Availability Monitor (Availmon) Reference Guide

Document Number 108-0169-002

Contributors

Written by Greg Russell and Julie Knoeller
Edited by Cindi Leiser
Illustrated by Srinivasa Phanindra and Dany Galgani
Production by Cindy Stief
Engineering contributions by Wei-Lun Kao and Srinivasa Phanindra

Availability Monitor (Availmon) Reference Guide
Document Number 108-0169-002

Contents

Figures

Tables

Introduction

This introduction contains important information to help you use this reference guide; it defines the typographic conventions that are used to convey meaning, and it also defines terminology that is specific to this document.

To report problems with this document such as missing or inaccurate information, send e-mail to:

`piglet@csd.sgi.com`

For questions regarding Availmon, please send e-mail to

`sri@csd.sgi.com` or `ist@csd.sgi.com`

We appreciate your feedback; a feedback form is located at:

http://ist.csd.sgi.com/Tools/Misc_pages/Tools_Feedback_rpt.html

(Accessible only to SGI employees.)

The Scope of This Document

The audience for this document comprises engineers, analysts, support personnel, and field service personnel. The scope of this document includes the following information:

- Chapter 1, “Introduction to the Availability Monitor,” is an overview of Availmon features and theory of operation.
- Chapter 2, “Availmon Installation, Registration, and Administration,” provides detailed installation, registration, and administration procedures that enable the user to configure and manage Availmon.
- Chapter 3, “Availmon Events, Reports, and Metrics,” describes Availmon reports, events, and metrics in detail.
- Chapter 4, “Retrieving Availmon Data,” describes how to access reports both locally and remotely.

Typographic Conventions

This document uses the following typographic conventions:

Convention	Meaning
`TYPEWRITER FONT`	Denotes literal items such as command names, file names, routines, directory names, path names, signals, messages, and programming language structures.
italic font	Denotes variable entries and words or concepts being defined.
`bold typewriter font`	In screen drawings of interactive sessions, denotes literal items entered by the user. Output is shown in nonbold typewriter font.
[]	Indicates an optional item.
<>	Indicates a required variable within an optional item.

Man Pages

Within this document, reference is made to the online man pages available under IRIX™ through the `man` command. A *man page* is a discussion of a particular element of the IRIX operating system or a compatible product.

Each man page includes a general description of one or more commands, routines, or other topics and provides details of their usage (command syntax, routine parameters, system call arguments, and so on). If more than one topic appears on a page, the entry will appear in the printed manual alphabetized only under its major name. You can access a man page named `amreport` online by entering **`man amreport`**.

Man pages are grouped into sections that are numbered from 1 to 8. Each section contains entries of a particular type. Types of entries include user commands (1), administrator commands (8), system calls (2), library routines (3), file formats (5), and device descriptions (4).

Section numbers appear in parentheses after man page names. Man pages are referenced in text by entry name and section number, such as amreport(1M). Availmon commands are discussed in detail in their corresponding man pages; they are located in section 1M (user commands).

Definition of Terms

The following terms and phrases appear in this document and have the following definitions:

- *Enter* means either to type a command or to select a menu command and then press the Enter key on your keyboard.
- *Event code* is the unique identifier of the system event that is the reason for sending an Availmon report. Events range from registration to reboot.
- *Hostname* is the internet address of the system as returned by `gethostname()` or `gethostbyname()` if `gethostname()` fails.
- *Old platforms* are systems that cannot return a machine-readable system serial number, which include platforms *not* in the following list: IP19, IP21, IP22, IP25, IP26, IP27, IP28, IP30, IP32.
- *Site logfile* is an appended accumulation of Availmon reports from different systems.
- *Start time* is the exact time that the system booted up to multi-user mode (init level 2).
- *System serial number* is the machine-readable serial number as returned by `syssgi(SGI_SYSID, ...)`. For older systems that have no machine-readable value, one must be specified explicitly using `amregister`.
- *System version*, for software:

  ```
  uname -a
  ```

  ```
  versions -n eoe.sw.unix support.sw.fru “patchSG*”
  ```

  For hardware:

  ```
  hinv -mvv
  ```

  ```
  gfxinfo -vv
  ```

Chapter 1

Introduction to the Availability Monitor

This chapter provides an overview of Availability Monitor (Availmon) features and theory of operation. You should fully understand the material in this chapter before you advance to Chapter 2, “Availmon Installation, Registration, and Administration”

1.1 Availmon Overview

The Availmon tool is a set of programs that collectively monitors and reports the availability of systems, and it also reports the diagnosis of system crashes. Availmon identifies the cause of a given shutdown by gathering information from diagnostic programs like ICRASH, FRU Analyzer, Syslog; and system configuration from versions, gfxinfo, and hinv. Availmon can also perform the following tasks:

- report data to various locations, depending on the configuration
- provide local statistics of system availability
- provide limited site-management facilities

Data gathered by Availmon can be sent to the Availmon database, which is maintained by Silicon Graphics. You may also access this database through the Web. Refer to Chapter 4, “Retrieving Availmon Data,” for more information on how to use the database.

1.1.1 Components of Availmon

Some important components of Availmon are as follows:

- `amconfig`, which is the base configuration tool for Availmon. For example, it allows the system administrator to control the transmission of e-mail reports to any set of addresses, to turn on or off shutdown request information, or to turn on or off the ticker daemon.
- `amregister`, which allows a system administrator to enable or disable the automatic sending of e-mail reports and which sends registration or deregistration reports in acknowledgment.
- `amreport`, which prints out statistical and availability information based on the reports generated after the system is taken down (for any reason). Normally, the information that it presents is hierarchical.

- `amsend`, which transmits (e-mail) reports in a specified format to specified e-mail addresses. `amsend` can be used if `autoemail` is not set.
- `amreceive`, which converts e-mail sent by `amnotify` or `amsend` back into the original report format. `amreceive` can select all reports or only a given report type (availability or diagnosis).

Refer to the man pages for more detailed information on Availmon components.

Availmon is embedded in system boot and shutdown processes. It differentiates controlled shutdowns, system panics, and system hangs. On high-end systems such as IP19, IP21, IP25, and IP27, it can further differentiate NMIs, power cycles, and power failures. A light-weight ticker daemon can be used to track uptime and send status reports.

1.1.2 Source Programs Used by Availmon

Availmon collects diagnostic and availability information from the following programs:

- ICRASH

  ICRASH is a hands-on utility that generates detailed kernel information in an easy-to-read format. ICRASH also enables report generation about system crash dumps that `savecore(1M)` creates. Depending on the type of system crash dump, ICRASH can create a unique report that contains information about what happened when the system crashed. (Refer to the *ICRASH Reference Guide*, Silicon Graphics publication number 108-0167-001, for detailed information about ICRASH.)

- Syslog

  Syslog prepares system status messages for entry into the system log. These messages contain a priority component (such as panic, immediate, critical, warning, and informational), and a facility (originator) component (such as kernel, user, mail, and daemon).

- hinv

  `hinv` provides the contents of the system hardware inventory table. This table is created each time the system is booted, and it contains entries that describe various pieces of hardware in the system. The items in the table include main memory size, cache sizes, the floating-point unit, and disk drives.

- versions

  `versions` provides information about the software that is currently installed on your system and the software that has been available for installation but is not presently installed. `versions` also displays lists of files on your system and information about those files.

- gfxinfo

  `gfxinfo` extracts the type of each graphics subsystem resident and displays information that is relevant to the various pieces of hardware located in each. The displayed material may include the subsystem type, the number of boards, the number of screens attached, and so forth.

1.1.3 When to Use Availmon

Some of the situations in which Availmon might be helpful include but are not limited to these:

- keeping track of hardware, software, and patches
- maintaining system availability data
- providing statistical information that relates to system availability
- finding the cause of a system shutdown or panic
- providing limited site-management facilities

A central Silicon Graphics database maintains all diagnostic and availability data for participating systems. Access to that database provides overall reliability data and a specific problem history for individual systems.

All aspects of Availmon operation are fully configurable.

1.1.4 Availmon Reporting Structure

The following diagram graphically illustrates the reporting structure.

