



Statistics

The following topics describe how to monitor the system:

- [About System Statistics, on page 1](#)
- [The Host Statistics Section, on page 1](#)
- [The Disk Usage Section, on page 2](#)
- [The Processes Section, on page 2](#)
- [The SFDDataCorrelator Process Statistics Section, on page 7](#)
- [The Intrusion Event Information Section, on page 8](#)
- [Viewing System Statistics, on page 9](#)

About System Statistics

The Statistics page lists the current status of general appliance statistics, including disk usage and system processes, Data Correlator statistics, and intrusion event information.

The Host Statistics Section

The following table describes the host statistics listed on the Statistics page.

Table 1: Host Statistics

| Category | Description |
|--------------|---|
| Time | The current time on the system. |
| Uptime | The number of days (if applicable), hours, and minutes since the system was last started. |
| Memory Usage | The percentage of system memory that is being used. |
| Load Average | The average number of processes in the CPU queue for the past 1 minute, 5 minutes, and 15 minutes. |
| Disk Usage | The percentage of the disk that is being used. Click the arrow to view more detailed host statistics. |
| Processes | A summary of the processes running on the system. |

The Disk Usage Section

The Disk Usage section of the Statistics page provides a quick synopsis of disk usage, both by category and by partition status. If you have a malware storage pack installed on a device, you can also check its partition status. You can monitor this page from time to time to ensure that enough disk space is available for system processes and the database.



Tip You can also use the Disk Usage health monitor to monitor disk usage and alert on low disk space conditions.

The Processes Section

The Processes section of the Statistics page allows you to see the processes that are currently running on an appliance. It provides general process information and specific information for each running process. You can use the management center's web interface to view the process status for any managed device.

Note that there are two different types of processes that run on an appliance: daemons and executable files. Daemons always run, and executable files are run when required.

Process Status Fields

When you expand the Processes section of the Statistics page, you can also view the following:

Cpu(s)

Lists the following CPU usage information:

- user process usage percentage
- system process usage percentage
- nice usage percentage (CPU usage of processes that have a negative nice value, indicating a higher priority). Nice values indicate the scheduled priority for system processes and can range between -20 (highest priority) and 19 (lowest priority).
- idle usage percentage

Mem

Lists the following memory usage information:

- total number of kilobytes in memory
- total number of used kilobytes in memory
- total number of free kilobytes in memory
- total number of buffered kilobytes in memory

Swap

Lists the following swap usage information:

- total number of kilobytes in swap
- total number of used kilobytes in swap
- total number of free kilobytes in swap
- total number of cached kilobytes in swap

The following table describes each column that appears in the Processes section.

Table 2: Process List Columns

| Column | Description |
|----------|--|
| Pid | The process ID number |
| Username | The name of the user or group running the process |
| Pri | The process priority |
| Nice | The <i>nice</i> value, which is a value that indicates the scheduling priority of a process. Values range between -20 (highest priority) and 19 (lowest priority) |
| Size | The memory size used by the process (in kilobytes unless the value is followed by <i>m</i> , which indicates megabytes) |
| Res | The amount of resident paging files in memory (in kilobytes unless the value is followed by <i>m</i> , which indicates megabytes) |
| State | <p>The process state:</p> <ul style="list-style-type: none"> • D — process is in uninterruptible sleep (usually Input/Output) • N — process has a positive nice value • R — process is runnable (on queue to run) • S — process is in sleep mode • T — process is being traced or stopped • W — process is paging • X — process is dead • Z — process is defunct • < — process has a negative nice value |
| Time | The amount of time (in hours:minutes:seconds) that the process has been running |
| Cpu | The percentage of CPU that the process is using |
| Command | The executable name of the process |

Related Topics

[System Daemons](#), on page 4

[Executables and System Utilities](#), on page 5

System Daemons

Daemons continually run on an appliance. They ensure that services are available and spawn processes when required. The following table lists daemons that you may see on the Process Status page and provides a brief description of their functionality.



Note The table below is not an exhaustive list of all processes that may run on an appliance.

