통계

다음 항목에서는 Firepower 시스템을 모니터링 하는 방법을 설명합니다.

시스템 통계 관련 정보

Statistics(통계) 페이지에는 디스크 사용 및 시스템 프로세스, Data Correlator(데이터 상관 처리) 통계 및 침입 이벤트 정보를 포함한 일반 어플라이언스 통계의 현재 상태가 나와 있습니다.

호스트 통계 섹션

다음 표는 Statistics(통계 자료) 페이지에 나열된 호스트 통계 자료에 대해 설명합니다.

표 ***1:*** 호스트 통계 자료

카테고리	설명
시간	시스템의 현재 시간
실행 시간	시스템이 마지막으로 시작된 후 경과한 날짜 수(해당되는 경우), 시간 및 분
메모리 사용	사용 중인 시스템 메모리의 백분율
로드 평균	지난 1분, 5분 15분 동안 CPU 큐 프로세스의 평균 수.

카테고리	설명
디스크 사용	사용 중인 디스크의 백분율 자세한 호스트 통계 자료를 보려면 화살표를 클릭합니다.
프로세스	시스템에서 실행 중인 프로세스의 요약.

Disk Usage(디스크 사용량) 섹션

Statistics(통계 자료) 페이지의 Disk Usage(디스크 사용) 섹션에서는 디스크 사용에 대한 즉각적인 개요를 카테고리 및 파티션 상태별로 제공합니다. 디바이스에 악성코드 스토리지 팩이 설치되어 있는 경우, 스토리지 팩의 파티션 상태도 확인할 수 있습니다. 이 페이지를 자주 모니터링하여 시스템 프로세스와 데이터베이스에 충분한 디스크 공간을 사용할 수 있는지 확인할 수 있습니다.

팁 또한 디스크 사용량 상태 모니터를 통해 디스크 사용량을 모니터링하고 디스크 공간 부족에 대해 알림을 보낼 수도 있습니다.

Processes(프로세스) 섹션

통계 페이지의 Processes(프로세스) 섹션에서는 현재 어플라이언스에서 실행 중인 프로세스를 볼 수 있습니다. 이 섹션에서는 실행되고 있는 각 프로세스에 대한 일반 처리 정보 및 특정 정보를 제공합니다. management center의 웹 인터페이스를 사용해 관리되는 모든 디바이스의 프로세스 상태를 볼 수 있습니다.

어플라이언스에서는 데몬 및 실행 파일이라는 두 가지 유형의 프로세스가 실행됩니다. 데몬은 항상 실행되며, 실행 파일은 필요한 경우 실행됩니다.

프로세스 상태 필드

통계 페이지의 프로세스 섹션을 확장하는 경우 다음을 확인할 수 있습니다.

CPU

다음 CPU 사용 정보를 확인할 수 있습니다.

- 사용자 처리 사용 백분율
- 시스템 처리 사용 백분율
- nice 사용 백분율(더 높은 우선 순위를 나타내는 음수인 nice 값을 지닌 프로세스의 CPU 사용량) nice 값은 시스템 프로세스에 대해 예약된 우선 순위를 나타내며 그 범위는 -20(가장 높은 우선 순위)에서 19(가장 낮은 우선 순위)까지입니다.
- 유휴 사용 백분율

MEM

다음 메모리 사용 정보를 확인할 수 있습니다.

- 메모리 내 총 킬로바이트 수
- 메모리 내 사용된 킬로바이트의 총 수
- 메모리 내 무료 킬로바이트의 총 수
- 메모리 내 버퍼된 킬로바이트의 총 수

Swap(스왑)

다음 스왑 사용 정보를 확인할 수 있습니다.

- 스왑 내 총 킬로바이트 수
- 스왑 내 사용된 킬로바이트의 총 수
- 스왑 내 무료 킬로바이트의 총 수
- 스왑 내 캐시된 킬로바이트의 총 수

다음 테이블은 프로세스 섹션의 각 열에 대해 설명합니다.

