

Statistics

The following topics describe how to monitor the system:

- System statistics, on page 1
- Host statistics section, on page 1
- Disk usage section, on page 2
- The processes section, on page 2
- SFDataCorrelator process statistics section, on page 7
- Intrusion event information section, on page 8
- View system statistics, on page 9

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 .

Host statistics section

The table lists the host statistics 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.

Disk usage section

The **Disk Usage** section of the **Statistics** page summarizes disk usage both by category and partition status. If a malware storage pack is installed on your device, you can also check its partition status within this section. Monitor this page regularly to ensure you have enough disk space for system processes and database operations.

Tip You can use the disk usage health monitor to monitor disk usage and receive alerts when the disk space is low.

The processes section

The **Processes** section of the **Statistics** page allows you to view the processes currently running on a managed appliance. This section provides both general and detailed information for every running process. You can use the Firewall Management Center's web interface to monitor the process status for any managed device.

There are two different types of processes that run on an appliance:

- Daemons: These processes always run in the background and are essential for system operations.
- Executable files: These processes run only when required, such as during specific tasks or operations.

Use the **Processes** section to quickly check which processes are active and understand their role in appliance management.

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 table describes each column that appears in the **Processes** section.

Table 2: Process list columns

Column	Description
Pid	The process ID number
Username	Name of the user or group running the process
Pri	The process priority
Nice	The value indicating the scheduling priority of a process. Values range from -20 (highest) to 19 (lowest)
Size	Memory size used by the process (in kilobytes, unless followed by `m` for megabytes)
Res	Amount of resident paging files in memory (in kilobytes, unless followed by `m` for megabytes)
State	The process state: • D: Uninterruptible sleep (usually Input/Output) • N: Positive nice value • R: Runnable (on queue to run) • S: Sleep mode • T: Being traced or stopped • W: Paging • X: Dead • Z: Defunct • <: Negative nice value
Time	Amount of time (in hours:minutes:seconds) that the process has been running
CPU	Percentage of CPU the process is using

Column	Description
Command	Executable name of the process

System daemons

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

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; checks for SSL and valid ce 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, performing 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 une
reportd	Manages reports
safe_mysqld	Manages safe mode operation of the database; restarts the database daemon if an error oc logs runtime information to a file
SFDataCorrelator	Manages data transmission
sfestreamer (Firewall Management Center only)	Manages connections to third-party client applications that use the Event Streamer
sfmgr	Provides the RPC service for remotely managing and configuring an appliance using an s connection to the appliance
SFRemediateD (Firewall Management Center only)	Manages remediation responses

Daemon	Description
sftimeserviced (Firewall Management Center only)	Forwards time synchronization messages to managed devices
sfmbservice	Provides access to the sfmb message broker process running on a remote appliance usi connection to the appliance. Used by health monitoring to send health events and alerts fr device to the Firewall Management Center.
sftroughd	Listens for connections on incoming sockets and invokes the correct executable (typic message broker, sfmb) to handle the request
sftunnel	Provides the secure communication channel for all processes requiring communication appliance
sshd	Manages the Secure Shell (SSH) process; runs in the background to provide SSH acce appliance
syslogd	Manages the system logging (syslog) process

Note This table does not include every possible process; additional daemons may be present depending on appliance configuration.

Executables and system utilities

There are a number of executables on the system that are launched by other processes or through user action. The table describes the executables and system utilities that may appear on the **Process Status** page.

Table 4: System executables and utilities

Executable	Description
awk	Executes programs written in the `awk` programming language
bash	GNU Bourne-Again Shell
cat	Reads files and writes content to standard output
chown	Changes user and group file permissions
chsh	Changes the default login shell
SFDataCorrelator (Firewall Management Center only)	Analyzes binary files created by the system to generate events, connection data, and network maps
cp	Copies files
df	Lists the amount of free space on the appliance
echo	Writes content to standard output

Executable	Description
egrep	Searches files and folders for specified input; supports extended set of regular expressions not supported in standard grep
find	Recursively searches directories for specified input
grep	Searches files and directories for specified input
halt	Stops the server
httpsdctl	Handles secure Apache Web processes
hwclock	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	Ends a session and process
killall	Ends all sessions and processes
ksh	Public domain version of the Korn shell
logger	Provides a way to access the syslog daemon from the command line
md5sum	Prints checksums and block counts for specified files
mv	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	Writes process information to standard output
sed	Edits one or more text files
sfheartbeat	Identifies a heartbeat broadcast, indicating that the appliance is active; used to maintain contact between a device and Firewall Management Center.
sfmb	Indicates a message broker process; handles communication between Firewall Management Centers and device.
sh	Public domain version of the Korn shell

Executable	Description
shutdown	Shuts down the appliance
sleep	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	Displays information about the top CPU processes **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. 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` 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%. Thus, the CPU usage reported in this utility appears 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.
touch	Changes the access and modification times of specified files
vim	Edits text files
wc	Performs line, word, and byte counts on specified files

SFDataCorrelator process statistics section

On the Firewall Management Center, you can view statistics about the data correlator and network discovery processes for the current day. The managed devices perform data acquisition, decoding, and analysis, and the network discovery process then correlates the data with the fingerprint and vulnerability databases. It then produces binary files, which are processed by the data correlator running on the Firewall 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 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.

These statistics help administrators monitor the performance and resource usage of the Firewall Management Center's data correlator and network discovery processes throughout the day.

Intrusion event information section

On both the Firewall 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 **Intrusion Event Information** section of the **Statistics** page reflects intrusion events stored locally on the managed device rather than those sent to the Firewall Management Center. If the managed device cannot store intrusion events, or if it is not configured to do so, no information appears in this section.

The table describes the statistics shown 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.

View system statistics

View system statistics to monitor the performance and resource utilization of the Firewall Management Center and its managed devices.

The display includes statistics for the Firewall Management Center and its managed devices.

Before you begin

- Make sure you have Admin or Maintenance user privileges.
- Ensure you are in the Global domain.

Follow these steps 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:

- Hover your pointer over a disk usage category in the **By Category** stacked bar to view these items in this order:
  - 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 a malware storage pack is installed, the **/var/storage** partition usage appears.

Step 5 (Optional) Click the arrow next to **Processes** to view the information described in View system statistics, on page 9.