SVM에서 NAS 이벤트를 감사합니다

ONTAP 9

NetApp
September 12, 2024

목차

SVM에서 NAS 이벤트를 감사합니다

SMB 및 NFS 감사 및 보안 추적

FPolicy를 사용하여 기본 감사 및 파일 정책 관리와 같은 ONTAP에서 SMB 및 NFS 프로토콜에 사용할 수 있는 파일 액세스 감사 기능을 사용할 수 있습니다.

다음과 같은 상황에서 SMB 및 NFS 파일 액세스 이벤트에 대한 감사를 설계하고 구현해야 합니다.

- 기본 SMB 및 NFS 프로토콜 파일 액세스가 구성되었습니다.
- 다음 방법 중 하나를 사용하여 감사 구성을 만들고 유지 관리하려고 합니다.
  - 기본 ONTAP 기능
  - 외부 FPolicy 서버

SVM에서 NAS 이벤트를 감사합니다

NAS 이벤트에 대한 감사는 스토리지 가상 시스템(SVM)에서 특정 SMB 및 NFS 이벤트를 추적하고 기록할 수 있는 보안 측정값입니다. 이를 통해 잠재적인 보안 문제를 추적하고 보안 위반의 증거를 제공할 수 있습니다. 또한 Active Directory 중앙 액세스 정책을 스테이징하고 감사하여 이러한 정책을 구현하면 어떤 결과가 초래되는지 확인할 수 있습니다.

SMB 이벤트

다음 이벤트를 감사할 수 있습니다.

- SMB 파일 및 폴더 액세스 이벤트입니다

  감사 기능이 활성화된 SVM에 속한 FlexVol 볼륨에 저장된 개체에 대해 SMB 파일 및 폴더 액세스 이벤트를 감사할 수 있습니다.

- SMB 로그온 및 로그오프 이벤트

  SVM에서 SMB 서버의 SMB 로그온 및 로그오프 이벤트를 감사할 수 있습니다.

- 중앙 액세스 정책 스테이징 이벤트입니다

  제안된 중앙 액세스 정책을 통해 적용된 권한을 사용하여 SMB 서버의 개체에 대한 효과적인 액세스를 감사할 수 있습니다. 중앙 액세스 정책의 스테이징을 통해 감사를 수행하여 중앙 액세스 정책이 구축되기 전에 어떤 영향이 있는지 확인할 수 있습니다.

  중앙 액세스 정책 스테이징에 대한 감사는 Active Directory GPO를 사용하여 설정되지만 SVM 감사 구성은 중앙 액세스 정책 스테이징 이벤트를 감사하도록 구성해야 합니다.

  SMB 서버에서 동적 액세스 제어를 사용하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만, 동적 액세스 제어를 설정한 경우에만 중앙 액세스 정책 스테이징 이벤트가 생성됩니다. 동적 액세스 제어는 SMB 서버 옵션을 통해 활성화됩니다. 기본적으로 활성화되어 있지 않습니다.

NFS 이벤트입니다

SVM에 저장된 객체에 NFSv4 ACL을 활용하여 파일 및 디렉토리 이벤트를 감사할 수 있습니다.

감사 작동 방식

기본 감사 개념

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 작동 방식

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.

감사 요구 사항 및 고려 사항

SVM(스토리지 가상 시스템)에 대한 감사를 구성 및 설정하기 전에 특정 요구사항과 고려 사항을 숙지해야 합니다.

- 지원되는 감사 사용 SVM의 최대 수는 사용 중인 ONTAP 버전에 따라 다릅니다.

ONTAP 버전입니다	최대
9.8 이하	50
9.9.1 이상	400

- 감사는 SMB 또는 NFS 라이센스와 관련이 없습니다.

  클러스터에 SMB 및 NFS 라이센스가 설치되어 있지 않은 경우에도 감사를 구성 및 활성화할 수 있습니다.

- NFS 감사는 보안 ACE(U형)를 지원합니다.
- NFS 감사의 경우 모드 비트와 감사 ACE 사이에 매핑이 없습니다.

  ACL을 모드 비트로 변환할 때 감사 ACE는 건너뜁니다. 모드 비트를 ACL로 변환할 때 감사 ACE가 생성되지 않습니다.