Table 3: System Daemons

| Daemon | Description |
|-------------------------------------|---|
| crond | Manages the execution of scheduled commands (cron jobs) |
| dhclient | Manages dynamic host IP addressing |
| fpcollect | Manages the collection of client and server fingerprints |
| httpd | Manages the HTTP (Apache web server) process |
| httpsd | Manages the HTTPS (Apache web server with SSL) service, and checks for working SSL certificate authentication; runs in the background to provide secure web access to the appliance |
| keventd | Manages Linux kernel event notification messages |
| klogd | Manages the interception and logging of Linux kernel messages |
| kswapd | Manages Linux kernel swap memory |
| kupdated | Manages the Linux kernel update process, which performs disk synchronization |
| mysqld | Manages database processes |
| ntpd | Manages the Network Time Protocol (NTP) process |
| pm | Manages all system processes, starts required processes, restarts any process that fails unexpectedly |
| reportd | Manages reports |
| safe_mysqld | Manages safe mode operation of the database; restarts the database daemon if an error occurs; logs runtime information to a file |
| SFDataCorrelator | Manages data transmission |
| sfstreamer (management center only) | Manages connections to third-party client applications that use the Event Streamer |

| Daemon | Description |
|---|---|
| sfmgr | Provides the RPC service for remotely managing and configuring an appliance using a connection to the appliance |
| SFRemediateD (management center only) | Manages remediation responses |
| sftimeserviced (management center only) | Forwards time synchronization messages to managed devices |
| sfmbservice | Provides access to the sfmb message broker process running on a remote appliance, using a connection to the appliance. Currently used only by health monitoring to send health events from a managed device to the management center. |
| sftroughd | Listens for connections on incoming sockets and then invokes the correct executable (Cisco message broker, sfmb) to handle the request |
| sftunnel | Provides the secure communication channel for all processes requiring communication with the appliance |
| sshd | Manages the Secure Shell (SSH) process; runs in the background to provide SSH access to the appliance |
| syslogd | Manages the system logging (syslog) process |

Executables and System Utilities

There are a number of executables on the system that run when executed by other processes or through user action. The following table describes the executables that you may see on the Process Status page.

Table 4: System Executables and Utilities

| Executable | Description |
|---|---|
| awk | Utility that executes programs written in the <code>awk</code> programming language |
| bash | GNU Bourne-Again Shell |
| cat | Utility that reads files and writes content to standard output |
| chown | Utility that changes user and group file permissions |
| chsh | Utility that changes the default login shell |
| SFDataCorrelator (management center only) | Analyzes binary files created by the system to generate events, connection data, and network maps |
| cp | Utility that copies files |
| df | Utility that lists the amount of free space on the appliance |
| echo | Utility that writes content to standard output |

| Executable | Description |
|------------------|---|
| egrep | Utility that searches files and folders for specified input; supports extended set of regular expressions not supported in standard grep |
| find | Utility that recursively searches directories for specified input |
| grep | Utility that searches files and directories for specified input |
| halt | Utility that stops the server |
| httpsdctl | Handles secure Apache Web processes |
| hwclock | Utility that allows access to the hardware clock |
| ifconfig | Indicates the network configuration executable. Ensures that the MAC address stays constant |
| iptables | Handles access restriction based on changes made to the Access Configuration page. |
| iptables-restore | Handles iptables file restoration |
| iptables-save | Handles saved changes to the iptables |
| kill | Utility that can be used to end a session and process |
| killall | Utility that can be used to end all sessions and processes |
| ksh | Public domain version of the Korn shell |
| logger | Utility that provides a way to access the syslog daemon from the command line |
| md5sum | Utility that prints checksums and block counts for specified files |
| mv | Utility that moves (renames) files |
| myisamchk | Indicates database table checking and repairing |
| mysql | Indicates a database process; multiple instances may appear |
| openssl | Indicates authentication certificate creation |
| perl | Indicates a perl process |
| ps | Utility that writes process information to standard output |
| sed | Utility used to edit one or more text files |
| sfheartbeat | Identifies a heartbeat broadcast, indicating that the appliance is active; heartbeat used to maintain contact between a device and management center. |
| sfmb | Indicates a message broker process; handles communication between management centers and device. |
| sh | Public domain version of the Korn shell |

