시스템 감사

다음 주제에서는 시스템에서의 활동을 감사하는 방법을 설명합니다.

시스템 로그

시스템 로그(syslog) 페이지에서는 어플라이언스에 대한 시스템 로그 정보를 제공합니다.

시스템에서의 활동은 다음 두 가지 방법으로 감사할 수 있습니다. Firepower System에 속하는 어플라이언스는 사용자와 웹 인터페이스의 각 상호 작용에 대한 감사 기록을 생성하고 시스템 로그에 시스템 상태 메시지도 로깅합니다.

시스템 로그는 시스템에서 생성된 각 메시지를 표시합니다. 다음 항목이 순서대로 나열됩니다.

- 메시지가 생성된 날짜
- 메시지가 생성된 시간
- 메시지를 생성한 호스트
- 메시지 자체

시스템 로그 보기

시스템 로그 정보는 로컬입니다. 예를 들어 Firepower Management Center를 사용하여 매니지드 디바이스에서 시스템 로그의 시스템 상태 메시지를 볼 수 없습니다.

UNIX 파일 검색 유틸리티 Grep에서 허용되는 대부분의 구문을 사용하여 메시지를 필터링할 수 있습니다. 이에 따라 패턴 매칭에 Grep 호환 정규식을 사용할 수 있습니다.

시작하기 전에

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

프로시저

단계 **1** **System(**시스템**)** > **Monitoring(**모니터링**)** > **Syslog**을(를) 선택합니다.

단계 **2** 시스템 로그에서 특정 메시지 내용을 검색하려면

a) 시스템 로그 필터 구문, 2 페이지에 설명된 대로 필터 필드에 단어 또는 쿼리를 입력합니다.

Grep 호환 검색 구문만 지원됩니다.

예:

사용자 이름 "Admin"이 포함된 모든 로그 항목을 검색하려면 `Admin`을 사용합니다.

11월 27일에 생성된 모든 로그 항목을 검색하려면 `Nov[[:space:]]*27` 또는 `Nov.*27`을 사용합니다(하지만 `Nov 27` 또는 `Nov*27` 은 사용하지 마십시오).

11월 5일의 권한 부여 디버깅 정보를 포함하는 모든 로그 항목을 검색하려면 `Nov[[:space:]]*5.*AUTH.*DEBUG`를 사용합니다.

b) 검색에서 대소문자를 구분하려면 **Case-sensitive**를 선택합니다. (기본적으로 필터는 대소문자를 구분하지 않습니다.)

c) 입력한 기준을 충족하지 않는 모든 시스템 로그 메시지를 검색하려면 **Exclusion**을 선택합니다.

d) **Go(**이동**)**를 클릭합니다.

시스템 로그 필터 구문

다음 표에서는 System Log 필터에서 사용할 수 있는 정규식 구문을 보여줍니다.

표 ***1:*** 시스템 로그 필터 구문

구문 구성 요소	설명	예
.	문자나 공백과 일치	`Admi.`는 `Admin`, `AdmiN`, `Admi1`, `Admi&`와 일치
`[[:alpha:]]`	알파벳 문자와 일치	`[[:alpha:]]dmin`은 `Admin`, `bdmin`, `Cdmin`과 일치
`[[:upper:]]`	알파벳 대문자와 일치	`[[:upper:]]dmin`은 `Admin`, `Bdmin`, `Cdmin`과 일치
`[[:lower:]]`	알파벳 소문자와 일치	`[[:lower:]]dmin`은 `admin`, `bdmin`, `cdmin`과 일치
`[[:digit:]]`	숫자와 일치	`[[:digit:]]dmin`은 `0dmin`, `1dmin`, `2dmin`과 일치
`[[:alnum:]]`	영숫자 문자와 일치	`[[:alnum:]]dmin`은 `1dmin`, `admin`, `2dmin`, `bdmin`과 일치