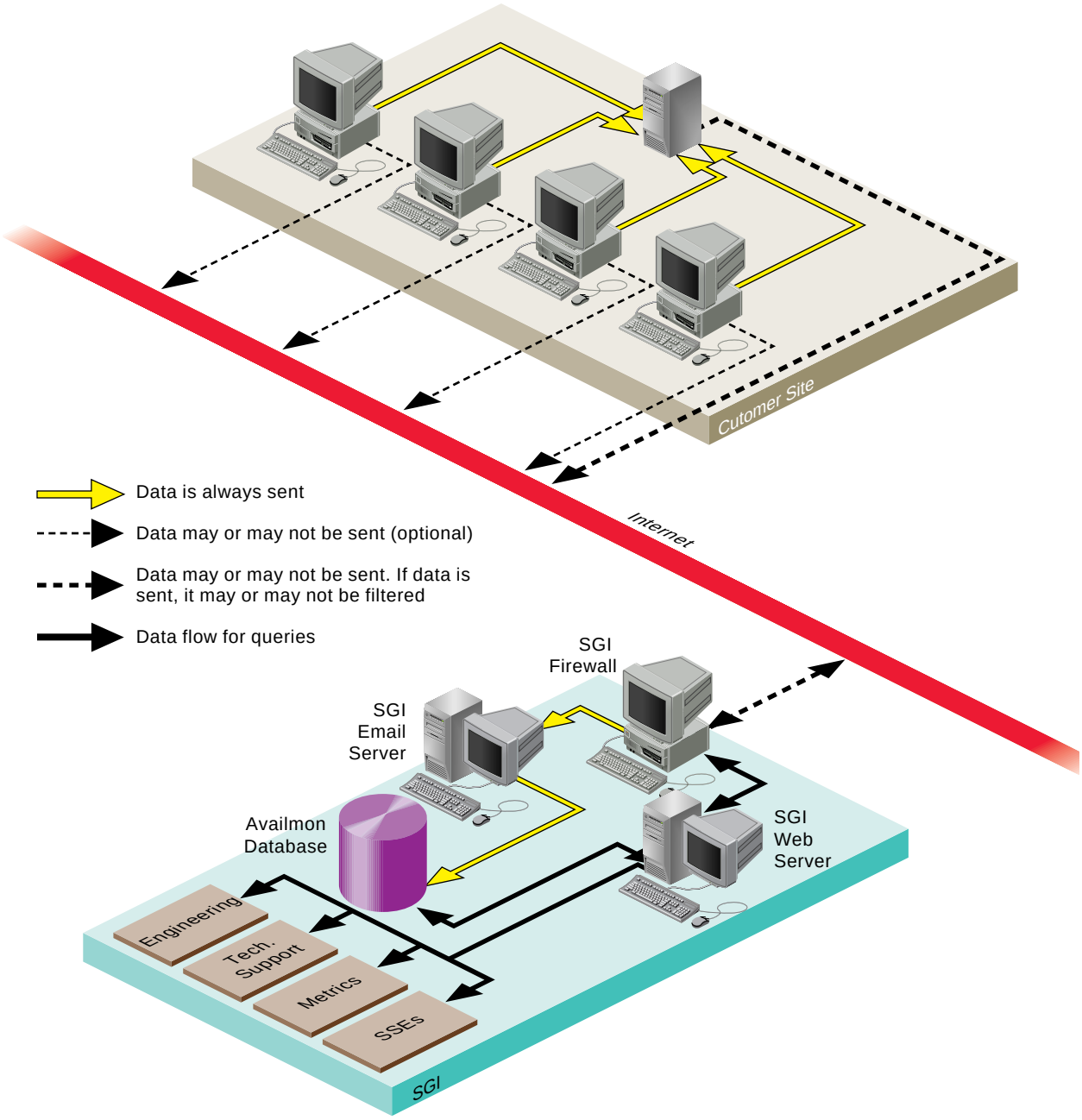

Figure 1-1 Availmon Reporting Structure

1.2 Theory of Operation

1.2.1 Registration of Availmon

You must register your system to enable the distribution of Availmon reports. For instructions on how to register your system for Availmon use, refer to Section 2.2, “Registration.”

Note: This process is not to be confused with customer registration; registration of Availmon only enables automatic delivery of data available on local systems.

1.2.2 Configuration

Availmon can be configured to operate in a number of ways:

- base configuration, which includes local system reporting only.
- base configuration plus registration of local e-mail, which includes local e-mail reports to a person or a centralized system.
- base configuration with Silicon Graphics registration, which sends e-mail reports to Silicon Graphics databases.
- custom configuration, which can include special e-mail lists, delivery to chatty pagers, and so on.

1.2.3 Report Types

There are three types of reports: availability, diagnosis, and pager reports. Availability reports consist of previous start time, event code, approximate time event occurred, start time, and a summary of the reason for the crash (where relevant). Diagnosis reports additionally contain the crash analysis report, FRU Analyzer result, important syslog messages, and system hardware and software configuration and version information. Pager reports include the hostname, event code description, and summary and are sent only to specified pager recipients.

Refer to Section 2.3 for information on Availmon files and directories, to Chapter 3 for detailed information on report types, and Chapter 4 for how to access the Availmon database.

1.2.4 Mailing Reports

You can configure Availmon reports for mailing in two ways: automatic or manual. In the automatic process, you can configure any number of recipients for each type of report. The recommended configuration is to send a diagnosis report to Silicon Graphics for entry into the Availmon database. Other examples of e-mail configuration include availability reports to the site system administrator and diagnosis reports to local Silicon Graphics field service personnel. In the manual process, two types of reports are created in the directory

/var/adm/crash. System administrators can "censor" or filter the reports and then use the `amsend` utility to transmit the filtered reports.

You can also configure Availmon to compress and encode data. At the receiving end, a conversion program called `amreceive` decodes and uncompresses the data. Data encryption, if not prohibited, is recommended.

1.2.5 Viewing Reports

The `amreport` program reviews saved availability report information and provides statistical and event history reports. By default, it will process the availability data on the local system, which is saved automatically by Availmon. The `amreport` program can also process received aggregate Availmon reports; that is, an appended accumulation of Availmon reports from different systems, which is referred to as a site logfile.

`amreport` runs interactively to view statistical or event history reports, or it can write such reports to standard output; `amreport` also accepts *from* and *to* arguments, which can be used to bound the time period being reported.

Refer also to Section 3.3, "Metrics" and Section 4.1, "amreport" for further information.

1.3 Installable Images

Availmon 2.1 is available as a patch for IRIX releases 5.3, 6.2, and 6.4.

Determine your operating system version by entering the command **`uname -r`**. You can install the latest version of Availmon (for a given OS release) from the following list:

IRIX 5.3 — Install patch 2002 from your local patch server.

IRIX 6.2 — Availmon is bundled with the base IRIX version. Install patch 2003 from the local patch server to update to Availmon 2.1.

IRIX 6.4 — Availmon is bundled with the base IRIX version. Install patch 2004 from the local patch server to update to Availmon 2.1.

You can obtain a patch in three ways:

- Support patches are available on your Internal Support Tools CD.
- Support patches are available to registered users from the Patches Resource on the Web at:
  http://www.sgi.com/Support/patch_intro.html
- You may call 1-800-800-4SGI from within North America or your local service provider from outside North America and request the patch.

Refer to Section 2.1 for installation instructions.

1.4 Configuration Control

Availmon has five configuration options and one e-mail list configuration file. The five options control particular functions of Availmon:

- `autoemail` enables automatic distribution of Availmon reports (normally turned on with `amregister`).
- `shutdownreason` enables querying for a controlled shutdown reason.
- `tickerd` enables running a light-weight daemon to monitor uptime.
- `hinvupdate` enables checking the changes of `hinv` and `gfx` information.
- `statusinterval` enables notification that the system is still running and reports are still enabled after some duration.

These flags should be turned on or off through `amconfig`. The e-mail list configuration file, `autoemail.list`, is used to control the report type, e-mail format, and e-mail addresses for Availmon reports. The e-mail list is maintained with `amconfig`.

The default configuration during installation is `autoemail` off; `shutdownreason` on, `tickerd` on, and `hinvupdate` on for high-end systems (off otherwise); `statusinterval` 60 days; and `autoemail.list` configured for a diagnosis report to be sent to Silicon Graphics.

Table 1-1 shows the configuration values and defaults.

Table 1-1 Availmon Configuration Values

Configuration Option	Value	Low-End Default	High-End Default
autoemail	on | off	off	off
autoemail.list	file	*	*
shutdownreason	on | off	off	on
tickerd	on | off	off	on
hinvupdate	on | off	off	on
statusinterval	<days>	60	60

Note: The autoemail.list default is the same for all platforms and is:
`diag (compressed, encrypted): availmon@csd.sgi.com`

Initial configuration and enabling autoemail distribution of Availmon reports is easily accomplished with `amregister`.

Chapter 2

Availmon Installation, Registration, and Administration

2.1 Installation Instructions

Patch software is installed like any other Silicon Graphics software product. Follow the instructions in your *Software Installation Administrator's Guide* to bring up the miniroot form of the software installation tools.

Select the location from which the patch has to be installed and follow these steps to install the patch:

1. At the `Inst>` prompt, enter:

   install patchSGxxxxxxx

   where **xxxxxxx** is the patch number.

2. Initiate the installation sequence by entering:

   `Inst>` **`go`**

3. You may find that two patches have been marked as incompatible. (The installation tools reject an installation request if an incompatibility is detected.) If this occurs, you must deselect one of the patches:

   `Inst>` **`keep patchSGxxxxxxx`**

   where **xxxxxxx** is the patch number.

4. After completing the installation process, exit by entering:

   `Inst>` **`quit`**

2.2 Registration

After installation and reboot, run `amregister` to turn on `autoemail` and register the system. You must register your system to enable the sending of Availmon reports.

For single systems that are not an *old platform* where the default configuration is functional, running `amregister -r` is sufficient to register.

For multiple systems, run `amconfig` on one system to set up a common e-mail configuration file (`/var/adm/avail/autoemail.list`) and copy this file to all the systems. Then run `amregister -r` on each system.

Note: You should follow this procedure before registering all systems because initial availability reports will be sent out when registering.