표 *2:* 프로세스 목록 열

열	설명
Pid	프로세스 ID 번호
사용자 이름	프로세스를 실행하는 사용자 또는 그룹 이름
Pri	프로세스 우선 순위
Nice	*nice* 값. 프로세스의 예약 우선 순위를 나타내는 값입니다. 그 범위는 -20(가장 높은 우선 순위)에서 19(가장 낮은 우선 순위)까지입니다.
크기	프로세스가 사용하는 메모리 크기(메가바이트를 나타내는 m표시가 없는 경우 킬로바이트 값)
Res	메모리에 상주하는 페이징 파일의 양(메가바이트를 나타내는 m이 값 뒤에 오지 않는 한 킬로바이트 단위)

열	설명
상태	프로세스 상태: • D — 프로세스가 중단할 수 없는 잠자기 상태에 있습니다(일반적으로 입력/출력). • N — 프로세스가 양수인 nice 값을 지닙니다. • R — 프로세스가 실행 가능합니다(실행을 위해 큐에서 대기). • S — 프로세스가 절전 모드에 있습니다. • T — 프로세스가 추적 또는 중지되고 있습니다. • W — 프로세스가 호출되고 있습니다. • X — 프로세스가 작동하지 않습니다. • Z — 프로세스가 작동하지 않습니다. • < — 프로세스가 음수인 nice 값을 지닙니다.
시간	프로세스가 실행되고 있는 시간(시간:분:초 단위)
Cpu	프로세스가 사용하고 있는 CPU의 백분율
명령	프로세스의 실행 가능한 이름

관련 항목

시스템 데몬, 4 페이지
실행 파일및 시스템 유틸리티, 6 페이지

시스템 데몬

데몬은 어플라이언스에서 계속 실행됩니다. 데몬은 필요한 경우 서비스의 가용성을 확인하고 프로세스를 생성합니다. 다음 표에서는 Process Status(처리 상태) 페이지에서 볼 수 있는 데몬을 나열하고 해당 기능에 대한 간단한 설명을 제공합니다.

참고 아래 표는 어플라이언스에서 실행할 수 있는 모든 프로세스의 전체 목록이 아닙니다.

표 ***3:*** 시스템 데몬

데몬	설명
crond	예약된 명령의 실행을 관리합니다(cron 작업).
dhclient	동적 호스트 IP 주소 부여를 관리합니다.
fpcollect	클라이언트 및 서버 지문의 컬렉션을 관리합니다.

데몬	설명
httpd	HTTP(Apache 웹 서버) 프로세스를 관리합니다.
httpsd	HTTPS(SSL을 사용하는 Apache 웹 서버) 서비스를 관리하고 작동하는 SSL 및 유 인증을 확인하며, 어플라이언스에 보안 웹 액세스를 제공하는 백그라운드에서
keventd	Linux 커널 이벤트 알림 메시지를 관리합니다.
klogd	Linux 커널 메시지의 차단 및 로깅을 관리합니다.
kswapd	Linux 커널 스왑 메모리를 관리합니다.
kupdated	디스크 동기화를 수행하는 Linux 커널 업데이트 프로세스를 관리합니다.
mysqld	데이터베이스 프로세스를 관리합니다.
ntpd	NTP(Network Time Protocol)프로세스를 관리합니다
pm	모든 시스템 프로세스를 관리하고 필요한 프로세스를 시작하며, 예기치 않게 실 로세스를 다시 시작합니다.
reportd	보고서를 관리합니다.
safe_mysqld	데이터베이스의 안전 모드 운영을 관리하고 오류가 발생하고 파일에 런타임 정 경우 데이터베이스 데몬을 다시 시작합니다.
SFDataCorrelator	데이터 전송을 관리합니다.
sfestreamer(management center만)	Event Streamer를 사용하는 서드파티 클라이언트 애플리케이션에 대한 연결을
sfmgr	어플라이언스로 향하는 sftunnel 연결을 사용하여 어플라이언스의 원격 관리 및 RPC 서비스를 제공합니다.
SFRemediateD(management center만)	교정 응답을 관리합니다.
sftimeserviced(management center만)	시간 동기화 메시지를 관리되는 디바이스에 전달합니다.
sfmbservice	어플라이언스에 대한 sftunnel 연결을 사용하여 원격 어플라이언스에서 실행되는 지 브로커 프로세스에 대한 액세스를 제공합니다. 현재는 상태 모니터가 매니지 에서 management center로 상태 이벤트 및 알림을 전송하는 데 사용됩니다.
sftroughd	수신 소켓에서 연결을 수신한 후 요청을 처리하기 위해 올바른 실행 파일(일반적 메시지 브로커, sfmb)을 호출합니다.
sftunnel	원격 어플라이언스와의 통신이 필요한 모든 프로세스에 안전한 커뮤니케이션 채 니다.