구문 구성 요소	설명	예
`[[:space:]]`	탭을 포함한 공백과 일치	`Feb[[:space:]]29`는 2월 29일의 로그와 일치
*	앞에 오는 0개 이상의 문자 또는 식 인스턴스와 일치	`ab*`는 `a`, `ab`, `abb`, `ca`, `cab`, `cabb`과 일치 `[ab] *`는 모두 일치
?	0개 또는 1개 인스턴스와 일치	`ab?`는 `a` 또는 `ab`와 일치
\	일반적으로 정규식 구문으로 해석되는 문자에 대한 검색 허용	`alert\?`는 `alert?`와 일치

시스템 감사 정보

Firepower System에 속하는 어플라이언스는 사용자와 웹 인터페이스의 각 상호 작용에 대한 감사 레코드를 생성합니다.

관련 항목

Introduction to Reports(보고서 소개)

감사 기록

Firepower Management Center 및 7000 및 8000 Series 디바이스는 사용자 활동에 대한 읽기 전용 감사 정보를 로깅합니다. 감사 로그는 감사 보기의 항목을 기준으로 감사 로그 메시지를 보고, 정렬하고, 필터링할 수 있는 표준 이벤트 보기에서 제공됩니다. 감사 정보를 손쉽게 삭제하고 보고할 수 있으며, 사용자가 변경한 내용에 대한 자세한 보고서를 볼 수 있습니다.

감사 로그에는 최대 100,000개의 항목이 저장됩니다. 감사 로그 항목 수가 100,000개를 초과하면 어플라이언스는 데이터베이스에서 가장 오래된 기록을 삭제하여 항목 수를 100,000개로 줄입니다.

참고 7000 또는 8000 Series 디바이스를 재부팅하고 가능한 한 빨리 보조 CLI에 로그인하는 경우, 로컬 웹 인터페이스를 사용할 수 있을 때까지는 실행하는 명령이 감사 로그에 기록되지 않습니다.

관련 항목

FMC에 대한 SSO 지침

감사 레코드 보기

Firepower Management Center 또는 7000 및 8000 Series 디바이스에서 감사 레코드의 테이블을 볼 수 있습니다. 사전 정의된 감사 워크플로에는 이벤트의 단일 테이블 보기가 포함되어 있습니다. 찾고 있

는 정보에 따라 테이블 보기를 조작할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Monitoring(**모니터링**)** > **Audit(**감사**)**를 사용하여 감사 로그 워크플로에 액세스합니다.

단계 **2** 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다. 자세한 내용은 이벤트 시간 제약 조건를 참고하십시오.

참고 어플라이언스의 구성된 타임 윈도우(전역 또는 이벤트 전용 모두 해당)를 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 테이블의 열 내용을 자세히 알아보려면 시스템 로그, 1 페이지를 참조하십시오.
- 현재 워크플로 페이지에서 이벤트를 정렬하고 제한하려면 테이블 보기 페이지 사용를 참조하십시오.
- 현재 제약 조건을 유지하면서 현재 워크플로의 페이지 사이를 이동하려면 워크플로 페이지의 왼쪽 위에서 해당 페이지 링크를 클릭합니다. 자세한 내용은 워크플로 사용를 참고하십시오.
- 워크플로에서 다음 페이지로 드릴다운하려면 드릴다운 페이지 사용 섹션을 참조하십시오.
- 특정 값으로 제한하려면 행 내의 값을 클릭합니다. 드릴다운 페이지에서 값을 클릭하면 다음 페이지로 이동하며 해당 값으로 제한됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다. 자세한 내용은 이벤트 보기 제약 조건를 참조하십시오.

  팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

- 감사 레코드를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭하거나 **Delete All(**모두 삭제**)**을 클릭하여 현재 제한된 보기의 모든 이벤트를 삭제합니다.
- 빠르게 돌아올 수 있도록 현재 페이지를 즐겨찾기하려면 **Bookmark This Page(**이 페이지 즐겨찾기**)**를 클릭합니다. 자세한 내용은 북마크를 참고하십시오.
- 즐겨찾기 관리 페이지로 이동하려면 **View Bookmarks(**즐겨찾기 보기**)**를 클릭합니다. 자세한 내용은 북마크를 참고하십시오.
- 현재 보기의 데이터를 기반으로 보고서를 생성하려면 **Report Designer(**리포트 디자이너**)**를 클릭합니다. 자세한 내용은 이벤트 보기에서 보고서 템플릿 생성를 참고하십시오.

