로깅 감사

ONTAP 9

NetApp
April 24, 2024

목차

로깅 감사

ONTAP에서 감사 로깅을 구현하는 방법

감사 로그에 기록된 관리 작업은 표준 AutoSupport 보고서에 포함되며, 특정 로깅 작업은 EMS 메시지에 포함됩니다. 또한 지정한 대상에 감사 로그를 전달할 수 있으며 CLI 또는 웹 브라우저를 사용하여 감사 로그 파일을 표시할 수 있습니다.

ONTAP 9.11.1부터 시스템 관리자를 사용하여 감사 로그 내용을 표시할 수 있습니다.

ONTAP 9.12.1부터 ONTAP는 감사 로그에 대한 변조 경고를 제공합니다. ONTAP는 매일 백그라운드 작업을 실행하여 audit.log 파일의 변조를 확인하고 변경 또는 변조된 로그 파일이 발견되면 EMS 경고를 보냅니다.

ONTAP는 클러스터에서 수행된 관리 작업(예: 실행된 요청, 요청을 트리거한 사용자, 사용자의 액세스 방법 및 요청 시간)을 기록합니다.

관리 활동은 다음 유형 중 하나일 수 있습니다.

- 일반적으로 표시되지 않는 명령 또는 작업에 적용되는 요청을 설정합니다
  - 예를 들어, 'create', 'modify', 'delete' 명령을 실행하면 이러한 요청이 실행됩니다.
  - 설정된 요청은 기본적으로 기록됩니다.
- 정보를 검색하여 관리 인터페이스에 표시하는 요청을 가져옵니다
  - 예를 들어 'show' 명령을 실행하면 이러한 요청이 실행됩니다.
  - GET 요청은 기본적으로 로깅되지 않지만 GET 요청이 ONTAP CLI에서 전송되는지 여부를 제어할 수 있습니다 (`-cliget`ONTAP API에서)를 클릭합니다 (-ontapiget`)를 선택하거나 REST API에서 가져옵니다 (`-httpget`)이 파일에 로그인되어 있습니다.

ONTAP는 노드의 `/mroot/etc/log/mlog/audit.log' 파일에 관리 활동을 기록합니다. CLI 명령(클러스터 셸, 노드 쉘, 비대화형 시스템 셸(대화형 시스템 셸 명령은 기록되지 않음))을 위한 세 개의 셸과 API 명령이 여기에 기록됩니다. 감사 로그에는 클러스터의 모든 노드가 시간 동기화되었는지 여부를 나타내는 타임스탬프가 포함됩니다.

Audit.log 파일은 AutoSupport Tool에 의해 지정된 수신인에게 전송된다. 또한 Splunk 또는 syslog 서버와 같이 지정한 외부 대상에 콘텐츠를 안전하게 전달할 수 있습니다.

Audit.log 파일은 매일 순환한다. 회전은 크기가 100MB에 도달하고 이전 48개 사본이 보존될 때도 발생합니다(최대 총 49개 파일). 감사 파일이 매일 회전을 수행하면 EMS 메시지가 생성되지 않습니다. 파일 크기 제한이 초과되어 Audit 파일이 회전하면 EMS 메시지가 발생한다.

ONTAP 9의 감사 로깅을 변경합니다

ONTAP 9부터는 Command-history.log 파일이 audit.log로 대체되고, mgwd.log 파일은 더 이상 Audit 정보를 포함하지 않는다. ONTAP 9로 업그레이드하는 경우 기존 파일과 해당 콘텐츠를 참조하는 스크립트나 도구를 검토해야 합니다.

ONTAP 9로 업그레이드한 후 기존 명령어 이력.log 파일을 보존한다. 새 감사.로그 파일이 (작성됨) 회전되면 해당 파일이 삭제(삭제)됩니다.

명령어-히스토리.로그 파일을 체크하는 툴과 스크립트는 업그레이드 시 명령어-히스토리.로그부터 audit.log로의 소프트 링크가 생성되기 때문에 계속 동작할 수 있다. 그러나 mgwd.log 파일을 확인하는 도구와 스크립트는 해당 파일에 더 이상 감사 정보가 없기 때문에 실패합니다.