데몬	설명
sshd	SSH(Secure Shell) 프로세스를 관리하고 어플라이언스에 SSH 액세스를 제공하는 백에서 실행됩니다.
syslogd	시스템 로깅(syslog) 프로세스를 관리합니다.

실행 파일및 시스템 유틸리티

다른 프로세스에 의해 또는 사용자 작업을 통해 수행될 때 실행되는 시스템에는 많은 실행 파일이 있습니다. 다음 표는 Process Status(처리 상태) 페이지에서 볼 수 있는 실행 파일에 대해 설명합니다.

표 *4:* 시스템 실행 파일 및 유틸리티

실행 파일	설명
awk	`awk` 프로그래밍 언어로 작성된 프로그램을 실행하는 유틸리티입니다.
bash	GNU Bourne-Again 셸
cat	파일을 읽고 표준 출력에 콘텐츠를 작성하는 유틸리티입니다.
chown	사용자 및 그룹 파일 권한을 변경하는 유틸리티입니다.
chsh	기본 로그인 셸을 변경하는 유틸리티입니다.
SFDataCorrelator(management center만)	이벤트, 연결 데이터, 네트워크 맵을 생성하기 위해 시스템이 생성한 이진 파일을 분석합니다.
cp	파일을 복제하는 유틸리티입니다.
df	어플라이언스의 여유 공간에 대한 볼륨을 나열하는 유틸리티입니다.
echo	표준 출력에 콘텐츠를 작성하는 유틸리티입니다.
egrep	지정된 입력에 대한 파일 및 폴더를 검색하는 유틸리티이며, 표준 grep에서 지원되지 않는 확장된 정규식 집합을 지원합니다.
find	지정된 입력에 대한 디렉토리를 되풀이하여 검색하는 유틸리티입니다.
grep	지정된 입력에 대한 파일 및 디렉토리를 검색하는 유틸리티입니다.
halt	서버를 중지하는 유틸리티입니다.
httpsdctl	보안 Apache 웹 프로세스를 처리합니다.
hwclock	하드웨어 클럭에 대한 액세스를 허용하는 유틸리티입니다.
ifconfig	네트워크 구성 실행 파일을 나타냅니다. MAC 주소가 일정한 상태를 유지하는지 확인합니다.