- 감사 로그에 기록된 변경의 요약을 보려면 **Message(**메시지**)** 열의 해당 이벤트 옆에 있는 **Compare(**비교**)**를 클릭합니다. 자세한 내용은 감사 로그를 사용하여 변경 검사, 6 페이지를 참고하십시오.

관련 항목

이벤트 보기 제약 조건

감사 로그 워크플로 필드

다음 표는 보고 검색할 수 있는 감사 로그 필드를 설명합니다.

표 *2:* 감사 로그 필드

필드	설명
시간	어플라이언스가 감사 레코드를 생성한 시간과 날짜.
User	감사 이벤트를 트리거한 사용자의 사용자 이름.
하위 시스템	감사 레코드를 생성하기 위해 사용자가 따른 전체 메뉴 경로. 예를 들어 **System(**시스템**)** > **Monitoring(**모니터링**)** > **Audit(**감사**)**는 감사 로그를 보기 위한 메뉴 경로입니다. 메뉴 경로와 관련이 없는 몇몇 경우에는 Subsystem(하위 시스템) 필드에 이벤트 유형만 표시됩니다. 예를 들어 **Login(**로그인**)**은 사용자 로그인 시도를 분류합니다.
Message	사용자가 수행한 작업 또는 사용자가 페이지에서 클릭한 버튼. 예를 들어 `Page View(페이지 보기)`는 단순히 사용자가 Subsystem(하위 시스템)에 표시된 페이지를 봤음을 의미하는 반면, `Save(저장)`는 사용자가 페이지에서 **Save(**저장**)** 버튼을 클릭했음을 의미합니다. Firepower System에 대한 변경 사항은 클릭하면 변경 사항 요약을 볼 수 있는 비교 아이콘과 함께 나타납니다.
Source IP(소스 IP)	사용자가 사용한 호스트와 연결된 IP 주소. 참고: 이 필드를 검색할 때는 특정 IP 주소를 입력해야 합니다. 로그 감사를 검색할 때는 IP 범위를 사용할 수 없습니다.

필드	설명
도메인	감사 이벤트가 트리거되었을 때 사용자의 현재 도메인. 이 필드는 Firepower Management Center에 멀티테넌시를 구성한 경우에만 표시됩니다.
구성 변경 (검색만 해당)	검색 결과에서 구성 변경의 감사 레코드를 볼지 여부를 지정합니다. (`yes` 또는 `no`)
Count(개수)	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다. 이 필드는 검색할 수 없습니다.

관련 항목

이벤트 검색

감사 이벤트 테이블 보기

이벤트 보기의 레이아웃을 변경하거나 보기의 이벤트를 필드 값으로 제한할 수 있습니다. 열을 비활성화할 때 나타나는 팝업 윈도우에서 숨기려는 컬럼 헤드의 닫기(✕)를 클릭한 다음 **Apply(적용)**를 클릭합니다. 비활성화한 열은 나중에 다시 추가하지 않는 한 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화하면 Count(카운트) 열이 추가됩니다.

다른 열을 숨기거나 표시하려면, 또는 비활성화된 열을 다시 보기에 추가하려면, 해당 확인란을 선택하거나 선택 취소한 후 **Apply(적용)**를 클릭하십시오.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되고 워크플로의 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

관련 항목

워크플로 사용

감사 로그를 사용하여 변경 검사

시스템 변경 사항에 대한 자세한 보고서를 보려면 감사 로그를 사용할 수 있습니다. 이러한 보고서는 시스템의 현재 구성을 특정 변경 이전의 최신 구성과 비교합니다.