- 감사 구성에 지정된 디렉토리가 있어야 합니다.

  이 명령이 없으면 감사 구성을 만드는 명령이 실패합니다.

- 감사 구성에 지정된 디렉토리는 다음 요구 사항을 충족해야 합니다.
  - 디렉토리에는 심볼 링크가 포함되어 있지 않아야 합니다.

    감사 구성에 지정된 디렉터리에 심볼 링크가 포함된 경우 감사 구성을 생성하는 명령이 실패합니다.

  - 절대 경로를 사용하여 디렉토리를 지정해야 합니다.

    예를 들어, '/vs1/…/'와 같은 상대 경로를 지정하면 안 됩니다.

- 감사는 스테이징 볼륨에 사용 가능한 공간이 있는 경우에 따라 달라집니다.

  감사된 볼륨이 포함된 애그리게이트에서 스테이징 볼륨에 충분한 공간이 있는지 확인하고 계획을 세워야 합니다.

- 감사는 변환된 이벤트 로그가 저장되는 디렉토리가 포함된 볼륨에 사용 가능한 공간이 있는지 여부에 따라 달라집니다.

  이벤트 로그를 저장하는 데 사용되는 볼륨에 충분한 공간이 있는지 확인하고 계획을 세워야 합니다. 감사 구성을 생성할 때 '-rotate-limit' 매개 변수를 사용하여 감사 디렉토리에 유지할 이벤트 로그 수를 지정할 수 있습니다. 감사 구성은 볼륨에 이벤트 로그에 사용할 수 있는 충분한 공간이 있는지 확인하는 데 도움이 됩니다.

- SMB 서버에서 동적 액세스 제어를 설정하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만 동적 액세스 제어를 활성화하여 중앙 액세스 정책 스테이징 이벤트를 생성해야 합니다.

  동적 액세스 제어는 기본적으로 사용되지 않습니다.

감사를 설정할 때 애그리게이트 공간 고려 사항

감사 구성이 생성되고 클러스터에서 하나 이상의 SVM(스토리지 가상 머신)에 감사가 활성화되어 있으면 감사 서브시스템이 모든 기존 애그리게이트 및 생성되는 모든 새 애그리게이트에 스테이징 볼륨을 생성합니다. 클러스터에서 감사를 활성화할 때는 애그리게이트 공간의 특정 고려 사항을 알아야 합니다.

애그리게이트에서 사용할 수 없는 공간으로 인해 스테이징 볼륨 생성이 실패할 수 있습니다. 감사 구성을 생성할 때 기존 애그리게이트에 스테이징 볼륨을 포함할 충분한 공간이 없는 경우 이러한 문제가 발생할 수 있습니다.

SVM에 대한 감사를 활성화하기 전에 스테이징 볼륨에 대한 기존 애그리게이트에 충분한 공간이 있는지 확인해야 합니다.

스테이징 파일의 감사 레코드 크기에 대한 제한 사항

스테이징 파일의 감사 레코드 크기는 32KB를 초과할 수 없습니다.

대규모 감사 레코드가 발생할 수 있는 경우

다음 시나리오 중 하나에서 관리 감사 중에 대규모 감사 레코드가 발생할 수 있습니다.

- 많은 수의 사용자가 있는 그룹에 사용자를 추가 또는 삭제합니다.
- 많은 수의 파일 공유 사용자와 파일 공유에서 파일 공유 ACL(액세스 제어 목록)을 추가 또는 삭제합니다.
- 기타 시나리오.

이 문제를 방지하려면 관리 감사를 사용하지 않도록 설정합니다. 이렇게 하려면 감사 구성을 수정하고 감사 이벤트 유형 목록에서 다음을 제거합니다.

- 파일 공유
- 사용자 계정
- 보안 그룹
- authorization-policy-change를 참조하십시오

  제거 후에는 파일 서비스 감사 하위 시스템에 의해 감사되지 않습니다.

너무 큰 감사 기록의 영향

- 감사 레코드 크기가 너무 크면(32KB 이상) 감사 레코드가 생성되지 않고 감사 하위 시스템에서 다음과 유사한 EMS(이벤트 관리 시스템) 메시지가 생성됩니다.

