統計情報

以下のトピックでは、システムをモニターする方法を示します。

システム統計について

[統計情報（Statistics）] ページには、アプライアンスの現在の一般的ステータスに関する統計情報（ディスク使用量とシステム プロセス）、データ コリレータ統計情報、侵入イベント情報が表示されます。

[ホスト統計情報（Host Statistics）] セクション

次の表に、[統計情報（Statistics）] ページにリストされるホスト統計情報を示します。

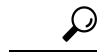
表 *1* : ホスト統計情報（*Host Statistics*）

カテゴリ	説明
時刻（Time）	システムの現在の時刻。
アップタイム（Uptime）	システムが前回起動してから経過した日数（該当する場合）、時間数、および分数。

カテゴリ	説明
メモリ使用率（Memory Usage）	使用中のシステム メモリの割合。
負荷平均（Load Average）	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
ディスク使用率（Disk Usage）	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。
プロセス（Processes）	システムで実行されているプロセスの概要。

[ディスク使用量（Disk Usage）] セクション

[統計情報（Statistics）] ページの [ディスク使用率（Disk Usage）] セクションは、カテゴリ別およびパーティション ステータス別に、ディスク使用量のクイック概要を示します。マルウェア ストレージ パックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的に監視して、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。



ヒント [ディスク使用量（Disk Usage）]ヘルスモニターを使用して、ディスク使用状況を監視し、ディスク容量不足の状態をアラートすることもできます。

[プロセス（Processes）] セクション

[統計情報（Statistics）] ページの [プロセス（Processes）] セクションでは、アプライアンスで現在実行中のプロセスを表示できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。Management Center の Web インターフェイスを使用すると、管理対象デバイスのプロセスのステータスを表示できます。

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの2種類があることに注意してください。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

プロセス使用状況フィールド

統計情報ページのプロセス セクションを展開すると、以下を表示できます。

[CPU（Cpu(s)）]

次の CPU 使用状況情報がリストされます：

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合（高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況）。nice 値は、システム プロセスのスケジュールされた優先度を示しており、-20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。
- アイドル状態の使用状況の割合

[メモリ（Mem）]

以下のメモリ使用状況情報がリストされます。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[切替（Swap）]

以下のスワップ使用状況情報がリストされます。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

次の表に、プロセス セクションに表示される各列を示します。

表 *2:* プロセス リスト カラム

カラム	説明
Pid	プロセス ID 番号
ユーザ名（Username）	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	nice 値。プロセスのスケジューリング優先度を示す値です。値は -20（最も高い優先度）から 19（最も低い優先度）までの範囲になります。

カラム	説明
Size	プロセスで使用されるメモリ サイズ（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
Res	メモリ内の常駐ページング ファイルの量（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
State	プロセスの状態： • D：プロセスが中断不能スリープ状態（通常は入出力）にある • N：プロセスの nice 値が正の値 • R：プロセスが実行可能である（実行するキュー上で） • S：プロセスがスリープ モードにある • T：プロセスがトレースまたは停止されている • W：プロセスがページングしている • X：プロセスがデッド状態である • Z：プロセスが機能していない • <：プロセスの nice 値が負の値
Time	プロセスが実行されてきた時間の長さ（時間数:分数:秒数）
Cpu	プロセスが使用している CPU の割合
Command	プロセスの実行可能ファイル名

関連トピック

システム デーモン （4 ページ）
実行可能ファイルおよびシステム ユーティリティ （6 ページ）

システム デーモン

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[プロセスのステータス（Process Status）] ページに表示されるデーモンをリストし、その機能について簡単に説明しています。

