감사 작동 방식
ONTAP 9

NetApp
February 12, 2026

목차

감사 작동 방식

기본적인 **ONTAP** 감사 개념에 대해 알아봅니다

ONTAP의 감사를 이해하려면 몇 가지 기본적인 감사 개념을 알고 있어야 합니다.

- * 스테이징 파일 *

  통합 및 변환 전에 감사 레코드가 저장되는 개별 노드의 중간 바이너리 파일입니다. 스테이징 파일은 스테이징 볼륨에 포함되어 있습니다.

- * 스테이징 볼륨 *

  ONTAP에서 스테이징 파일을 저장하기 위해 생성한 전용 볼륨입니다. 애그리게이트당 하나의 스테이징 볼륨이 있습니다. 스테이징 볼륨은 모든 감사 가능 스토리지 가상 시스템(SVM)에서 공유되며, 해당 애그리게이트 내 데이터 볼륨의 데이터 액세스 감사 레코드를 저장합니다. 각 SVM의 감사 레코드는 스테이징 볼륨 내의 개별 디렉토리에 저장됩니다.

  클러스터 관리자는 스테이징 볼륨에 대한 정보를 볼 수 있지만 다른 대부분의 볼륨 작업은 허용되지 않습니다. ONTAP만 스테이징 볼륨을 생성할 수 있습니다. ONTAP는 스테이징 볼륨에 이름을 자동으로 할당합니다. 모든 스테이징 볼륨 이름은 mdv_AUD_ 로 시작하고 그 스테이징 볼륨을 포함하는 애그리게이트의 UUID로 시작합니다 (예: mdv_AUD_1d0131843d4811e296fc123478563412).

- * 시스템 볼륨 *

  파일 서비스 감사 로그의 메타데이터와 같은 특수 메타데이터가 포함된 FlexVol 볼륨입니다. admin SVM은 시스템 볼륨을 소유하며 클러스터 전체에서 볼 수 있습니다. 스테이징 볼륨은 시스템 볼륨의 유형입니다.

- * 통합 작업 *

  감사가 설정되어 있을 때 생성되는 작업입니다. 각 SVM에서 장기적으로 실행되는 이 작업은 SVM 구성원 노드 전체의 스테이징 파일에서 감사 레코드를 가져갑니다. 이 작업은 감사 레코드를 날짜순으로 정렬하여 병합한 다음, evtx 또는 XML 파일 형식으로 감사 구성에 지정된 사용자 판독 가능한 이벤트 로그 형식으로 변환합니다. 변환된 이벤트 로그는 SVM 감사 구성에 지정된 감사 이벤트 로그 디렉토리에 저장됩니다.

ONTAP 감사 프로세스의 기능에 대해 알아봅니다

ONTAP 감사 프로세스는 Microsoft 감사 프로세스와 다릅니다. 감사를 구성하기 전에 ONTAP 감사 프로세스의 작동 방식을 이해해야 합니다.

감사 레코드는 처음에 개별 노드의 이진 스테이징 파일에 저장됩니다. SVM에서 감사를 사용하면 모든 구성원 노드가 해당 SVM에 대한 스테이징 파일을 유지합니다. 주기적으로 이러한 로그는 통합되어 사용자가 읽을 수 있는 이벤트 로그로 변환되며, SVM의 감사 이벤트 로그 디렉토리에 저장됩니다.

SVM에서 감사를 활성화할 때의 프로세스입니다

감사는 SVM에서만 활성화할 수 있습니다. 스토리지 관리자가 SVM에 대한 감사를 활성화할 때 감사 하위 시스템은 스테이징 볼륨이 있는지 여부를 확인합니다. SVM이 소유한 데이터 볼륨이 포함된 각 애그리게이트의 스테이징 볼륨이 있어야 합니다. 감사 하위 시스템은 필요한 스테이징 볼륨이 없는 경우 이를 생성합니다.

감사 하위 시스템은 감사를 사용하기 전에 다른 필수 구성 요소 작업도 완료합니다.

- 감사 서브시스템은 로그 디렉토리 경로를 사용할 수 있고 symlink를 포함하지 않는지 확인합니다.

  로그 디렉토리는 SVM 네임스페이스 내의 경로로 이미 존재해야 합니다. 감사 로그 파일을 보관할 새 볼륨 또는 qtree를 생성하는 것이 좋습니다. 감사 하위 시스템은 기본 로그 파일 위치를 할당하지 않습니다. 감사 구성에 지정된 로그 디렉토리 경로가 올바른 경로가 아닌 경우 "지정한 경로"/path"가 SVM "Vserver_NAME" 오류가 있는 네임스페이스에 없으므로 구성 생성을 감사하지 못합니다.