  "파일 서비스 감사 하위 시스템이 max_audit_record_size 값보다 크기 때문에 작업에 실패했거나 감사 레코드를 잘라냅니다. SVM UUID=%s, event_id=%u, size=%u

  감사가 보장된 경우 감사 레코드를 생성할 수 없기 때문에 파일 작업이 실패합니다.

- Audit Record의 크기가 9,999바이트보다 큰 경우 위와 동일한 EMS 메시지가 출력된다. 키 값이 더 큰 부분 감사 레코드가 누락되었습니다.
- 감사 레코드가 2,000자를 초과하면 실제 값 대신 다음 오류 메시지가 표시됩니다.

  이 필드의 값이 너무 길어 표시할 수 없습니다

지원되는 감사 이벤트 로그 형식은 무엇입니까

변환된 감사 이벤트 로그에 지원되는 파일 형식은 evtx 및 XML 파일 형식입니다.

감사 구성을 만들 때 파일 형식의 유형을 지정할 수 있습니다. 기본적으로 ONTAP는 바이너리 로그를 'evtx' 파일 형식으로 변환합니다.

감사 이벤트 로그를 봅니다

감사 이벤트 로그를 사용하여 적절한 파일 보안이 있는지 여부와 잘못된 파일 및 폴더 액세스 시도가 있는지 여부를 확인할 수 있습니다. evtx 또는 XML 파일 형식으로 저장된 감사 이벤트 로그를 보고 처리할 수 있습니다.

- evtx 파일 형식

  Microsoft 이벤트 뷰어를 사용하여 변환된 'evtx' 감사 이벤트 로그를 저장된 파일로 열 수 있습니다.

  이벤트 뷰어를 사용하여 이벤트 로그를 볼 때 사용할 수 있는 두 가지 옵션이 있습니다.

  - 일반 보기

모든 이벤트에 공통되는 정보는 이벤트 레코드에 대해 표시됩니다. 이 버전의 ONTAP에서는 이벤트 레코드에 대한 이벤트 관련 데이터가 표시되지 않습니다. 상세도를 사용하여 이벤트 관련 데이터를 표시할 수 있습니다.

  - 상세보기

    친숙한 뷰와 XML 뷰를 사용할 수 있습니다. 보기 및 XML 보기에는 모든 이벤트에 공통되는 정보와 이벤트 레코드에 대한 이벤트 관련 데이터가 모두 표시됩니다.

- 'xml' 파일 형식

  XML 파일 형식을 지원하는 타사 응용 프로그램에서 XML 감사 이벤트 로그를 보고 처리할 수 있습니다. XML 스키마와 XML 필드 정의에 대한 정보가 있는 경우 XML 보기 도구를 사용하여 감사 로그를 볼 수 있습니다. XML 스키마 및 정의에 대한 자세한 내용은 을 참조하십시오 "ONTAP 감사 스키마 참조".

이벤트 뷰어를 사용하여 활성 감사 로그를 보는 방법

클러스터에서 감사 통합 프로세스가 실행 중인 경우 통합 프로세스에서 감사 사용 스토리지 가상 시스템(SVM)에 대한 새 레코드를 활성 감사 로그 파일에 추가합니다. 이 활성 감사 로그는 Microsoft 이벤트 뷰어에서 SMB 공유를 통해 액세스하고 열 수 있습니다.

이벤트 뷰어에는 기존 감사 레코드를 보는 것 외에도 콘솔 창에서 콘텐츠를 새로 고칠 수 있는 새로 고침 옵션이 있습니다. 새로 추가된 로그를 이벤트 뷰어에서 볼 수 있는지 여부는 활성 감사 로그에 액세스하는 데 사용된 공유에 oplocks가 설정되어 있는지 여부에 따라 달라집니다.

공유에 oplocks 설정을 지정합니다	동작
활성화됨	이벤트 뷰어는 해당 시점까지 기록된 이벤트가 포함된 로그를 엽니다. 새로 고침 작업은 통합 프로세스에 추가된 새 이벤트로 로그를 새로 고치지 않습니다.
사용 안 함	이벤트 뷰어는 해당 시점까지 기록된 이벤트가 포함된 로그를 엽니다. 새로 고침 작업은 통합 프로세스에 추가된 새 이벤트로 로그를 새로 고칩니다.

