로깅 감사

Active IQ Unified Manager 9.14

NetApp
August 22, 2024

목차

로깅 감사

감사 로그를 사용하여 감사 로그가 손상되었는지 여부를 감지할 수 있습니다. 사용자가 수행하는 모든 작업은 감사 로그에 모니터링 및 기록됩니다. 감사는 Active IQ Unified Manager의 모든 사용자 인터페이스 및 공개적으로 노출된 API 기능에 대해 수행됩니다.

감사 로그: 파일 보기 * 를 사용하여 Active IQ Unified Manager에서 사용 가능한 모든 감사 로그 파일을 보고 액세스할 수 있습니다. Audit Log: File View(감사 로그: 파일 보기)의 파일은 생성 날짜를 기준으로 나열됩니다. 이 보기에는 설치 또는 업그레이드 시 캡처된 모든 감사 로그의 정보가 시스템에 있는 것으로 표시됩니다. Unified Manager에서 작업을 수행할 때마다 정보가 업데이트되고 로그에서 사용할 수 있습니다. 각 로그 파일의 상태는 로그 파일의 변조 또는 삭제를 감지하기 위해 능동적으로 모니터링되는 ""파일 무결성 상태"" 속성을 사용하여 캡처됩니다. 시스템에서 감사 로그를 사용할 수 있는 경우 감사 로그에 다음 상태 중 하나가 포함될 수 있습니다.

상태	설명
활성	로그가 현재 로그되고 있는 파일입니다.
정상	비활성, 압축 및 시스템에 저장된 파일입니다.
변조되었습니다	파일을 수동으로 편집한 사용자에 의해 손상된 파일입니다.
manual_delete(수동 삭제)	권한이 있는 사용자가 삭제한 파일입니다.
롤오버_삭제	롤링 구성 정책에 따라 롤오프로 인해 삭제된 파일입니다.
Unexpected_delete를 선택합니다	알 수 없는 이유로 삭제된 파일입니다.

감사 로그 페이지에는 다음과 같은 명령 단추가 있습니다.

- 구성
- 삭제
- 다운로드

delete * 버튼을 사용하면 Audit Logs 보기에 나열된 감사 로그를 삭제할 수 있습니다. 감사 로그를 삭제하고 나중에 유효한 삭제를 확인하는 데 도움이 되는 파일을 삭제할 이유를 선택적으로 제공할 수 있습니다. Reason 열에는 삭제 작업을 수행한 사용자의 이름과 함께 이유가 나열됩니다.

> 로그 파일을 삭제하면 시스템에서 파일이 삭제되지만 DB 테이블의 항목은 삭제되지 않습니다.

감사 로그 섹션의 * 다운로드 * 버튼을 사용하여 Active IQ Unified Manager에서 감사 로그를 다운로드하고 감사 로그 파일을 내보낼 수 있습니다. "보통" 또는 "무단 변경"으로 표시된 파일은 압축된 .gzip 형식으로 다운로드됩니다.

감사 로그 파일은 주기적으로 보관되며 참조를 위해 데이터베이스에 저장됩니다. 보관 전에 보안 및 무결성을 유지하기 위해 감사 로그에 디지털 서명됩니다.

전체 AutoSupport 번들이 생성되면 지원 번들에는 아카이빙 및 액티브 감사 로그 파일이 모두 포함됩니다. 하지만

간단한 지원 번들이 생성되면 활성 감사 로그만 포함됩니다. 보관된 감사 로그는 포함되지 않습니다.

감사 로그 구성

감사 로그 섹션의 * 구성 * 버튼을 사용하여 감사 로그 파일에 대한 롤링 정책을 구성하고 감사 로그에 대한 원격 로깅을 활성화할 수 있습니다.