| Executable | Description |
|------------|---|
| shutdown | Utility that shuts down the appliance |
| sleep | Utility that suspends a process for a specified number of seconds |
| smtpclient | Mail client that handles email transmission when email event notification functionality is enabled |
| snmptrap | Forwards SNMP trap data to the SNMP trap server specified when SNMP notification functionality is enabled |
| snort | Indicates that Snort is running |
| ssh | Indicates a Secure Shell (SSH) connection to the appliance |
| sudo | Indicates a sudo process, which allows users other than admin to run executables |
| top | <p>Utility that displays information about the top CPU processes</p> <p>Note The CPU usage output of this utility is a split-up of different types of usages of the CPU core. You must add both user and system processes usage to know the actual total CPU usage.</p> <p>For example, if the output of top command is: %Cpu(s): 76.6 us, 22.1 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 1.3 si, 0.0 st</p> <p>Here, 76.6% of CPU time is used by user processes, 22.1% of CPU time is used by system(kernel) processes. The total CPU usage is 98.7%.</p> <p>Thus, the CPU usage reported in this utility appear to be different from the Health Monitor dashboard. In addition, this utility uses a three seconds interval to calculate the CPU usage. Whereas, the management center health monitor uses one-second intervals.</p> |
| touch | Utility that can be used to change the access and modification times of specified files |
| vim | Utility used to edit text files |
| wc | Utility that performs line, word, and byte counts on specified files |

Related Topics

[Configure an Access List](#)

The SFDataCorrelator Process Statistics Section

On the management center, you can view statistics about the Data Correlator and network discovery processes for the current day. As the managed devices perform data acquisition, decoding, and analysis, the network discovery process correlates the data with the fingerprint and vulnerability databases, then produces binary files that are processed by the Data Correlator running on the management center. The Data Correlator analyzes the information from the binary files, generates events, and creates network maps.

The statistics that appear for network discovery and the Data Correlator are averages for the current day, using statistics gathered between 12:00 AM and 11:59 PM for each device.

The following table describes the statistics displayed for the Data Correlator process.

Table 5: Data Correlator Process Statistics

| Category | Description |
|------------------------|---|
| Events/Sec | Number of discovery events that the Data Correlator receives and processes per second |
| Connections/Sec | Number of connections that the Data Correlator receives and processes per second |
| CPU Usage — User (%) | Average percentage of CPU time spent on user processes for the current day |
| CPU Usage — System (%) | Average percentage of CPU time spent on system processes for the current day |
| VmSize (KB) | Average size of memory allocated to the Data Correlator for the current day, in kilobytes |
| VmRSS (KB) | Average amount of memory used by the Data Correlator for the current day, in kilobytes |

The Intrusion Event Information Section

On both the management center and managed devices, you can view summary information about intrusion events on the Statistics page. This information includes the date and time of the last intrusion event, the total number of events that have occurred in the past hour and the past day, and the total number of events in the database.



Note The information in the Intrusion Event Information section of the Statistics page is based on intrusion events stored on the managed device rather than those sent to the management center. No intrusion event information is listed on this page if the managed device cannot (or is configured not to) store intrusion events locally.

The following table describes the statistics displayed in the Intrusion Event Information section of the Statistics page.

Table 6: Intrusion Event Information

| Statistic | Description |
|--------------------------|--|
| Last Alert Was | The date and time that the last event occurred |
| Total Events Last Hour | The total number of events that occurred in the past hour |
| Total Events Last Day | The total number of events that occurred in the past twenty-four hours |
| Total Events in Database | The total number of events in the events database |

Viewing System Statistics

The display includes statistics for the management center and its managed devices.

Before you begin

You must be an Admin or Maintenance user and be in the Global domain to view system statistics.

Procedure

-
- | | |
|---------------|---|
| Step 1 | Choose System (⚙️) > Monitoring > Statistics . |
| Step 2 | Choose a device from the Select Device(s) list, and click Select Devices . |
| Step 3 | View available statistics. |
| Step 4 | In the Disk Usage section, you can: <ul style="list-style-type: none">• Hover your pointer over a disk usage category in the By Category stacked bar to view (in order):<ul style="list-style-type: none">• the percentage of available disk space used by that category• the actual storage space on the disk• the total disk space available for that category• Click the arrow next to By Partition to expand it. If you have a malware storage pack installed, the <code>/var/storage</code> partition usage is displayed. |
| Step 5 | (Optional) Click the arrow next to Processes to view the information described in Viewing System Statistics, on page 9 . |
-