실행 파일	설명
iptables	Access Configuration(액세스 구성) 페이지에 적용된 변경 사항에 기반하여 액세스 제한을 처리합니다.
iptables-restore	iptables 파일 복원을 처리합니다
iptables-save	iptables에 저장된 변경 사항을 처리합니다.
kill	세션 및 프로세스를 종료하는 데 사용할 수 있는 유틸리티입니다.
killall	모든 세션 및 프로세스를 종료하는 데 사용할 수 있는 유틸리티입니다
ksh	Korn 셸의 공개 도메인 버전입니다.
logger	명령줄에서 syslog 데몬에 액세스하는 방법을 제공하는 유틸리티입니다.
md5sum	지정된 파일에 대한 체크섬 및 블록 횟수를 인쇄하는 유틸리티입니다.
mv	파일을 옮기는 (이름을 바꾸는) 유틸리티입니다
myisamchk	데이터베이스 표 확인 및 복구를 나타냅니다.
mysql	데이터베이스 프로세스를 나타내며 여러 인스턴스가 표시될 수 있습니다.
openssl	인증서 인증 생성을 나타냅니다.
perl	perl 프로세스를 나타냅니다.
ps	표준 출력에 처리 정보를 작성하는 유틸리티입니다.
sed	하나 이상의 텍스트 파일을 수정하는 데 사용하는 유틸리티입니다.
sfheartbeat	어플라이언스가 활성 상태임을 나타내는 하트비트 브로드캐스트를 식별합니다. 하트비트는 디바이스와 management center 사이의 연결을 유지하는 데 사용됩니다.
sfmb	메시지 브로커 프로세스를 나타내며 management center과 디바이스 간 통신을 처리합니다.
sh	Korn 셸의 공개 도메인 버전입니다.
shutdown	어플라이언스를 종료하는 유틸리티입니다.
sleep	지정된 시간(초) 동안 프로세스를 중지하는 유틸리티입니다.
smtpclient	이메일 이벤트 알림 기능이 활성화된 경우 이메일 전송을 처리하는 메일 클라이언트입니다.

실행 파일	설명
snmptrap	SNMP 알림 기능이 활성화된 경우 지정된 SNMP 트랩 서버에 SNMP 트랩 데이터를 전달합니다.
snort	Snort가 실행되고 있음을 나타냅니다.
ssh	어플라이언스로 향하는 SSH(Secure Shell) 연결을 나타냅니다.
sudo	관리자가 아닌 사용자가 실행 파일을 실행할 수 있는 sudo 프로세스를 나타냅니다.
top	상위 CPU 프로세스에 대한 정보를 표시하는 유틸리티입니다. 참고 이 유틸리티의 CPU 사용량 출력은 CPU 코어의 여러 사용량 유형이 분할된 것입니다. 실제 총 CPU 사용량을 확인하려면 사용자 프로세스와 시스템 프로세스 사용량을 모두 추가해야 합니다. top 명령의 출력 예: `%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` 여기서 CPU 시간의 76.6%는 사용자 프로세스에 의해, CPU 시간의 22.1%는 시스템(커널) 프로세스에 의해 사용됩니다. 총 CPU 사용량은 98.7%입니다. 따라서 이 유틸리티에서 보고되는 CPU 사용량은 상태 모니터 대시보드와 다르게 나타납니다. 또한, 이 유틸리티는 3초 간격을 사용하여 CPU 사용량을 계산합니다. 반면 Management Center 상태 모니터는 1초 간격을 사용합니다.
touch	지정된 파일의 액세스 및 변경 횟수를 변경하는 데 사용할 수 있는 유틸리티입니다.
vim	텍스트 파일을 수정하는 데 사용하는 유틸리티입니다.
wc	지정된 파일에서 회선, 단어 및 바이트 계산을 수행하는 유틸리티입니다.

관련 항목

액세스 목록 구성

SFDataCorrelator 프로세스 통계 섹션

management center에서 현재 날짜까지의 Data Correlator 및 네트워크 검색 프로세스에 대한 통계를 볼 수 있습니다. 관리되는 디바이스가 데이터 수집, 디코딩 및 분석을 수행하는 동안 네트워크 검색 프로세스는 데이터를 지문 및 취약성 데이터베이스와 상호 연결한 다음, management center에서 실행되는 Data Correlator에 의해 처리되는 이진 파일을 생성합니다. The Data Correlator는 이진 파일의 정보를 분석하고 이벤트를 생성하고 네트워크 맵을 만듭니다.

네트워크 검색 및 Data Correlator에 표시되는 통계는 현재 날짜의 평균으로 오전 12:00부터 오후 11:59 사이에 각 기기에서 수집된 통계가 사용됩니다.