If you want a site logfile for multiple systems, create a pseudo e-mail alias to pipe availability reports to `amreceive`, whose output is then appended to the site logfile.

After setting up Availmon, run `amreport` on each system to view the availability statistics and reports for that system, or run `amreport`, using the site logfile as input, to view overall availability statistics for all systems and availability reports for any system. Refer to Section 4.1 for detailed information on `amreport`.

After you register your system, you can confirm registration by viewing the Web site at:

http://availmon.csd.sgi.com/availmon/

The following examples explain how to register Availmon. The first two examples are for standard customers who automatically transmit reports outside the site; the other two examples are for secure sites that do not transmit reports outside the site but may or may not use an internal reporting process. The reports can be filtered before they are sent. A sample display follows each example.

2.2.1 Standard Example for a Single System

The following registration sequence applies to customers who automatically transmit reports outside their site.

1. If Availmon is installed on only one system, reboot the system after installation.
2. Log on as root. If you are satisfied with the default Availmon configuration, and you are not running on an old platform, you can complete Availmon registration by entering `amregister -r`. Otherwise, proceed with Step 3.
3. Enter **`amregister`** without any argument to register and configure the e-mail lists.

   This step turns on `autoemail` and sends registration reports to all configured addresses when complete. If the system is not an IP19, IP21, IP22, IP25, IP26, IP27, IP28, IP30, or IP32 system, `amregister` asks you to enter the serial number of the system (located on the back of the CPU cabinet). `Shutdownreason`, `tickerd`, `hinvupdate`, and `statusinterval` can be changed anytime. Refer also to the man page `amconfig(1M)` for more information. The default `autoemail.list` is:

   ```
   availability(compressed,encrypted):
   availability(compressed):
   availability(text):
   diagnosis(compressed,encrypted): availmon@csd.sgi.com
   diagnosis(compressed):
   diagnosis(text):
   pager (concise text):
   ```

4. Enter the following arguments, if desired:

   ```
   availability(text): <local_sysadmin>
   diagnosis(compressed,encrypted): <local_SGI_support>
   ```

5. For locations where encrypted e-mail data is prohibited, move those addresses from the `(compressed, encrypted)` lists to the `(compressed)` lists.

The following display illustrates the standard registration process (using default responses):

```
oddity 3# amregister
Do you want auto-email on? [y/n] (y)

The availability report will be sent to:
        in compressed and encrypted form:
        in compressed form:
        in plain text form:

The diagnosis report will be sent to:
        in compressed and encrypted form:  availmon@csd.sgi.com
        in compressed form:
        in plain text form:

The pager report will be sent to:
        in concise text form:

Do you want to modify the addresses? [y/n] (n)
```

Note: If you wish to modify the addresses, enter **y** in response to this question. The registration program will call up the file `/var/adm/avail/config/autoemail.list`. Using the vi editor, enter your changes at this time. After you exit vi, the registration display reappears containing the revised information. This process repeats until you enter **n** in response to the address modification question.

2.2.2 Standard Example for Multiple Systems

If Availmon is installed on several systems, and if you wish to create a site logfile and perform automatic registration, use the following procedure:

1. After you have installed Availmon and rebooted all the systems, create an e-mail alias in the system's aliases on the mail server or on only one system.
2. Pipe the availability reports to `amreceive`, and then append the output to a file. For example, if the site logfile is `/disk/amrlog`, add one line to the mail server's `/etc/aliases`: **`amrlog: | /var/adm/avail/amreceive >> /disk/amrlog`** and enter **`newaliases`** to set up this e-mail alias.
3. Run `amconfig` on one system to configure the e-mail lists. For example:

```
availability(compressed,encrypted):
availability(compressed):
availability(text): <local_sysadmin> amrlog
diagnosis(compressed,encrypted):availmon@csd.sgi.com <local_SGI_support>
diagnosis(compressed):
diagnosis(text):
```

4. Copy `/var/adm/avail/config/autoemail.list` from this system to the rest of the systems.
5. Enter **`amregister -r`** on all IP19, IP21, IP22, IP25, IP26, IP27, IP28, IP30, and IP32 systems. Using a script and the `rsh` command, you can automate this process.

6. If `shutdownreason`, `tickerd`, `hinvupdate`, or `statusinterval` needs to be turned off for some high-end systems or turned on for some low-end systems, enter **`amconfig shutdownreason off (on)`** or **`amconfig tickerd off (on)`**, etc. on those systems. For old platforms enter `amregister -r -s <serial_number>` to specify serial numbers.
7. After everything is set up, `amreport -s /disk/amrlog` will show the overall statistics, system statistics, and individual availability reports.

2.2.3 Example for Secure Sites with Internal Report Mailing

This setup procedure is similar to the standard examples in Section 2.2.1, "Standard Example for a Single System" and Section 2.2.2, "Standard Example for Multiple Systems," (excluding `availmon@csd.sgi.com` and `<local_SGI_support>` from `autoemail.list`). After the system administrators have received the Availmon reports, they can check the latest diagnosis report (which is located in `/var/adm/crash/diagreport` on the system that was just rebooted), delete any sensitive data, and use `amsend` to mail the filtered report to *availmon@csd.sgi.com* and to local SGI support people. If the diagnosis report contains any ICRASH, Syslog, hinv, versions, or gfxinfo data, enter

```
amsend -i -z -x availmon@csd.sgi.com <local_SGI_support>
```

to mail the report. If there is no such data in the report, enter the following:

```
amsend -d -z -x availmon@csd.sgi.com <local_SGI_support>
```

If encrypted data in e-mail is prohibited, remove `-x` from the command.

Example 2-1 illustrates the registration process for secure sites with internal report mailing.

Example 2-1 Registration Process

```
oddity 3# amregister
Do you want auto-email on? [y/n] (y)

The availability report will be sent to:
        in compressed and encrypted form:
        in compressed form:
        in plain text form:

The diagnosis report will be sent to:
        in compressed and encrypted form: <system_administrator>
        in compressed form:
        in plain text form:

The pager report will be sent to:
        in concise text form:

Do you want to modify the addresses? [y/n] (y)
```

Note: Any reports received by the system administrator or by a local machine should be piped through `amreceive` to produce correct Availmon reports. Refer to Section 2.2.2, "Standard Example for Multiple Systems," to set up an alias using `amreceive`.

2.2.4 Example for Secure Sites without Report Mailing

There are no special set-up needs for this case. However, for platforms without IP19, IP21, IP22, IP25, IP26, IP27, IP28, IP30, and IP32 boards, you should still run `amregister -s <serial_number>` to specify serial numbers. `Shutdownreason` and `tickerd` can also be turned on or off.

Because there is no report mailed after the system reboots, system administrators must determine if the system has been down and then check the reports to determine the reason. If the system crashes more than once before checking, the old reports are overwritten by new reports (core dumps and ICRASH reports will be kept until explicitly removed). Therefore, Silicon Graphics recommends internal report mailing for secure sites.

You can transmit diagnosis reports to Silicon Graphics using `amsend` in Section 2.2.3, "Example for Secure Sites with Internal Report Mailing," or you can run `amconfig` to configure standard e-mail lists so that when reports must be sent, `amnotify` transmits the reports accordingly.

The following display illustrates the registration process for secure sites without internal report mailing (for old platforms only):

```
oddity 2# amregister -s <serial_number>
Do you want auto-email on? [y/n] (y)n
```

2.2.5 Adding and Deleting E-mail Addresses with amconfig

After e-mail is enabled (`amregister -r` has been run), if you run `amconfig autoemail.list` to add or delete an e-mail address, `amconfig` sends a registration report to each address that you add and a deregistration report to each address that you delete. This means that the following two sequences *yield the same results*:

- From the default state, run `amconfig autoemail.list`.

  Add `<address>` to an e-mail list.

  Run `amregister -r`.

  Reports are sent to both *availmon@csd.sgi.com* and to `<address>`.

- First run `amregister -r` (this results in a registration report being sent to *availmon@csd.sgi.com*).

  Run `amconfig autoemail.list` and add `<address>` to an e-mail list (this results in a registration report being sent to `<address>`)

For example, suppose there is a system administrator who has already registered with the default `autoemail.list`. He or she then wants to add the `<local-admin>` e-mail alias and wants to be absolutely sure that a registration report is sent to `<local-admin>`. Just adding `<local-admin>` directly with `amconfig autoemail.list` will do exactly that, but the administrator may decide to run the following sequence instead:

```
amregister -d
amconfig autoemail.list # to add <local-admin>
amregister -r
```

This method sends a confusing and superfluous deregistration and registration sequence to *availmon@csd.sgi.com* (or any other configured address).

`amconfig` can be run interactively from the command prompt to configure the options. For example, to turn off the prompting of shutdown reasons, you can enter the following command:

```
amconfig shutdownreason off
```

Note: Availability data is always recorded locally and `amreport` can always view local metrics and incidents; registration is not required.

2.2.6 Using Pager Notification

The pager notification option enables users of Availmon to post a minimized version of an availability report to the configured address. This address may be an alias to a chatty pager. Follow the instructions that Section 2.2.1 lists, and specify a pager address.