Compare Configurations 페이지에는 차이점을 쉽게 파악할 수 있도록 변경 이전의 시스템 구성과 실행 중인 구성이 나란히 배치됩니다. 감사 이벤트 유형, 마지막 수정 시간 및 변경을 수행한 사용자의 이름이 각 구성 위의 제목 표시줄에 표시 됩니다.

두 구성의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 구성 사이에서 다름을 나타내고, 그러한 차이점은 빨간색 텍스트로 표시됩니다.

- 녹색은 강조 표시된 설정이 둘 중 한 구성에만 나타남을 의미합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **Monitoring(**모니터링**)** > **Audit(**감사**)**을(를) 선택합니다.

단계 **2** **Message(**메시지**)** 열의 해당 감사 로그 이벤트 옆에 있는 **Compare(**비교**)**를 클릭합니다.

팁 제목 표시줄 위에 있는 **Previous(**이전**)** 또는 **Next(**다음**)**를 클릭하여 변경 사항을 개별적으로 탐색할 수 있습니다. 변경 요약의 길이가 한 페이지를 넘으면 오른쪽에 있는 스크롤바를 이용해 추가 변경 내용을 볼 수 있습니다.

감사 레코드 억제

감사 정책에서 Firepower System과의 특정 사용자 상호 작용 유형을 감사하도록 요구하지 않는 경우, 그러한 상호 작용이 Firepower Management Center 또는 7000 및 8000 Series 디바이스에서 감사 레코드를 생성하는 것을 차단할 수 있습니다. 예를 들어 기본적으로 사용자가 온라인 도움말을 볼 때마다 Firepower System은 감사 레코드를 생성합니다. 이러한 상호 작용 레코드를 유지할 필요가 없으면 자동으로 억제할 수 있습니다.

감사 이벤트 억제를 구성하려면 어플라이언스의 `admin` 사용자 계정에 대한 액세스 권한이 있어야 하며, 어플라이언스의 콘솔에 액세스하거나 SSH(Secure Shell)를 열 수 있어야 합니다.

⚠

주의 권한이 있는 사용자만 어플라이언스 및 `admin` 계정에 액세스할 수 있습니다.

시작하기 전에

이 절차를 수행하려면 관리자 사용자여야 합니다.

프로시저

`/etc/sf` 디렉터리에서 다음 형식으로 `AuditBlock` 파일을 생성합니다. 여기서 type은 감사 블록 유형, 8 페이지에 설명된 유형 중 하나입니다.

`AuditBlock.type`

참고 특정 유형의 감사 메시지에 대해 `AuditBlock.type` 파일을 생성한 후 억제를 해제하려는 경우 `AuditBlock.type` 파일의 내용을 삭제하되 파일 자체는 Firepower System에 남겨두어야 합니다.

감사 블록 유형

각 감사 블록 유형의 내용은 다음 표에 설명한 것처럼 특정 형식으로 지정해야 합니다. 파일 이름에 대/소문자를 정확하게 사용해야 합니다. 파일의 내용 역시 대/소문자를 구분합니다.

`AuditBlock` 파일을 추가하면 `Audit` 하위 시스템과 `Audit Filter type Changed` 메시지가 있는 감사 레코드가 감사 이벤트에 추가됩니다. 보안상의 이유로 이 감사 레코드는 억제할 수 없습니다.

표 ***3:*** 감사 블록 유형

유형	설명
주소	`AuditBlock.address` 파일을 생성하고, 감사 로그에서 억제하려는 각 IP 주소를 한 줄에 하나씩 포함합니다. 주소의 시작 부분부터 매핑되는 경우, 부분적인 IP 주소를 사용할 수 있습니다. 예를 들어 부분 주소 `10.1.1`은 `10.1.1.0~10.1.1.255` 범위의 주소와 일치합니다.
메시지	이름이 `AuditBlock.message`인 파일을 생성하고, 억제하려는 메시지 하위 문자열을 한 줄에 하나씩 포함합니다. 파일에 `backup`을 포함하면 `backup`이라는 단어가 포함된 모든 메시지가 억제되도록 하위 문자열이 매칭됩니다.
하위 시스템	이름이 `AuditBlock.subsystem`인 파일을 생성하고, 억제하려는 각 하위 시스템을 한 줄에 하나씩 포함합니다. 하위 문자열은 매칭되지 않습니다. 정확한 문자열을 사용해야 합니다. 감사 대상 하위 시스템 목록은 감사 하위 시스템, 9 페이지를 참조하십시오.
사용자	이름이 `AuditBlock.user`인 파일을 생성하고, 억제하려는 각 사용자 계정을 한 줄에 하나씩 포함합니다. 사용자 이름의 시작 부분부터 매핑되는 것이라면 부분적인 문자열 매칭을 사용할 수 있습니다. 예를 들어 부분적 사용자 이름 `IPSAnalyst`는 사용자 이름 `IPSAnalyst1` 및 `IPSAnalyst2`과 일치합니다.