시스템에 저장할 데이터의 양과 빈도에 따라 * MAX 파일 크기 * 및 * 감사 로그 보존 일 * 의 값을 설정할 수 있습니다. 필드 * 총 감사 로그 크기 * 의 값은 시스템에 있는 총 감사 로그 데이터의 크기입니다. 롤오버 정책은 * 감사 로그 보존 기간 *, * 최대 파일 크기 * 및 * 총 감사 로그 크기 * 필드의 값에 따라 결정됩니다. 감사 로그 백업의 크기가 * TOTAL AUDIT LOG SIZE * 에 구성된 값에 도달하면 먼저 아카이빙된 파일이 삭제됩니다. 즉, 가장 오래된 파일이 삭제됩니다. 그러나 파일 항목은 데이터베이스에서 계속 사용할 수 있으며 ""롤오버 삭제""로 표시됩니다. 감사 로그 보존 기간 * 값은 감사 로그 파일이 보존되는 일수입니다. 이 필드에 설정된 값보다 오래된 파일은 롤오버됩니다.

단계

1. 감사 로그 * >> * 구성 * 을 클릭합니다.
2. 최대 파일 크기 *, * 총 감사 로그 크기 * 및 * 감사 로그 보존 기간 * 에 값을 입력합니다.

   원격 로깅을 활성화하려면 * 원격 로깅 사용 * 을 선택해야 합니다.

감사 로그의 원격 로깅을 사용하도록 설정합니다

감사 로그 구성 대화 상자에서 * 원격 로깅 사용 * 확인란을 선택하여 원격 감사 로깅을 활성화할 수 있습니다. 이 기능을 사용하여 감사 로그를 원격 Syslog 서버로 전송할 수 있습니다. 이렇게 하면 공간 제약 조건이 있을 때 감사 로그를 관리할 수 있습니다.

감사 로그의 원격 로깅은 Active IQ Unified Manager 서버의 감사 로그 파일이 변조될 경우에 대비하여 변조 불가능한 백업을 제공합니다.

단계

1. 감사 로그 구성 * 대화 상자에서 * 원격 로깅 사용 * 확인란을 선택합니다.

   원격 로깅을 구성하는 추가 필드가 표시됩니다.

2. 연결할 원격 서버의 * HOSTNAME * 및 * 포트 * 를 입력합니다.
3. server CA certificate * 필드에서 * browse * 를 클릭하여 대상 서버의 공용 인증서를 선택합니다.

   인증서는 '.pem' 형식으로 업로드되어야 합니다. 이 인증서는 대상 Syslog 서버에서 받아야 하며 만료되지 않아야 합니다. 인증서는 선택한 "hostname"을 'subjectAltName'(SAN) 속성의 일부로 포함해야 합니다.

4. * CHARSET *, * CONNECTION TIMEOUT *, * 재연결 지연 * 필드에 값을 입력합니다.

   이러한 필드의 값은 밀리초 단위입니다.

5. 필요한 Syslog 형식과 TLS 프로토콜 버전을 * format * 및 * protocol * 필드에서 선택합니다.
6. 대상 Syslog 서버에 인증서 기반 인증이 필요한 경우 * 클라이언트 인증 활성화 * 확인란을 선택합니다.

   감사 로그 구성을 저장하기 전에 클라이언트 인증 인증서를 다운로드하여 Syslog 서버에 업로드해야 합니다. 그렇지

않으면 연결이 실패합니다. Syslog 서버의 유형에 따라 클라이언트 인증 인증서의 해시를 만들어야 할 수도 있습니다.

예: syslog-ng를 사용하려면 ' openssl x509 -noout -hash -in cert.pem' 명령을 사용하여 인증서의 <hash>를 만들어야 합니다. 그런 다음 클라이언트 인증 인증서를 <hash>.0 뒤에 명명된 파일에 상징적으로 연결해야 합니다.

7. 저장 * 을 클릭하여 서버와의 연결을 구성하고 원격 로깅을 활성화합니다.

   감사 로그 페이지로 리디렉션됩니다.

> 연결 시간 초과 * 값은 구성에 영향을 줄 수 있습니다. 설정에 정의된 값보다 응답하는 데 시간이 오래 걸리는 경우 연결 오류로 인해 구성 오류가 발생할 수 있습니다. 성공적으로 연결하려면 * 연결 시간 초과 * 값을 늘리고 구성을 다시 시도하십시오.