（注） 次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 *3:* システム デーモン

デーモン	説明
crond	スケジュールされたコマンド（cron ジョブ）の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
fpcollect	クライアントとサーバのフィンガープリントの収集を管理します
httpd	HTTP（Apache Web サーバ）プロセスを管理します
httpsd	HTTPS（SSL を使用した Apache Web サーバー）サービスを管理し、SSL お 明書の認証が機能しているかチェックし、アプライアンスへの安全な Web 供するためにバックグラウンドで実行します
keventd	Linux カーネルのイベント通知メッセージを管理します
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理し
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	データベース プロセスを管理します
ntpd	Network Time Protocol（NTP）プロセスを管理します
pm	すべてのシステムプロセスを管理し、必要なプロセスを始動し、予期せず セスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデ モンを再始動し、ランタイム情報をファイルに記録します
SFDataCorrelator	データ転送を管理します
sfestreamer （Management Center のみ）	Event Streamer を使用するサード パーティ製クライアント アプリケーショ 理します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンス 定するための RPC サービスを提供します
SFRemediateD（Management Center のみ）	修復応答を管理します
sftimeserviced（Management Center のみ）	時間同期メッセージを管理対象デバイスに転送します

デーモン	説明
sfmbservice	アプライアンスへの sftunnel 接続を使用して、リモート アプライアンスで実行 sfmb メッセージ ブローカ プロセスへのアクセスを提供します。現在、ヘルス グでのみ使用されており、管理対象デバイスから Management Center へ正常な アラートを送信します。
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル（通常は、 セージ ブローカ sfmb）を呼び出して要求を処理します
sftunnel	リモートアプライアンスとの通信を必要とするすべてのプロセスに対し、安全 ネルを提供します。
sshd	セキュア シェル（SSH）プロセスを管理し、アプライアンスへの SSH アクセ るためにバックグラウンドで実行します
syslogd	システム ロギング（syslog）プロセスを管理します

実行可能ファイルおよびシステム ユーティリティ

システム上には、他のプロセスまたはユーザー操作によって実行される実行可能ファイルが数多く存在します。次の表に、[プロセス ステータス（Process Status）] ページで表示される実行可能ファイルについて説明します。

表 *4:* システムの実行可能ファイルおよびユーティリティ

実行可能ファイル	説明
awk	awkプログラミング言語で作成されたプログラムを実行するユーティリティ
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
SFDataCorrelator（Management Center のみ）	システムで作成されるバイナリ ファイルを分析し、イベント、接続データ、およびネットワーク マップを生成します。
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
echo	コンテンツを標準出力に書き込むユーティリティ

実行可能ファイル	説明
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準grepでサポートされていない正規表現の拡張セットをサポートします
find	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MACアドレスが常に一定になるようにします
iptables	[アクセス権の設定（Access Configuration）]ページに加えられた変更に基づいてアクセス制限を処理します。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
logger	コマンドラインからsyslogデーモンにアクセスする方法を提供するユーティリティ
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動（名前変更）するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します
perl	perl プロセスを示します
ps	標準出力にプロセス情報を書き込むユーティリティ

実行可能ファイル	説明
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ
sfheartbeat	アプライアンスがアクティブであることを示す、ハートビート ブロードキャストを識別します。ハートビートはデバイスとManagement Centerの間の接続を維持するのに使用されます。
sfmb	メッセージ ブローカ プロセスを示します。Management Centerとデバイスとの間の通信を処理します。
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メール イベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップ サーバに SNMP トラップ データを転送します
snort	Snort が動作していることを示します
ssh	アプライアンスへのセキュア シェル（SSH）接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ （注） このユーティリティの CPU 使用率の出力は、CPU コアのさまざまなタイプの使用率が分離されたものです。実際の合計CPU使用率を知るには、ユーザープロセスとシステムプロセスの両方の使用率を加算する必要があります。 たとえば、top コマンドの出力が次の場合：`%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` この場合、CPU 時間の 76.6% がユーザープロセスによって使用され、CPU 時間の 22.1% がシステム（カーネル）プロセスによって使用されています。合計 CPU 使用率は 98.7% です。 そのため、このユーティリティでレポートされる CPU 使用率は、ヘルス モニター ダッシュボードとは異なるように見えます。また、このユーティリティでは 3 秒の間隔を使用して CPU 使用率が計算されます。一方、Management Centerのヘルスモニターでは 1 秒の間隔が使用されます。

実行可能ファイル	説明
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキスト ファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