또한 ONTAP 9 이상의 감사 로그에는 유용하지 않고 불필요한 로깅 활동을 유발하기 때문에 다음 항목이 더 이상 포함되지 않습니다.

- ONTAP에서 실행되는 내부 명령(즉, username=root)
- 명령 별칭(해당 명령이 가리키는 명령과는 별개)

ONTAP 9부터는 TCP 및 TLS 프로토콜을 사용하여 감사 로그를 외부 대상으로 안전하게 전송할 수 있습니다.

감사 로그 내용을 표시합니다

ONTAP CLI, System Manager 또는 웹 브라우저를 사용하여 클러스터의 `/mroot/etc/log/mlog/audit.log' 파일의 내용을 표시할 수 있습니다.

클러스터의 로그 파일 항목은 다음과 같습니다.

시간
: 로그 항목 타임 스탬프입니다.

응용 프로그램
: 클러스터에 연결하는 데 사용되는 애플리케이션입니다. 가능한 값의 예로는 'internal, console, ssh, http, ontapi, SNMP, rsh, telnet, service-processor 등이 있다.

사용자
: 원격 사용자의 사용자 이름입니다.

상태
: 성공, 보류, 오류 등 감사 요청의 현재 상태입니다.

메시지
: 명령 상태에 대한 오류 또는 추가 정보를 포함할 수 있는 선택적 필드입니다.

세션 **ID**입니다
: 요청이 수신된 세션 ID입니다. 각 SSH_SESSION_에는 세션 ID가 할당되고 각 HTTP, ONTAPI 또는 SNMP_REQUEST_에는 고유한 세션 ID가 할당됩니다.

스토리지 **VM**
: 사용자가 연결하는 데 사용되는 SVM.

범위
: 데이터 스토리지 VM에 요청이 있으면 'VM'을 표시하고, 그렇지 않으면 '클러스터'를 표시합니다.

명령 **ID**입니다
: CLI 세션에서 수신한 각 명령의 ID입니다. 이렇게 하면 요청과 응답을 서로 연관시킬 수 있습니다. ZAPI, HTTP 및 SNMP 요청에는 명령 ID가 없습니다.

웹 브라우저에서 ONTAP CLI의 클러스터의 로그 항목을 표시하고 시스템 관리자에서 ONTAP 9.11.1로 시작할 수 있습니다.

시스템 관리자

- 인벤토리를 표시하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택합니다. + 각 열에는 필터링, 정렬, 검색, 표시 및 인벤토리 범주를 제어하는 컨트롤이 있습니다. 재고 세부 정보는 Excel 통합 문서로 다운로드할 수 있습니다.
- 필터를 설정하려면 오른쪽 위에 있는 * Filter * (필터 *) 버튼을 클릭하고 원하는 필드를 선택합니다. +세션 ID 링크를 클릭하여 장애가 발생한 세션에서 실행된 모든 명령을 볼 수도 있습니다.

CLI를 참조하십시오

클러스터의 여러 노드에서 병합된 감사 항목을 표시하려면 +'보안 감사 로그 show_[parameters]_'를 입력합니다

'security audit log show' 명령을 사용하면 개별 노드의 감사 항목을 표시하거나 클러스터의 여러 노드에서 병합한 감사 항목을 표시할 수 있습니다. 웹 브라우저를 사용하여 단일 노드에 '/mroot/etc/log/mlog' 디렉토리의 컨텐츠를 표시할 수도 있습니다. 자세한 내용은 man 페이지를 참조하십시오.

웹 브라우저

웹 브라우저를 사용하여 단일 노드에 '/mroot/etc/log/mlog' 디렉토리의 내용을 표시할 수 있습니다. "웹 브라우저를 사용하여 노드의 로그, 코어 덤프 및 MIB 파일에 액세스하는 방법에 대해 알아보십시오".

감사 가져오기 요청 설정을 관리합니다

설정된 요청이 기본적으로 기록되지만 GET 요청은 기록되지 않습니다. 그러나 ONTAP HTML('-HttpGet'), ONTAP CLI('-cliget') 또는 ONTAP API('-ontapiget')에서 보낸 GET 요청이 파일에 기록되는지 여부를 제어할 수 있습니다.