2.3 Availmon Files and Directories

On IRIX releases 6.2 and above, Availmon is located in the following directories:

- Availmon components and raw data logs reside permanently in `/var/adm/avail/*`
- The most recent availability report is stored in `/var/adm/crash/availreport`
- The most recent diagnostic report is stored in `/var/adm/crash/diagreport`
- The most recent single-user availability report is stored in `/var/adm/crash/availreport.su`
- The most recent single-user diagnostic report is stored in `/var/adm/crash/diagreport.su`
- The most recent pager report is stored in `/var/adm/crash/pagerreport`

Availability information is permanently stored in `/var/adm/avail/availlog`.

Caution: Files in `/var/adm/avail` are maintained by Availmon and should not be deleted, modified, or moved.

The most recent availability and diagnostic reports are subject to removal like core dumps.

Chapter 3

Availmon Events, Reports, and Metrics

This chapter describes event codes, provides event code listings, and describes various report types, report syntax, and metrics.

3.1 Events

An event in Availmon initiates the sending of a report. Examples of events include controlled shutdowns, system panics, registration, system ID change, and so on. Each event is associated with an event code. The following sections describe in detail these event codes and their associated events.

3.1.1 Event Codes

The event code in any Availmon report uniquely identifies the cause of the report. An event code is a signed integer value, but you should never consider event codes as an ordered sequence; for example, event codes c1, c2: c1 < c2 or c1 < 0 have no inherent meaning.

In the case of a controlled shutdown, if `shutdownreason` is configured ON, you are prompted to identify the reason for rebooting the system or for bringing the system down to single-user mode. Enter the reason for shutdown as prompted by the system:

```
Please select one of the following choices by number:
     1.) Administrative
     2.) Hardware upgrade
     3.) Software upgrade
     4.) Fix/replace hardware
     5.) Install patch
     6.) Fix software problem
```

In the case of an uncontrolled shutdown or other events, Availmon gathers information from various diagnostic packages to try to identify the event.

Note: Please do not reset the machine or cause an NMI when the system is dumping information as a result of a previous panic as it may result in Availmon reporting an incorrect event.

3.1.2 Event Code Listings

Table 3-1 lists the event code groups, event codes, and their descriptions.

Note: Time in single-user mode is treated as downtime, just as for unexpected or controlled reboots.

Event codes 1 through 7 represent the old shutdown reasons from Availmon versions prior to 2.1. These codes are obsolete in Availmon 2.1, and they are replaced by 11 through 16 for reboot and 21 through 26 for single-user mode. The obsolete event codes are marked with an asterisk (*) in the following table.

Table 3-1 Event Code Descriptions

Group	Code	Description
Registration		
	-8	De-registration
	-9	Registration
Update		
	-13	Status update
	-18	System ID change
Controlled Shutdown		
	0	System shutdown, cause unknown
Reboot		
	-1	Timed-out waiting for shutdown reason
	-2	Shutdown reason unknown (not configured)
	11	Administrative
	12	Hardware upgrade
	13	Software upgrade
	14	Fix/replace hardware
	15	Install patch
	16	Fix software problem
	1*	Environmental reasons
	2*	Upgrade/add hardware or peripheral
	3*	Replace failed hardware component
	4*	Install software that requires reboot
	5*	Scheduled reboot/routine maintenance
	6*	Software problem

Table 3-1 (continued) Event Code Descriptions

Group	Code	Description
	7*	Other unclassified reasons
Single User		
	19	Timed-out waiting for shutdown reason
	20	Shutdown reason unknown (not configured)
	21	Administrative
	22	Hardware upgrade
	23	Software upgrade
	24	Fix/replace hardware
	25	Install patch
	26	Fix software problem
Unexpected Reboot		
	-3	Panic, unknown cause
	-4	Panic, hardware fault
	-5	Interrupt
	-6	System off
	-7	Power failure
	-14	Panic, software fault
	-15	NMI
	-16	System reset
	-17	Power cycle
Live Diagnostics		
	-10	No error
	-11	Hardware error
	-12	Software error

3.2 Reports

The following sections describe report types and syntax.

3.2.1 Report Types

Table 3-2 outlines and describes the types of reports that Availmon sends. The table also indicates who receives the reports and what they contain. Table notations (A, D, and P) are described in footnotes. Reports are sent to the e-mail addresses specified in the `autoemail.list` configuration file [refer also to man page amconfig(1M)]. This allows specification of e-mail addresses for availability, diagnostic, and pager reports.

Table 3-2 Availmon Reports

Report	A[a]	D[b]	P[c]	Description
Registration	X	X		Notification to new e-mail address that the system is enabled to send reports to that address; D reports additional system information.
Deregistration	X	X		Notification to e-mail address that the system will no longer send reports; same report sent to A and D.
ID Correction	X	X		Notification that a change in the system serial number or hostname has been detected at reboot; same report sent to A and D.
Status Update	X	X		Reminder that a system is still up; same report sent to A and D.
Reboot	X	X	X	Sent on every system reboot, including return from single-user to multi-user mode. A includes basic time information and summary. D adds system version information and diagnostic information (Syslog, ICRASH, FRU Analyzer). P includes concise message intended for chatty pager.
Resend	X	X		A reboot report that is resent through `amreport` after the fact; like reboot report except diagnostic report may contain less data and no pager report.
Live Diagnostic		X		Report from a live system; currently used for IRS audit and KPM diagnostic reporting.

a. A stands for the set of e-mail addresses configured to receive availability reports.

b. D stands for the set of e-mail addresses configured to receive diagnostic reports.

c. P stands for the set of e-mail addresses configured to receive pager reports.

As the previous table shows, most reports are sent to both groups A and D; the form of the report is either the same for both, or the diagnostic report is a superset of the availability report. Pager reports are sent only for reboots, and diagnostic reports are sent for live diagnosis.

All reports identify the system by system serial number and hostname and include the event code that uniquely identifies the cause of the reported event.

3.2.2 Report Syntax

Availmon reports can be sent in plain text, compressed, or compressed and encrypted formats, as specified in `autoemail.list` [see man page amconfig(1M)].

Reports should be piped to `amreceive`, which always produces the correct plain text report. The e-mail subject defines the format of the report and is required so that `amreceive` can determine how to process the report.

Note: Pager reports are an exception and should not be piped to `amreceive`; they are sent only in plain text form and are intended strictly for chatty pagers. The content of a pager report is concise: hostname, event code description, and summary. Further discussion in this section excludes pager reports.

3.2.2.1 E-mail Report Subject

The Availmon e-mail report subject has the following form:

```
AMR-<t>[-R]-<f>
    type <t> =
    A : availability
    D : diagnostic
    I : “interesting” diagnostic (*)
```

`-R` is included only for Registration | Deregistration reports

```
format <f> =
    T     : plain text
    Z-U   : compressed(Z), uuencoded(U)
    Z-X-U : compressed(Z), encrypted(X), uuencoded(U)
```

(*) “interesting” diagnostic reports include ICRASH or Syslog or FRU Analyzer [refer to the man page `amreceive(1M) -i` option]

3.2.2.2 Report Syntax

Reports consist of a sequence of field | value records, which have two record formats:

(1) a scalar value (one line)

(2) a report value (multiple lines)

A `FIELDNAME` is a reserved word and is always uppercase. The | is used as a separator.

```
(1) FIELDNAME|<value>
```

`<value>` is always terminated by a new line; there may be multiple components of the value, which are also separated by “|”, such as `<v1>|<v2>|...`

```
(2) FIELDNAME|begin
...
FIELDNAME|end
```

The “report” consists of all lines between the FIELDNAME begin and end lines. There are no syntactic constraints on the body of the report, except that it cannot contain a line with the exact content FIELDNAME|end.

3.2.2.3 FIELDNAME Definitions

Every Availmon report identifies the sending system and the Availmon version:

```
SERIALNUM|<string>
HOSTNAME|<string>       # <<hostname>>
AMRVERSION|2.1          # pre-2.0 reports don't include this field
```

Every Availmon report identifies the event:

```
EVENT|<event code>|<timestamp>|<date-string>
```

The time is the time when the event occurred: the time the system went down in the case of a reboot. An absolute time is represented as:

<timestamp>|<date-string> where:

<timestamp> - number of seconds since Jan 1, 1970

<date-string> - date string in the default format (see date(1), +%c option)

The other times included in reports are:

```
PREVSTART|<timestamp>|<date-string>[|NOTMULTIUSER]
START|<timestamp>|<date-string>[|NOTMULTIUSER]
LASTTICK|<timestamp>|<date-string> (or LASTTICK|-1|unknown)
```

PREVSTART and START represent start times. PREVSTART is the start time preceding this report; for a reboot report (including single-user), it is the start time before the system went down. START is always the start time when the system came back up, immediately preceding the Availmon report being sent.

There is one special case for the START or PREVSTART time in which the time is not strictly a start time. This occurs when the system is taken down to single-user mode, and then a controlled or an unscheduled reboot occurs while it is still in single-user mode. In this case, the START time that marks the end of the single-user interval appends |NOTMULITUSER to the end. The PREVSTART time for the subsequent reboot event also includes |NOTMULITUSER. The use of |NOTMULTIUSER distinguishes the above case from one where a system returning from single-user mode to multi-user mode panics immediately upon re-entering multi-user mode.