이 정보는 evtx 이벤트 로그에만 적용됩니다. XML 이벤트 로그는 브라우저에서 SMB를 통해 보거나 XML 편집기나 뷰어를 사용하여 NFS를 통해 볼 수 있습니다.

감사할 수 있는 **SMB** 이벤트입니다

감사할 수 있는 **SMB** 이벤트 개요

ONTAP는 특정 파일 및 폴더 액세스 이벤트, 특정 로그온 및 로그오프 이벤트, 중앙 액세스 정책 스테이징 이벤트를 비롯한 특정 SMB 이벤트를 감사할 수 있습니다. 감사할 수 있는 액세스 이벤트를 알면 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

ONTAP 9.2 이상에서 다음과 같은 추가 SMB 이벤트를 감사할 수 있습니다.

이벤트 ID(EVT/evtx)	이벤트	설명	범주

4670)을 참조하십시오	개체 권한이 변경되었습니다	객체 액세스: 권한이 변경되었습니다.	파일 액세스
4907	개체 감사 설정이 변경되었습니다	개체 액세스: 감사 설정이 변경되었습니다.	파일 액세스
4913	객체 중앙 액세스 정책이 변경되었습니다	개체 액세스: 캡이 변경되었습니다.	파일 액세스

다음 SMB 이벤트는 ONTAP 9.0 이상에서 감사할 수 있습니다.

이벤트 ID(EVT/evtx)	이벤트	설명	범주
540/4624	계정이 성공적으로 로그온되었습니다	로그온/로그오프: 네트워크(SMB) 로그온.	로그온 및 로그오프
529/4625	계정 로그온에 실패했습니다	로그온/로그오프: 알 수 없는 사용자 이름 또는 잘못된 암호입니다.	로그온 및 로그오프
530/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정 로그온 시간 제한.	로그온 및 로그오프
531/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정이 현재 비활성화되었습니다.	로그온 및 로그오프
532/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자 계정이 만료되었습니다.	로그온 및 로그오프
533/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자가 이 컴퓨터에 로그온할 수 없습니다.	로그온 및 로그오프
534/4625	계정 로그온에 실패했습니다	로그온/로그오프: 여기에 로그온 유형이 부여되지 않았습니다.	로그온 및 로그오프
535/4625	계정 로그온에 실패했습니다	로그온/로그오프: 사용자 암호가 만료되었습니다.	로그온 및 로그오프
537/4625	계정 로그온에 실패했습니다	로그온/로그오프: 위의 이유 이외의 이유로 로그온하지 못했습니다.	로그온 및 로그오프
539/4625	계정 로그온에 실패했습니다	로그온/로그오프: 계정이 잠겼습니다.	로그온 및 로그오프
538/4634	계정이 로그오프되었습니다	로그온/로그오프: 로컬 또는 네트워크 사용자 로그오프.	로그온 및 로그오프