関連トピック

アクセス リストの設定

[SFDataCorrelator プロセス統計情報（SFDataCorrelator Process Statistics）] セクション

Management Center では、現在の日付のデータコリレータとネットワーク検出プロセスに関する統計情報を表示できます。管理対象デバイスがデータの取得、復号化、および分析を実行する際に、ネットワーク検出プロセスはデータをフィンガープリントおよび脆弱性データベースと関連付けてから、Management Center で実行中のデータ コリレータで処理されるバイナリ ファイルを生成します。データ コリレータはバイナリ ファイルの情報を分析し、イベントを生成し、ネットワーク マップを作成します。

ネットワーク検出とデータ コリレータに表示される統計情報は、デバイスごとに 0:00 から 23:59 までの間に収集された統計情報を使用した、当日の平均です。

次の表に、データ コリレータ プロセスに表示される統計情報を示します。

表 *5:* データ コリレータ プロセスの統計情報

カテゴリ	説明
Events/Sec	データ コリレータが受信し処理する検出イベントの 1 秒あたりの数
Connections/Sec	データ コリレータが受信し処理する接続の 1 秒あたりの数
CPU Usage — User (%)	当日のユーザープロセスで使用される CPU 時間の平均パーセンテージ
CPU Usage — System (%)	当日のシステム プロセスで使用される CPU 時間の平均パーセンテージ
VmSize（KB）	データ コリレータに割り当てられたメモリの当日の平均サイズ（キロバイト単位）
VmRSS（KB）	当日のデータ コリレータで使用されるメモリの平均量（キロバイト単位）

[侵入イベント情報（Intrusion Event Information）] セクション

Management Center デバイスと管理対象デバイスのどちらでも、[統計情報（Statistics）] ページで、侵入イベントに関するサマリ情報を確認できます。表示される情報には、前回の侵入イベントの日時、過去 1 時間および過去 1 日に発生したイベントの合計数、データベース内のイベントの合計数などがあります。

（注） [統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションにある情報は、Management Center に送信された侵入イベントではなく、管理対象デバイスに保存されている侵入イベントに基づいています。管理対象デバイスが侵入イベントをローカルに格納できない（または格納しないように設定されている）場合、侵入イベント情報はこのページに表示されません。

次の表に、[統計情報（Statistics）] ページの [侵入イベント情報（Intrusion Event Information）] セクションに表示される統計情報を示します。

表 *6 :* 侵入イベント情報（*Intrusion Event Information*）

統計	説明
前回のアラート（Last Alert Was）	前回のイベントが発生した日時
過去 1 時間のイベントの合計（Total Events Last Hour）	過去 1 時間に発生したイベントの合計数
過去 1 日のイベントの合計（Total Events Last Day）	過去 24 時間に発生したイベントの合計数
データベース内のイベントの合計（Total Events in Database）	イベント データベース内のイベントの合計数

システム統計情報の表示

この表示には、Management Center とその管理対象デバイスの統計情報が含まれています。

始める前に

システム統計を表示するには、管理者またはメンテナンスユーザーであり、グローバルドメインにいる必要があります。

手順

ステップ 1 システム（⚙） > **[モニタリング（Monitoring）]** > **[統計（Statistics）]**を選択します。

ステップ 2 [デバイスの選択（Select Device(s)）] リストからデバイスを選択し、[デバイスの選択（Select Devices）] をクリックします。

ステップ 3 使用可能な統計を表示します。

ステップ 4 [ディスク使用状況（Disk Usage）] セクションでは、次の操作を実行できます。

- [カテゴリ別（By Category）]積み上げ横棒で、ディスク使用量カテゴリの上にポインタを移動すると、以下が（順番に）表示されます。
  - そのカテゴリが使用する使用可能なディスク領域の割合
  - ディスク上の実際のストレージ領域
  - そのカテゴリで使用可能なディスク領域の合計
- [パーティション別（By Partition）] の横にある矢印をクリックして展開します。マルウェア ストレージ パックがインストールされている場合は、`/var/storage` パーティションの使用状況が表示されます。

ステップ 5 （オプション）[プロセス（Processes）] の横にある矢印をクリックすると、システム統計情報の表示 （10 ページ）で説明されている情報が表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。