  디렉토리가 있지만 symlink가 포함된 경우 구성을 생성할 수 없습니다.

- 감사 기능은 통합 작업을 예약합니다.

  이 작업이 예약되면 감사가 활성화됩니다. SVM 감사 구성 및 로그 파일은 재부팅 후에도 또는 NFS 또는 SMB 서버가 중지 또는 재시작되어도 유지됩니다.

이벤트 로그 통합

로그 통합은 감사가 비활성화될 때까지 정기적으로 실행되는 예약된 작업입니다. 감사를 사용하지 않도록 설정하면 통합 작업에서 나머지 모든 로그가 통합되었는지 확인합니다.

감사 보장

기본적으로 감사는 보장됩니다. ONTAP는 노드를 사용할 수 없는 경우에도 감사 가능한 모든 파일 액세스 이벤트(구성된 감사 정책 ACL에 의해 지정됨)를 기록합니다. 해당 작업에 대한 감사 레코드가 영구 저장소의 스테이징 볼륨에 저장될 때까지 요청된 파일 작업을 완료할 수 없습니다. 공간이 부족하거나 다른 문제로 인해 스테이징 파일의 디스크에 감사 레코드를 커밋할 수 없는 경우 클라이언트 작업이 거부됩니다.

> 관리자 또는 권한 수준 액세스 권한이 있는 계정 사용자는 NetApp Manageability SDK 또는 REST API를 사용하여 파일 감사 로깅 작업을 건너뛸 수 있습니다. Audit.LOG 파일에 저장된 Command History 로그를 검토하여 NetApp Manageability SDK 또는 REST API를 사용하여 파일 작업이 수행되었는지 확인할 수 있습니다.
>
> 명령 기록 감사 로그에 대한 자세한 내용은 의 "관리 활동에 대한 감사 로깅 관리" 섹션을 참조하십시오 "시스템 관리".

노드를 사용할 수 없는 경우의 통합 프로세스

감사가 설정된 SVM에 속하는 볼륨을 포함하는 노드를 사용할 수 없는 경우 통합 감사 작업의 동작은 노드의 스토리지 페일오버(SFO) 파트너(또는 2노드 클러스터의 경우 HA 파트너)를 사용할 수 있는지 여부에 따라 달라집니다.

- SFO 파트너를 통해 스테이징 볼륨을 사용할 수 있는 경우 노드에서 마지막으로 보고된 스테이징 볼륨이 스캔되고 통합이 정상적으로 진행됩니다.
- SFO 파트너를 사용할 수 없는 경우 작업에 부분 로그 파일이 생성됩니다.

  노드에 연결할 수 없는 경우 통합 작업은 해당 SVM의 사용 가능한 다른 노드의 감사 레코드를 통합합니다. 작업이 완료되지 않은 것을 확인하기 위해 통합 파일 이름에 접미사 .partial이 추가됩니다.

- 사용할 수 없는 노드를 사용할 수 있게 되면 해당 노드의 감사 레코드가 해당 시점에 다른 노드의 감사 레코드와 통합됩니다.

- 모든 감사 레코드가 보존됩니다.

이벤트 로그 회전

감사 이벤트 로그 파일은 구성된 임계값 로그 크기에 도달하거나 구성된 일정에 도달하면 회전합니다. 이벤트 로그 파일이 순환되면 예약된 통합 작업에서 먼저 활성 변환된 파일의 이름을 타임 스탬프 아카이브 파일로 바꾼 다음 새 활성 변환 이벤트 로그 파일을 만듭니다.

SVM에서 감사를 사용하지 않도록 설정할 때의 프로세스입니다

SVM에서 감사를 사용하지 않도록 설정하면 통합 작업이 마지막으로 한 번 트리거됩니다. 모든 미해결, 기록된 감사 레코드는 사용자가 읽을 수 있는 형식으로 기록됩니다. SVM에서 감사를 사용하지 않도록 설정하고 확인할 수 있으면 이벤트 로그 디렉토리에 저장된 기존 이벤트 로그가 삭제되지 않습니다.

해당 SVM에 대한 기존 스테이징 파일이 모두 통합된 후에는 통합 작업이 일정에서 제거됩니다. SVM에 대한 감사 구성을 비활성화해도 감사 구성은 제거되지 않습니다. 스토리지 관리자는 언제든지 감사를 다시 활성화할 수 있습니다.

감사를 사용할 때 생성되는 감사 통합 작업은 통합 작업을 모니터링하고 오류로 인해 통합 작업이 종료되는 경우 다시 만듭니다. 사용자가 감사 통합 작업을 삭제할 수 없습니다.