시스템 관리자에서 감사 로깅 설정을 ONTAP CLI에서 수정할 수 있으며 ONTAP 9.11.1부터 시작할 수 있습니다.

시스템 관리자

1. 이벤트 및 작업 > 감사 로그 * 를 선택합니다.
2. 을 클릭합니다 ⚙ 오른쪽 위 모서리에서 추가 또는 제거할 요청을 선택합니다.

CLI를 참조하십시오

- ONTAP CLI 또는 API의 GET 요청을 감사 로그(audit.log 파일)에 기록하도록 지정하려면 기본 설정 요청 외에 + '보안 감사 수정[-cliget{on|off}][-HttpGet{ on|off}][-ontapiget{on|off}]'을 입력합니다
- 현재 설정을 표시하려면 + 보안 감사 표시 를 입력합니다

자세한 내용은 man 페이지를 참조하십시오.

감사 로그 대상을 관리합니다

감사 로그를 최대 10개의 대상으로 전달할 수 있습니다. 예를 들어, 모니터링, 분석 또는 백업을

위해 로그를 Splunk 또는 syslog 서버로 전달할 수 있습니다.

이 작업에 대해

전달을 구성하려면 syslog 또는 Splunk 호스트의 IP 주소, 포트 번호, 전송 프로토콜 및 전달된 로그에 사용할 syslog 기능을 제공해야 합니다. "syslog 기능에 대해 자세히 알아보십시오".

다음 전송 값 중 하나를 선택할 수 있습니다.

UDP 암호화되지 않음

보안이 없는 사용자 데이터그램 프로토콜(기본값)

TCP 암호화되지 않음

보안 기능이 없는 전송 제어 프로토콜

TCP 암호화

전송 계층 보안(TLS)이 있는 전송 제어 프로토콜 + A * 서버 확인 * 옵션은 TCP 암호화 프로토콜이 선택된 경우에 사용할 수 있습니다.

ONTAP CLI에서 감사 로그를 전달하고 ONTAP 9.11.1부터 System Manager에서 전달할 수 있습니다.

시스템 관리자

- 감사 로그 대상을 표시하려면 * 클러스터 > 설정 * 을 선택합니다. +로그 대상 수가 * 알림 관리 타일 * 에 표시됩니다. 을 클릭합니다 ⋮ 를 눌러 세부 정보를 표시합니다.
- 감사 로그 대상을 추가, 수정 또는 삭제하려면 * 이벤트 및 작업 > 감사 로그 * 를 선택한 다음 화면 오른쪽 상단의 * 감사 대상 관리 * 를 클릭합니다. 를 누릅니다 + Add 또는 을 클릭합니다 ⋮ 항목을 편집하거나 삭제하려면 * 호스트 주소 * 열에 입력합니다.

CLI를 참조하십시오

1. 감사 로그를 전달할 각 대상에 대해 대상 IP 주소 또는 호스트 이름 및 보안 옵션을 지정합니다.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - "cluster log-forwarding create" 명령이 대상 호스트를 ping하여 연결을 확인할 수 없으면 명령이 실패하고 오류가 표시됩니다. 권장하지는 않지만 명령과 함께 '-force' 매개 변수를 사용하면 연결 확인이 생략됩니다.
   - '-verify-server' 매개 변수를 'true'로 설정하면 로그 전달 대상 ID가 인증서의 유효성을 확인하여 확인됩니다. 프로토콜 필드에서 TCP 암호화 값을 선택한 경우에만 이 값을 'true'로 설정할 수 있습니다.

2. cluster log-forwarding show 명령을 사용하여 대상 레코드가 올바른지 확인합니다.

```
cluster1::> cluster log-forwarding show

                                                    Verify Syslog
Destination Host           Port   Protocol         Server Facility
-------------------------- ------ --------         ------ --------
192.168.123.96             514    udp-unencrypted false  user
192.168.123.98             514    tcp-encrypted   true   user
2 entries were displayed.
```

자세한 내용은 man 페이지를 참조하십시오.