감사 하위 시스템

다음 표에는 감사 대상 하위 시스템이 나열되어 있습니다.

표 *4:* 하위 시스템 이름

이름	포함되는 사용자 상호 작용
Admin(관리자)	시스템 및 액세스 구성, 시간 동기화, 백업 및 복원, 디바이스 관리, 사용자 계정 관리, 예약 등의 관리 기능
알림	이메일, SNMP, syslog 알림 등의 알림 기능
감사 로그	감사 이벤트 보기
감사 로그 검색	감사 이벤트 검색
명령행	명령줄 인터페이스
구성	이메일 알림
상황별로 크로스 실행	시스템에 추가되거나 대시보드 및 이벤트 보기에서 액세스한 외부 리소스
COOP	운영 연속성 기능
날짜	이벤트 보기의 날짜 및 시간 범위
기본 하위 시스템	할당된 하위 시스템이 없는 옵션
탐지 및 예방 정책	침입 정책에 대한 메뉴 옵션
오류	시스템 레벨 오류
eStreamer	eStreamer 구성
최종 사용자 라이선스 계약	최종 사용자 라이선스 계약 검토
이벤트	침입 및 검색 이벤트 보기
이벤트 클립보드	침입 이벤트 클립보드
검토된 이벤트	검토된 침입 이벤트
이벤트 검색	모든 이벤트 검색
규칙 업데이트 `rule_update_id` 설치 실패	규칙 업데이트 설치 중
헤더	사용자 로그인 후 유저 인터페이스의 초기 표시
상태	상태 모니터링

이름	포함되는 사용자 상호 작용
상태 이벤트	상태 모니터링 이벤트 보기
도움말	온라인 도움말
고가용성	고가용성 쌍에서 Firepower Management Center 설정 및 관리
IDS 영향 플래그	침입 이벤트에 대한 영향 플래그 구성
IDS 정책	침입 정책
IDSRule sid:`sig_id` rev:`rev_num`	SID 기준 침입 규칙
인시던트	침입 인시던트
설치	업데이트 설치
침입 이벤트	침입 이벤트
로그인	웹 인터페이스 로그인 및 로그 아웃 기능
메뉴	모든 메뉴 옵션
Configuration export > `config_type` > `config_name`	특정 유형 및 이름의 구성가져오기
권한 에스컬레이션	사용자 역할 에스컬레이션
선호	사용자 계정의 표준 시간대와 개별 이벤트 환경 설정 등의 사용자 환경 설정
정책	침입 정책을 비롯한 모든 정책
등록	다음에서 디바이스 등록: FMC
RemoteStorageDevice	원격 스토리지 디바이스 구성
보고서	보고서 나열 및 리포트 디자이너 기능
규칙	침입 규칙 편집기 및 규칙 가져오기 프로세스를 비롯한 침입 규칙
규칙 업데이트 가져오기 로그	규칙 업데이트 가져오기 로그 보기
규칙 업데이트 설치	규칙 업데이트 설치
상태	Syslog, 호스트 및 성능 통계
시스템	다양한 시스템 전체 설정
작업 대기열	백그라운드 프로세스 상태 보기

이름	포함되는 사용자 상호 작용
사용자	사용자 계정과 역할 생성 및 수정