다음 테이블은 Data Correlator 프로세스에 표시되는 통계에 대해 설명합니다.

표 ***5: Data Correlator*** 프로세스 통계

카테고리	설명
이벤트/초	Data Correlator에서 초당 수신하여 처리하는 검색 이벤트의 수
연결/초	Data Correlator에서 초당 수신하여 처리하는 연결의 수
CPU 사용량 — 사용자(%)	현재 날짜에 대해 사용자 프로세스에 소비되는 평균 CPU 시간의 비율
CPU 사용량 — 시스템(%)	현재 날짜에 대해 시스템 프로세스에 소비되는 평균 CPU 시간의 비율
VmSize(KB)	현재 날짜에 대해 Data Correlator에 할당된 평균 메모리의 크기(킬로바이트 단위)
VmRSS	현재 날짜에 대해 Data Correlator에서 사용하는 평균 메모리의 양(킬로바이트 단위)

침입 이벤트 정보 섹션

management center 및 관리되는 디바이스의 통계 페이지에서 침입 이벤트에 대한 요약 정보를 볼 수 있습니다. 이 정보에는 마지막 침입 이벤트 날짜 및 시간, 이전 시간 및 날짜에 발생한 총 이벤트 수, 데이터베이스의 총 이벤트 수가 포함됩니다.

참고 통계 페이지 내 침입 이벤트 정보 섹션의 정보는 management center에 전송된 침입 이벤트가 아니라 관리되는 디바이스에 저장된 침입 이벤트를 기반으로 합니다. 만약 관리되는 디바이스가 로컬에서 침입 이벤트를 저장할 수 없는 (또는 저장하지 않도록 설정된) 경우 이 페이지에 침입 이벤트가 표시되지 않습니다.

다음 테이블은 통계 페이지의 침입 이벤트 정보 섹션에 표시되는 통계에 대해 설명합니다.

표 ***6:*** 침입 이벤트 정보

통계	설명
최근 경보	마지막 이벤트가 발생한 날짜 및 시간을 나타냅니다.
최근 1시간의 전체 이벤트	최근 1시간 동안 발생한 전체 이벤트 수를 나타냅니다.
최근 1일의 전체 이벤트	지난 24시간 동안 발생한 전체 이벤트 수를 나타냅니다.

통계	설명
데이터베이스의 전체 이벤트	이벤트 데이터베이스에 있는 전체 이벤트 수를 나타냅니다.

시스템 통계 보기

management center 및 관련 매니지드 디바이스에 대한 통계도 표시됩니다.

시작하기 전에

시스템 통계를 보려면 관리자 또는 유지 보수 사용자여야 하며 전역 도메인에 있어야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Monitoring(**모니터링**)** > **Statistics(**통계**)**을(를) 선택합니다.

단계 **2** **Select Device(s)(**디바이스 선택**)** 목록에서 디바이스를 선택하고 **Select Devices(**디바이스 선택**)**를 클릭합니다.

단계 **3** 사용 가능한 통계를 봅니다.

단계 **4** 디스크 사용량 섹션에서 다음을 수행할 수 있습니다.

- 다음을 보려면 **By Category(**카테고리별로**)** 누적 막대의 디스크 사용량 카테고리 위에 포인터를 올려 놓습니다. (순서대로)
  - 해당 카테고리에 사용된 사용 가능한 디스크 공간의 백분율
  - 디스크의 실제 저장 공간
  - 해당 카테고리에 사용 가능한 모든 디스크 공간
- **By Partition(**파티션별**)** 옆의 화살표를 클릭하여 확대합니다. 악성코드 스토리지 팩이 설치되어 있는 경우, `/var/storage` 파티션 사용량이 표시됩니다.

단계 **5** (선택 사항) 시스템 통계 보기, 10 페이지에 설명된 정보를 보려면 **Processes(**프로세스**)** 옆의 화살표를 클릭합니다.