LASTTICK is the time recorded by amtickerd (when enabled). This normally records the time every 5 minutes (configurable). LASTTICK is used to approximate when the system went down in the case of a hang. If tickerd is not enabled, this field contains:

```
LASTTICK|-1|unknown
```

Systems may optionally issue Status Update reports. These reports notify e-mail addresses that the system is still running and that Availmon reports are still enabled after some

duration. The duration is controlled by the configurable value `statusinterval` (refer to man page amconfig(1M)). This value is reported in Availmon reports as follows:

```
STATUSINTERVAL|<days>
```

where `<days> = 0` indicates that status update reports are not enabled.

The basic version identification for the system is (refer to man page uname(1), `-a` option):

```
UNAME|<os-name> <node-name> <os-release> <os-vers> <cpu-board>
```

Extended version information in diagnostic reports includes hardware, software, and graphics information:

```
HINV|begin
...             # report generated by `hinv -mvv`
HINV|end
VERSIONS|begin
...             # report generated by `versions -n` on
...             # eoe.sw.unix support.sw.fru “patchSG*”
VERSIONS|end
GFXINFO|begin
...             # report generated by `gfxinfo -vv`
GFXINFO|end
```

Reboot reports may include a summary:

```
SUMMARY|Begin
...             # panic string, FRU summary ...
SUMMARY|End
```

Extended diagnostic information in diagnostic reboot reports includes:

```
ICRASH|Begin
...             # summary report from `icrash -r -a ...`
...             # will include FRU results if available
ICRASH|End
SYSLOG|Begin
...             # compressed information from syslog
...             # since last report (see amsyslog(1M))
SYSLOG|End
```

3.3 Metrics

The `amreport` program produces reports from the information gathered by the Availmon facility. These reports, which can be viewed interactively or written to standard output, include availability statistics either for the local system or on multiple systems from a site logfile. In the latter case, statistics can be viewed for all systems or for each system individually. The statistical information can be used for metric evaluation. Figure 3-1 shows a sample `amreport` display on a local machine.

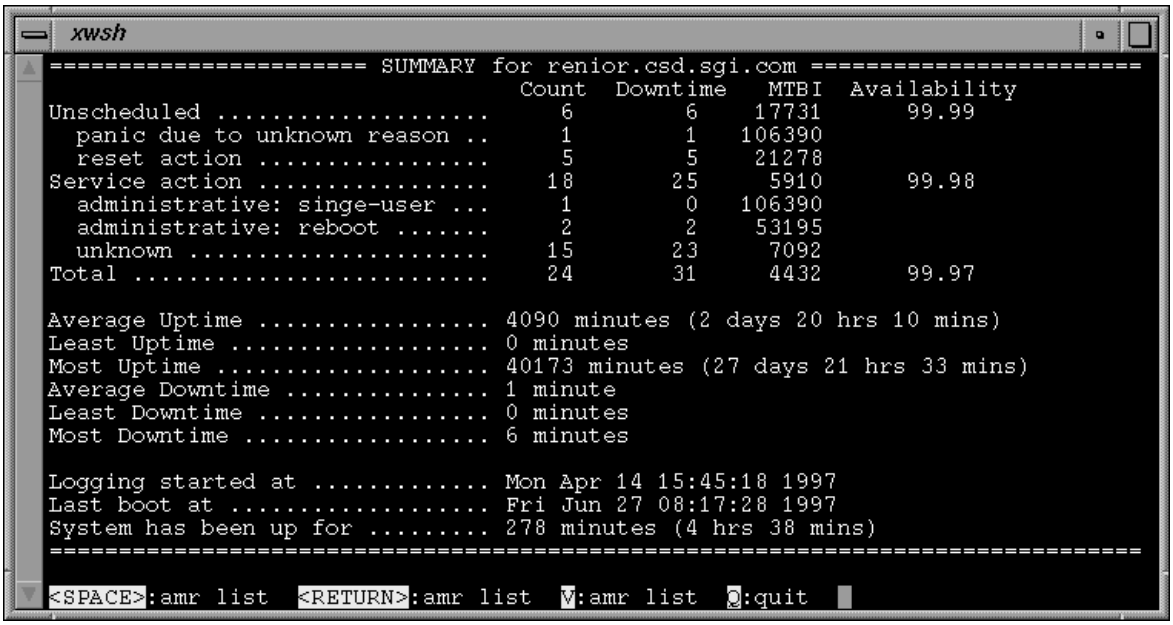

Figure 3-1 amreport Display

The top portion of Figure 3-1 (in 5-column tabular format) shows the statistics for different categories of events. The bottom portion of the figure shows general statistics irrespective of events. The column headings are described below:

Category Categories are subdivided into `Unscheduled` and `Service action`. Unscheduled events include any shutdowns of the system caused by unforeseen problems. Service action events include both controlled reboots and taking the system down to single-user mode. Individual events under these categories are shown only if their count is 1 or more.

Count The number of events that occurred in the category.

Downtime Total downtime caused by such events.

MTBI Mean time between interrupts, which is calculated as follows:
(Total Time) / count

Availability This is calculated as follows:
100 * ((Total Time - Downtime) / Total Time)

Chapter 4

Retrieving Availmon Data

This chapter describes how to retrieve Availmon data. There are two ways to retrieve Availmon data: by using `amreport` and by using the database query tool.

4.1 amreport

The `amreport` program reviews saved availability report information and provides statistical and event history reports. By default, it will process the availability data on the local system, which is saved automatically by Availmon. The `amreport` program can also process received aggregate Availmon reports; that is, an appended accumulation of Availmon reports from different systems, which is referred to as a *site logfile*.

The `amreport` program can be run interactively or it can generate statistical or event history reports, which are written to standard output. Interactively, it presents a statistical summary and allows hierarchical selection and display of a list of events or detail on particular events. Run interactively on a site logfile, `amreport` presents the same statistical or event information either on all systems or on each system individually. In either case, `amreport` can generate statistical, event list, event detail, or combined reports written to standard output.

The `amreport` program accepts *from* and *to* arguments, which can be used to bound the time period being reported. Run interactively on the local system, `amreport` also supports resending event data from selected historical events to specified e-mail addresses.

For additional information about Availmon reporting, refer to the man pages availmon(5) and amreport(1M), which includes a discussion of the *to* and *from* arguments that specify time range for reporting.

4.1.1 Interactive Use

The following illustrations show `amreport` displays, and the corresponding tables describe the command options you can use to view information and to send information to designated locations. The statistical information that is displayed as the first screen when `amreport` is invoked is discussed in Section 3.3, “Metrics.”

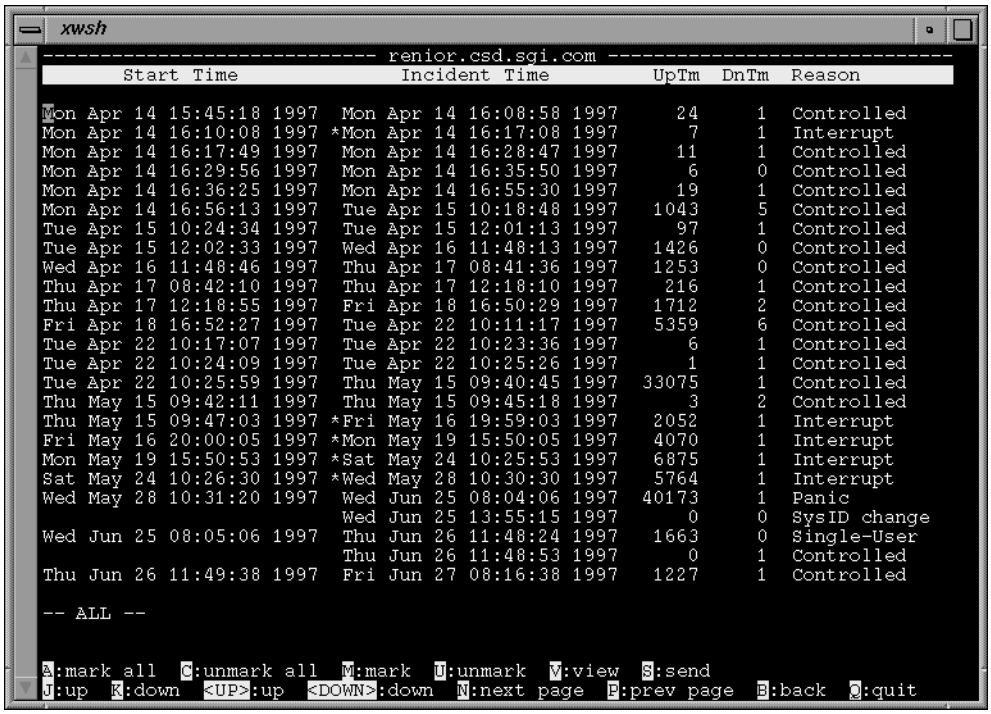

Figure 4-1 amreport Incident Display

Table 4-1 Incident Display Screen Commands

A	Marks (selects) all events displayed.
C	Unmarks all events displayed if previously selected with A.
M	Marks event at cursor.
U	Unmarks selected event at cursor.
V	Brings up screen that allows you to view information about event(s) you have marked, including internet address, shutdown reason, start time, incident time, re-start time, uptime, and downtime. Refer to Figure 4-2 and Table 4-2 for information on using the View screen.
S	Allows you to send marked information. Choosing S brings up the display shown in Figure 4-3, from which you can send (S), edit `autoemail.list` (E), or cancel (C). Refer also to Table 4-3.
J	Allows you to scroll upward in listings.
K	Allows you to scroll downward in listings.
N	Allows you to go to the next page of incident listings if there is more than one.
P	Allows you to go to the previous page of incident listings if there is more than one.