560/4656)을 참조하십시오	객체 열기/객체 생성	오브젝트 액세스: 오브젝트(파일 또는 디렉토리)가 열려 있습니다.	파일 액세스
563/4659	삭제 의도에 따라 개체를 엽니다	오브젝트 액세스: 오브젝트(파일 또는 디렉토리)에 대한 핸들이 삭제 의향과 함께 요청되었습니다.	파일 액세스
564/4660	개체 삭제	오브젝트 액세스: 오브젝트 삭제(파일 또는 디렉토리). ONTAP는 Windows 클라이언트가 개체(파일 또는 디렉터리)를 삭제하려고 할 때 이 이벤트를 생성합니다.	파일 액세스
567/4663	개체 읽기/개체 쓰기/개체 속성 가져오기/개체 특성 설정	오브젝트 액세스: 오브젝트 액세스 시도(읽기, 쓰기, get 속성, set 속성) • 참고: * 이 이벤트의 경우 ONTAP는 개체에 대한 첫 번째 SMB 읽기 및 첫 번째 SMB 쓰기 작업(성공 또는 실패)만 감사합니다. 이렇게 하면 단일 클라이언트가 개체를 열고 동일한 개체에 대해 여러 번의 연속 읽기 또는 쓰기 작업을 수행할 때 ONTAP에서 과도한 로그 항목을 만들지 못하게 됩니다.	파일 액세스
해당 없음/4664	하드 링크	개체 액세스: 하드 링크를 만들려고 했습니다.	파일 액세스
해당 없음/4818	제안된 중앙 액세스 정책은 현재 중앙 액세스 정책과 동일한 액세스 권한을 부여하지 않습니다	객체 액세스: 중앙 액세스 정책 스테이징.	파일 액세스
NA/NA Data ONTAP 이벤트 ID 9999	개체 이름 바꾸기	오브젝트 액세스: 오브젝트 이름 바꾸기. ONTAP 이벤트입니다. 현재 Windows에서 단일 이벤트로 지원되지 않습니다.	파일 액세스
NA/NA Data ONTAP 이벤트 ID 9998	개체 연결 끊기	개체 액세스: 개체 연결 해제됨. ONTAP 이벤트입니다. 현재 Windows에서 단일 이벤트로 지원되지 않습니다.	파일 액세스

이벤트 **4656**에 대한 추가 정보

감사 XML 이벤트의 HandleID 태그에는 액세스한 개체(파일 또는 디렉터리)의 핸들이 들어 있습니다. evtx 4656 이벤트에 대한 "HandleID" 태그는 open 이벤트가 새 개체를 만들거나 기존 개체를 여는 데 사용되는지 여부에 따라 다른 정보를 포함합니다.

- Open event가 Open request로 새로운 object(file or directory)를 생성하려는 경우 Audit XML event의 HandleID 태그는 빈 HandleID를 표시합니다(예: "<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>").

  실제 개체 생성이 발생하기 전과 핸들이 있기 전에 열려 있는(새 개체 만들기) 요청을 감사하기 때문에 "HandleID"가 비어 있습니다. 같은 개체에 대한 후속 감사 이벤트에는 'HandleID' 태그에 올바른 객체 핸들이 있습니다.

- open event가 기존 object를 열기 위한 open 요청인 경우 audit event는 'HandleID' 태그(예: "<Data Name="HandleID">0000000401;00;000000ea;00123ed4</Data>")에서 해당 object의 할당된 handle을 갖게 됩니다.

감사된 개체에 대한 전체 경로를 결정합니다

감사 레코드에 대한 "<ObjectName>" 태그에 인쇄된 객체 경로에는 볼륨의 이름(괄호 안에 표시)과 포함하는 볼륨의 루트에서의 상대 경로가 포함됩니다. 연결 경로를 포함하여 감사된 개체의 전체 경로를 결정하려면 특정 단계를 수행해야 합니다.

단계

1. 감사 이벤트의 "<ObjectName>" 태그를 확인하여 감사된 개체에 대한 볼륨 이름 및 상대 경로를 확인합니다.

   이 예에서 볼륨 이름은 "data1"이고 파일의 상대 경로는 "/dir1/file.txt"입니다.

   '<Data Name="ObjectName">"(data1); /dir1/file.txt'</Data>'

2. 이전 단계에서 확인한 볼륨 이름을 사용하여 감사된 개체가 포함된 볼륨의 연결 경로를 결정합니다.

   이 예에서 볼륨 이름은 "data1"이고 감사 대상 객체가 포함된 볼륨의 연결 경로는 "/data/data1"입니다.

   '볼륨 표시-접합-볼륨 데이터1'

```
                                Junction                     Junction
Vserver   Volume       Language Active    Junction Path     Path Source
--------- ------------ -------- --------  ----------------- -----------
vs1       data1        en_US.UTF-8
                                true      /data/data1       RW_volume
```

3. 볼륨의 접합 경로에 "<ObjectName>" 태그에 있는 상대 경로를 추가하여 감사된 개체의 전체 경로를 확인합니다.

   이 예에서 볼륨의 접합 경로는 다음과 같습니다.

