install this new Health Monitoring service (for example, a Sun Cobalt CacheRaQ™ 4 and a Sun Cobalt Qube™ 3).
5. Upload the package to the control station through the Software Management Module. Use Software Management Module either to publish the package or to install on selected servers.

For more information, refer to the PDF *Software Management Module*.