Table 4-1 (continued) Incident Display Screen Commands

B	Allows you to move backward one level of screen.
Q	Allows you to quit `amreport`.

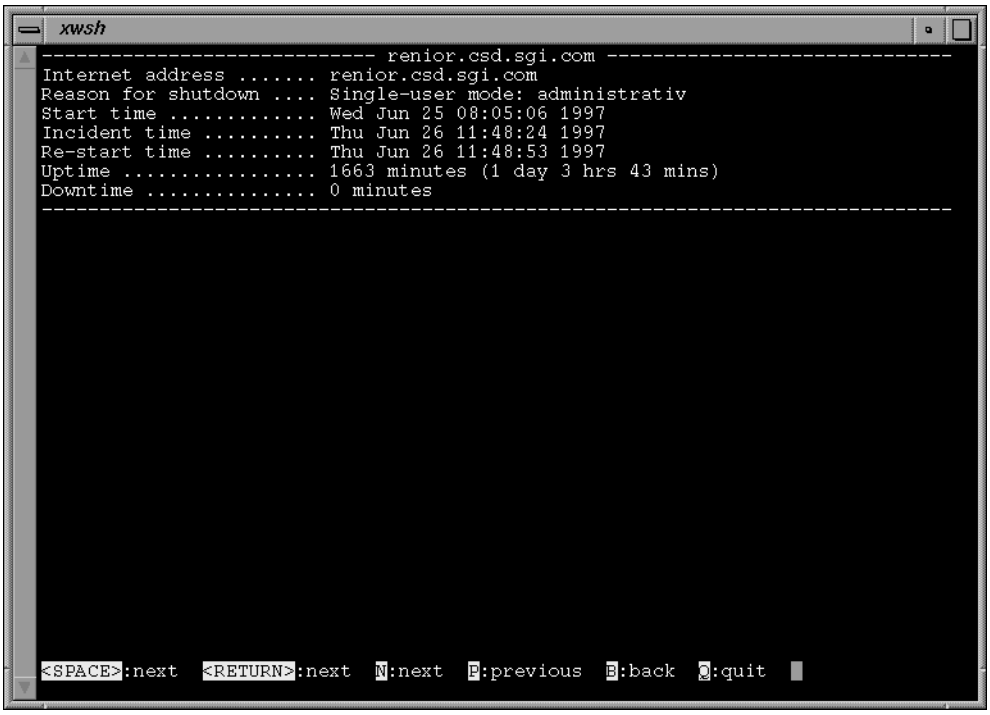

Figure 4-2 amreport View (V) Display

Table 4-2 amreport View (V) Display Screen Commands

<SPACE>	Allows you to move to the View screen for the next incident you have marked, if you have marked multiple incidents for viewing.
<RETURN>	Allows you to move to the View screen for the next incident you have marked, if you have marked multiple incidents for viewing.
N	Allows you to move to the View screen for the next incident you have marked, if you have marked multiple incidents for viewing.
P	Allows you to move to the View screen for the previous incident you have marked, if you have marked multiple incidents for viewing.
B	Allows you to move backward one level of screen.
Q	Allows you to quit `amreport`.

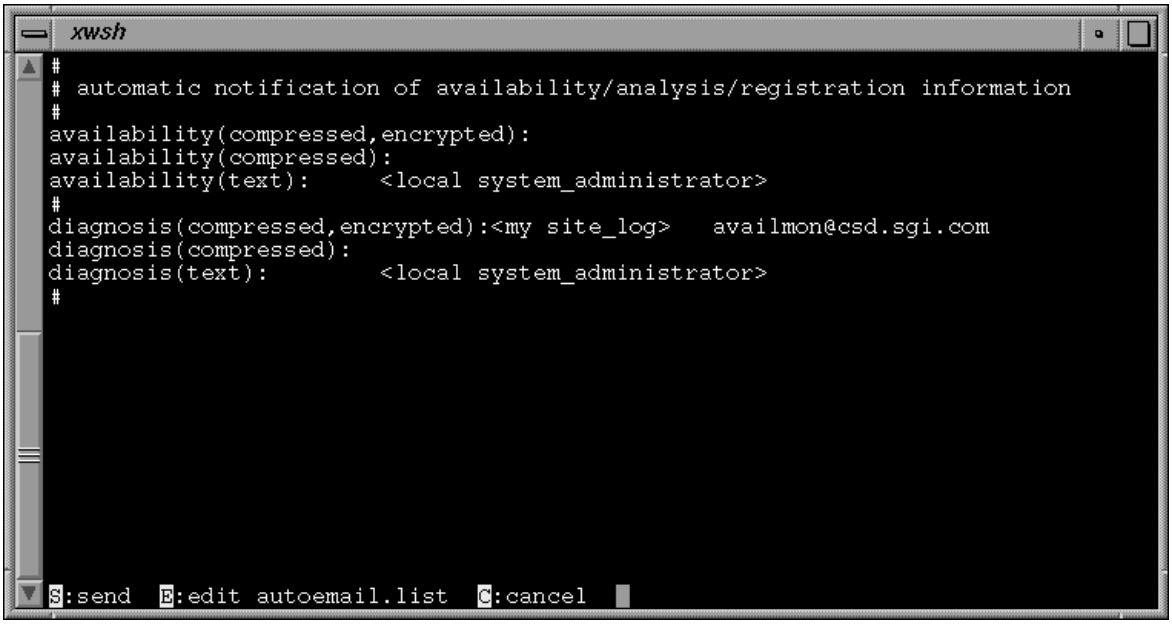

Figure 4-3 amreport Send (S) Screen Display

Table 4-3 amreport Send (S) Display Screen Commands

S	Allows you to send marked information to specified addresses.
E	Allows you to use vi editor on a copy of the `autoemail.list`. This selection allows you to make changes ONLY for sending in amreport. Any change here does not affect the `autoemail.list` file or standard Availmon report distribution. If a change is made for sending, and the user selects *Send* again while still in the same session of `amreport`, then the changed copy of `autoemail.list` is shown; that is, if you change the addresses for the first send operation, the same changed addresses can easily be applied to the next send operation.
C	Allows you to cancel this screen and return to main listing.

4.1.2 Generating Reports

Running `amreport` with the following arguments causes `amreport` to write the selected report(s) to standard output (capitalized letters correspond to argument letter):

-r statistical (metric) Report

-e Event list

-d event Detail

-p Print statistical report and event list

The reports written are identical to what is displayed on the interactive screens.

The following example shows invocations of `amreport` that generate regular status and event detail reports on the local system. This example assumes that "`stats`" and "`events`" are names of statistical and event detail reports, which are to be regularly created. It uses a file `LASTREPORT` to record the time stamp of the reports in the same format as the `touch(1) -t` argument, which is the format accepted by `amreport(1M)` for its `-f` and `-t` arguments.

```
amreport -r -f `cat LASTREPORT` >"stats"  2>/dev/null

amreport -d -f `cat LASTREPORT` >"events" 2>/dev/null

date +%y%m%d%H%M >LASTREPORT
```

The above example can be run regularly, perhaps monthly, using the crontab(1) facility.

4.2 Availmon Database Queries

In addition to `amreport`, you can view Availmon data through the Web at:

http://availmon.csd.sgi.com/availmon/

This Web site is accessible only to employees of Silicon Graphics.

The Availmon query tool provides three query levels:

- *Basic* query page requires that you input the host name or serial number, or both.
- *Detailed* query page allows you to find Availmon reports based on the configuration of the system.
- *Custom* query page allows you to query for information based on the criteria you select.

The query pages allow you to list all the hosts that match the criteria as well as all the incidents; or, you can search for specific strings in the logs or request the actual Availmon reports.

The following pages illustrate each query page and describe each page's options sequentially.

4.2.1 Basic Query Page

This query provides Availmon information by searching for host name, domain name, or serial number. All entries can be wildcarded by using an asterisk (*) before or after the entry. Refer to Table 4-4 for brief explanations of the report options, and refer to Figure 4-4 for an illustration of the basic query page. Step-by-step instructions for using the page follow the figure.