   '/data/data1/dir1/file.text'

Symlink 및 하드 링크를 감사할 때의 고려 사항

symlink 및 hard link를 감사할 때는 몇 가지 고려 사항을 염두에 두어야 합니다.

감사 레코드에는 "ObjectName" 태그에서 식별되는 감사 객체의 경로를 비롯하여 감사 중인 객체에 대한 정보가

포함되어 있습니다. symlink와 hard link의 path가 ObjectName 태그에 기록되는 방식을 알고 있어야 합니다.

Symlink

Symlink는 대상 오브젝트의 위치에 대한 포인터가 포함된 별도의 inode가 있는 파일이며, 대상이라고 합니다. symlink를 통해 개체에 액세스할 때 ONTAP는 자동으로 symlink를 해석하고 볼륨의 대상 개체에 대한 실제 정규 프로토콜 무관 경로를 따릅니다.

다음 예제 출력에는 둘 다 target.txt라는 파일을 가리키는 두 개의 symlink가 있습니다. 심볼 링크 중 하나는 상대 symlink로, 다른 하나는 절대 symlink입니다. symlink 중 하나가 감사되는 경우 audit event의 ObjectName 태그에 "target.txt" 파일의 경로가 포함됩니다.

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

하드 링크

하드 링크는 파일 시스템의 기존 파일과 이름을 연결하는 디렉토리 항목입니다. 하드 링크는 원본 파일의 inode 위치를 가리킵니다. ONTAP에서 symlink를 해석하는 방법과 마찬가지로 ONTAP는 하드 링크를 해석하고 볼륨의 대상 개체에 대한 실제 정규 경로를 따릅니다. 하드 링크 개체에 대한 액세스가 감사되면 감사 이벤트는 하드 링크 경로가 아닌 ObjectName 태그에 이 절대 정규 경로를 기록합니다.

대체 **NTFS** 데이터 스트림을 감사할 때의 고려 사항

NTFS 대체 데이터 스트림을 사용하여 파일을 감사할 때 고려해야 할 몇 가지 사항이 있습니다.

감사대상 개체의 위치는 이벤트 레코드에 ObjectName 태그(경로)와 HandleID 태그(핸들)라는 두 개의 태그를 사용하여 기록됩니다. 기록되는 스트림 요청을 제대로 식별하려면 NTFS 대체 데이터 스트림에 대한 다음 필드의 ONTAP 레코드를 알고 있어야 합니다.

- evtx ID: 4656 이벤트(감사 이벤트 열기 및 만들기)
  - 대체 데이터 스트림의 경로는 ObjectName 태그에 기록됩니다.
  - 대체 데이터 스트림의 핸들은 HandleID 태그에 기록됩니다.
- evtx ID: 4663 이벤트(읽기, 쓰기, GetAttr 등과 같은 기타 모든 감사 이벤트)
  - 대체 데이터 스트림이 아닌 기본 파일의 경로는 ObjectName 태그에 기록됩니다.
  - 대체 데이터 스트림의 핸들은 HandleID 태그에 기록됩니다.

예

다음 예제에서는 "HandleID" 태그를 사용하여 대체 데이터 스트림에 대한 evtx ID: 4663 이벤트를 식별하는 방법을 보여 줍니다. READ AUDIT 이벤트에 기록된 ObjectName 태그(경로)가 기본 파일 경로에 있더라도 HandleID 태그를 사용하여 대체 데이터 스트림에 대한 감사 레코드로 이벤트를 식별할 수 있습니다.

스트림 파일 이름은 base_file_name:stream_name 형식으로 지정됩니다. 이 예제에서 dIR1 디렉토리에는 다음

경로를 가진 대체 데이터 스트림이 있는 기본 파일이 포함되어 있습니다.

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

> 다음 이벤트 예제의 출력은 표시된 대로 잘립니다. 출력에 해당 이벤트에 사용할 수 있는 출력 태그가 모두 표시되지 않습니다.

evtx ID 4656(열린 감사 이벤트)의 경우 대체 데이터 스트림에 대한 감사 레코드 출력은 "ObjectName" 태그에 대체 데이터 스트림 이름을 기록합니다.