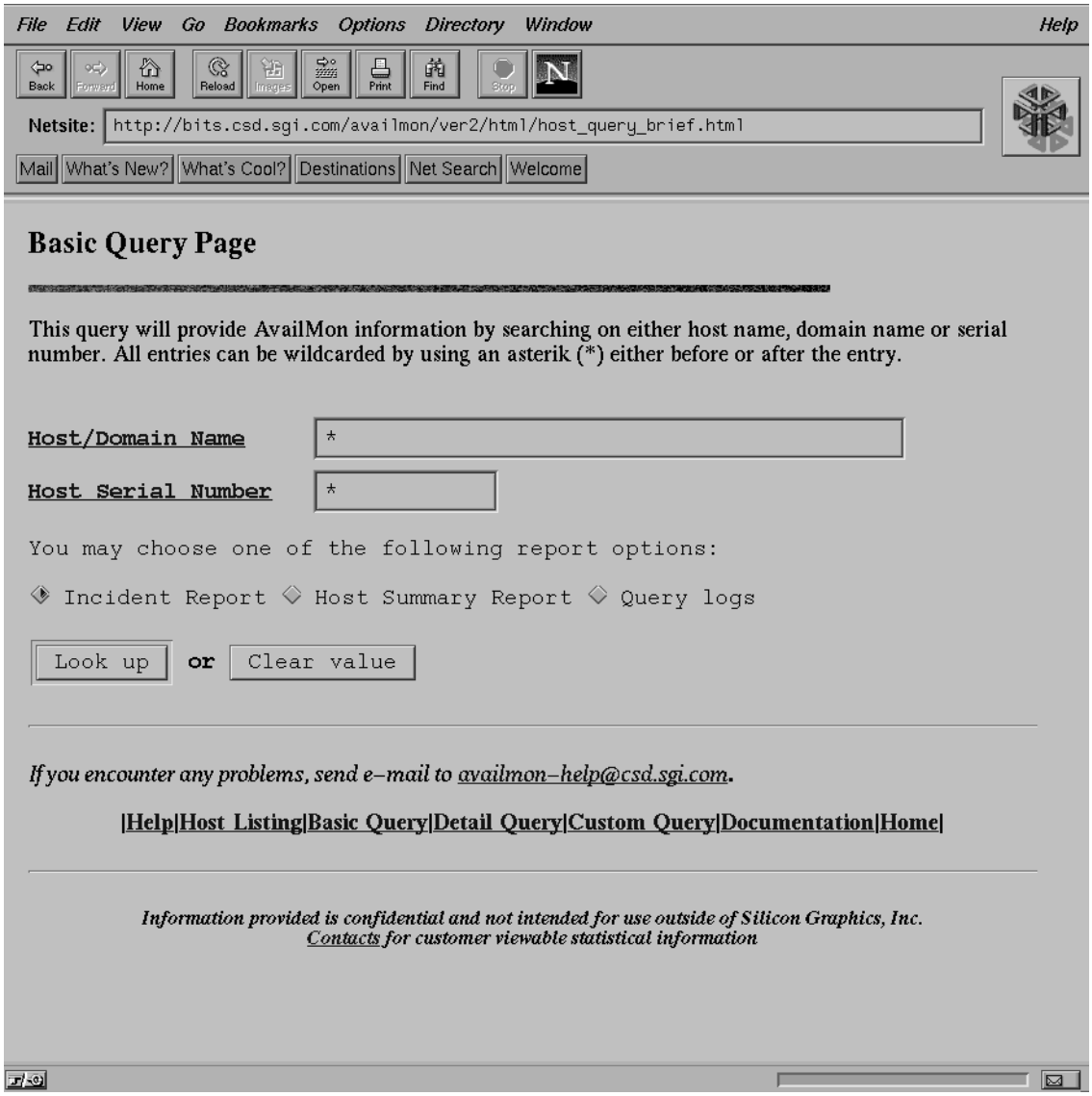

Figure 4-4 Basic Query Page

To use this query page, follow these steps:

1. Enter the host or domain name in the first field, or enter the host serial number, or both. (If you need help, click on the appropriate highlighted links.)
2. Choose a report option from the list by clicking on the diamond in front of it. Table 4-4 describes the report options.
3. If you are satisfied with the choices you have indicated, click on the *Look up* button to access the report.
4. If you wish to begin again, click on the *Clear value* button and start over.

Table 4-4 Query Page Report Options

Incident Report	The Availmon Incident Report lists times when a system was down for any reason -- as reported by the system when it comes back up.
Host Summary Report	The Host Summary Report displays a list of the most recent incidents of all the hosts that satisfy a selection criterion on the Basic Query Page or the Detailed Query Page. The fields that are reported include the serial number of the host, the host name, OS-related information for the host, hardware-related information for the host, the total uptime for the host, the registration status of the host, the presence or absence of logs, and the reason for the most recent incident.
Query logs	This query page generates an incident report based on a string search criterion.The types of logs to be searched are syslogs by default. Enter the desired search string in the field provided. Choose the logs you wish to search by clicking on the box next to *Icrash Logs*, *Panic Logs*, or *Sys Logs*. Click on *Submit* when you are satisfied with your selection, or click on *Clear Selection* to begin again.

4.2.2 Detailed Query Page

This query page provides Availmon information by adding options that allow you to narrow your search by choosing more specific criteria, such as a date range, number of disk drives, number of CPUs, CPU rev, and so on. Refer to Figure 4-5 for an illustration of the detailed query page. Instructions for using this page follow the figure.

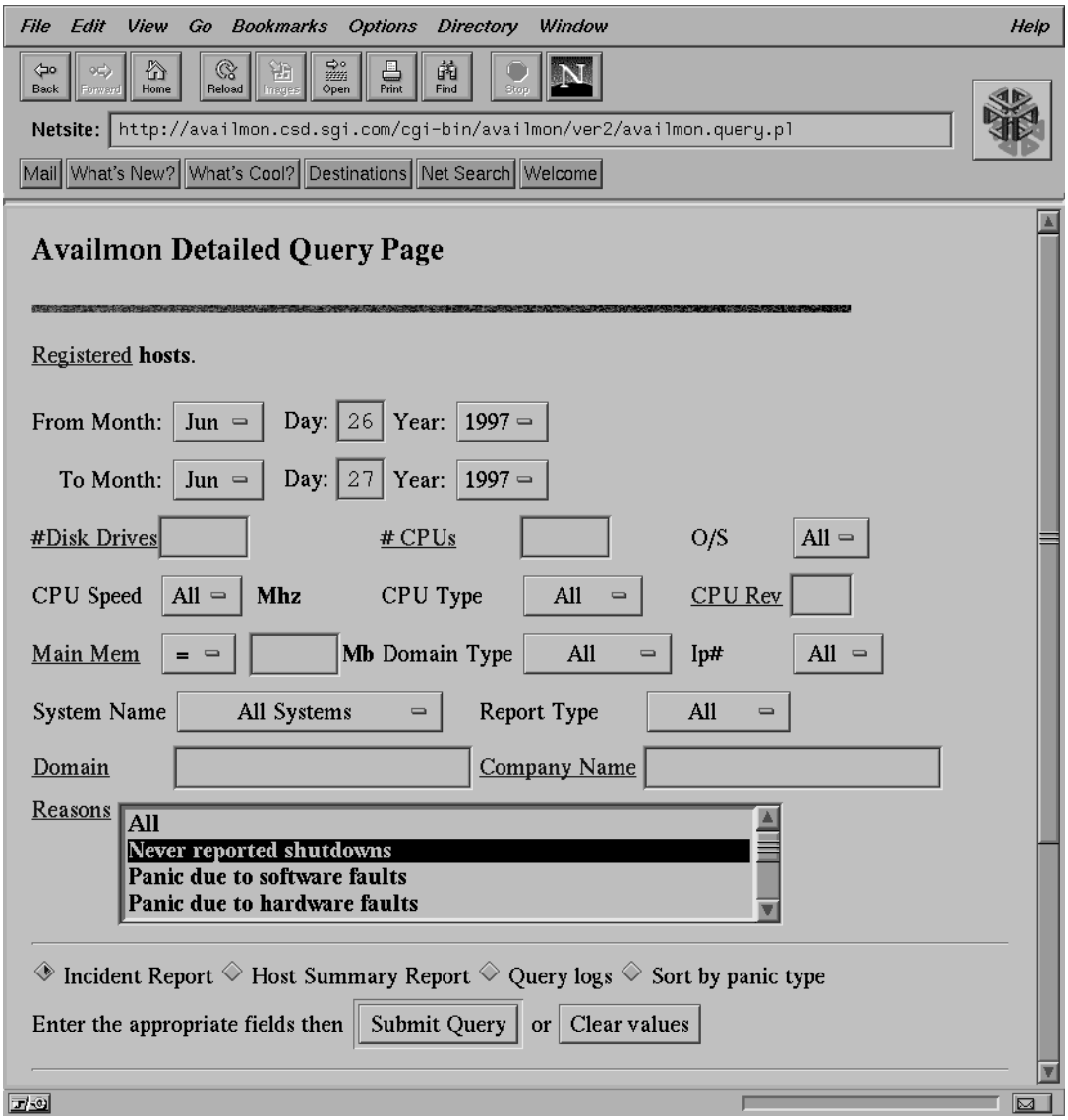

Figure 4-5 Detailed Query Page

To use the detailed query page, follow these steps:

1. Click on the highlighted link *Registered Hosts*.

   Choosing this link opens the Registration Query Page. On it you can enter your choices for *Host/Domain Name* and *Host Serial Number*, or you can click on those text links to help you make your selection.

   Click on *Look up* button to continue, or click on *Clear value* button to begin again.

2. On the detailed query page, choose a date range by selecting a month and year from the pulldown menu, and enter the day in the field provided.
3. Enter the number of desired disk drives in the field provided. For more information on how to complete this field, click on the highlighted *# Disk Drives* link. The *Disk Drive Help Page* appears.
4. Enter the number of desired CPUs in the field provided. For more information on how to complete this field, click on the highlighted *# CPUs* link. The *# CPUs Help Page* appears.
5. Choose the appropriate operating system version from the pulldown menu labeled *O/S*.
6. Choose the appropriate CPU speed from the pulldown menu provided.
7. Enter the CPU rev in the field provided; for more information on how to complete this field, click on the *CPU Rev* link.The *CPU Rev Help Page* appears.
8. Choose a main memory option from the pulldown menu provided, and enter a number in the field provided. For more information on how to complete this field, click on the *Main Mem* link provided. The *Main Mem Help Page* appears.
9. Choose a domain type from the pulldown menu provided.
10. Choose an IP number from the pulldown menu provided.
11. Choose a system name from the pulldown menu provided.
12. Choose a report type from the pulldown menu provided.
13. Enter the appropriate domain in the field provided. For more information on how to complete this field, click on the highlighted *Domain* link provided. The *Domain Name Help Page* appears.
14. Enter the appropriate company name in the field provided. Click on the highlighted *Company Name* link for more information. The *Company Name Help Page* appears.
15. Choose the appropriate reporting reason in the scroll box provided.
16. Choose the appropriate reporting option(s) by clicking on the diamond that precedes it. Table 4-4 describes the report options.
17. If you are satisfied with your selection, click on the *Submit Query* button. If you wish to begin again, click on *Clear values* and begin again.

4.2.3 Custom Query Page

The custom query page allows you to query for information based only on the criteria selected. Refer to Figure 4-6 for an illustration of the custom query page building tool. Instructions for using the tool follow the figure.

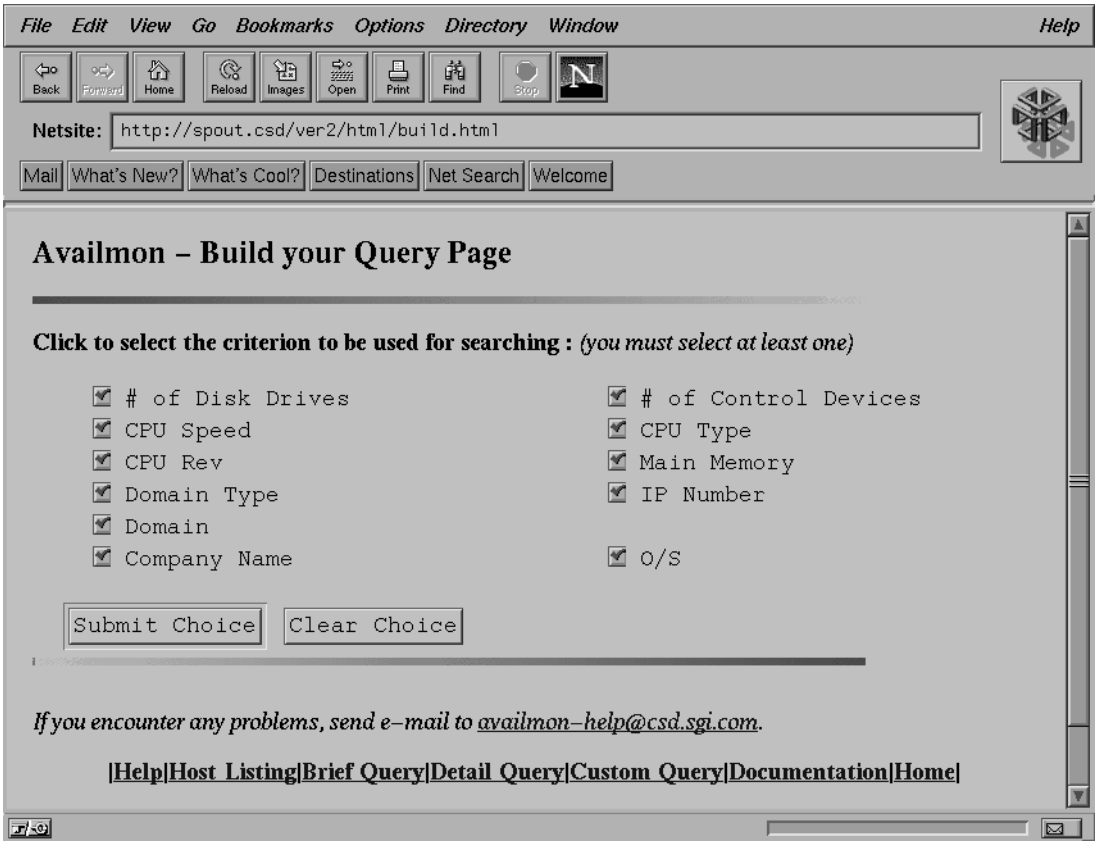

Figure 4-6 Custom Query Page Selection Criteria

To create your custom query page, follow these steps:

1. Select at least one search criterion by clicking on the box in front of it. A red check mark should appear in each box that you select.
2. Click on the *Submit Choice* button if you are satisfied with your selections. Click on *Clear Choice* if you wish to begin again.

   A customized query page appears that contains options based on your criteria (refer to Figure 4-7).
3. Enter appropriate information by typing in the fields provided and by using the pulldown menus provided. For additional information, click on the highlighted text links that correspond to some fields.
4. Click on the *Submit Choice* button to begin your search if you are satisfied that the information you have entered is accurate. If you wish to begin again, click on the *Clear* button.

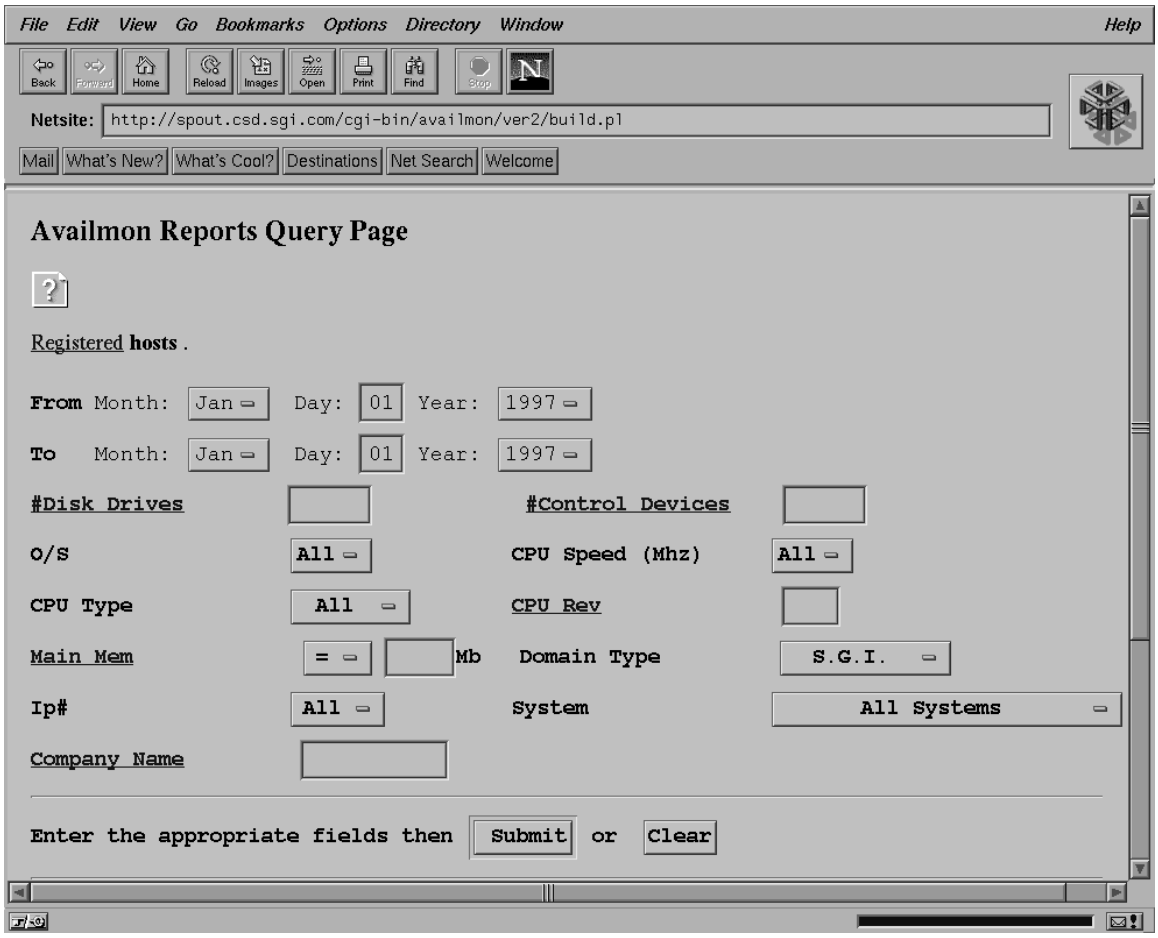

Figure 4-7 Custom Query Page