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

evtx ID 4663(감사 이벤트 읽기)의 경우 동일한 대체 데이터 스트림에 대한 감사 레코드 출력은 "ObjectName" 태그에 기본 파일 이름을 기록합니다. 그러나 "HandleID" 태그의 핸들은 대체 데이터 스트림의 핸들로, 이 이벤트를 대체 데이터 스트림과 연관시키는 데 사용할 수 있습니다.

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

감사할 수 있는 **NFS** 파일 및 디렉토리 액세스 이벤트입니다

ONTAP는 특정 NFS 파일 및 디렉토리 액세스 이벤트를 감사할 수 있습니다. 감사할 수 있는 액세스 이벤트를 알면 변환된 감사 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

다음 NFS 파일 및 디렉토리 액세스 이벤트를 감사할 수 있습니다.

- 읽기
- 개방형
- 를 닫습니다
- readdir
- 쓰기
- SetAttr
- 생성
- 링크
- 운영
- 제거
- GetAttr
- 확인합니다
- nVerify(확인)
- 이름 바꾸기

NFS 이름 바꾸기 이벤트를 안정적으로 감사하려면 디렉터리 권한이 충분한 경우 파일 권한이 이름 바꾸기 작업에 대해 검사되지 않으므로 파일 대신 디렉터리에 감사 ACE를 설정해야 합니다.

감사 구성을 계획합니다

SVM(스토리지 가상 시스템)에 대한 감사를 구성하기 전에 사용 가능한 구성 옵션을 파악하고 각 옵션에 설정할 값을 계획해야 합니다. 이 정보는 비즈니스 요구 사항에 맞는 감사 구성을 구성하는 데 도움이 됩니다.

모든 감사 구성에 공통적으로 적용되는 특정 구성 매개 변수가 있습니다.

또한 통합 및 변환된 감사 로그를 회전할 때 사용할 메서드를 지정하는 데 사용할 수 있는 특정 매개 변수가 있습니다. 감사를 구성할 때 다음 세 가지 방법 중 하나를 지정할 수 있습니다.

- 로그 크기에 따라 로그를 회전합니다

  로그를 회전시키는 데 사용되는 기본 방법입니다.

- 일정에 따라 로그를 회전합니다
- 로그 크기 및 일정에 따라 로그 회전(먼저 발생하는 이벤트)

로그 회전 방법 중 하나 이상이 항상 설정되어야 합니다.

모든 감사 구성에 공통으로 사용되는 매개 변수입니다

감사 구성을 만들 때 지정해야 하는 필수 매개 변수는 두 가지입니다. 다음 세 가지 옵션 매개 변수도 지정할 수 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다	포함	당신의 가치
_SVM 이름 _ 감사 구성을 생성할 SVM의 이름입니다. SVM이 이미 존재해야 합니다.	'-vserver''vserver_name'	예	예	

_로그 대상 경로 _ 변환된 감사 로그가 저장되는 디렉토리, 일반적으로 전용 볼륨 또는 qtree를 지정합니다. 경로는 SVM 네임스페이스에 이미 존재해야 합니다. 경로는 최대 864자까지 가능하며 읽기-쓰기 권한이 있어야 합니다. 경로가 유효하지 않으면 감사 구성 명령이 실패합니다. SVM이 SVM 재해 복구 소스인 경우 로그 타겟 경로가 루트 볼륨에 있을 수 없습니다. 루트 볼륨 컨텐츠가 재해 복구 대상에 복제되지 않기 때문입니다. FlexCache 볼륨은 로그 대상(ONTAP 9.7 이상)으로 사용할 수 없습니다.	목적지 텍스트	예	예	

_ 감사할 이벤트의 범주 _ 감사할 이벤트의 범주를 지정합니다. 다음 이벤트 범주를 감사할 수 있습니다. • 파일 액세스 이벤트(SMB 및 NFSv4 모두) • SMB 로그온 및 로그오프 이벤트 • 중앙 액세스 정책 스테이징 이벤트입니다 중앙 액세스 정책 스테이징 이벤트는 Windows 2012 Active Directory 도메인부터 사용할 수 있습니다. • 파일 공유 범주 이벤트입니다 • 정책 변경 이벤트를 감사합니다 • 로컬 사용자 계정 관리 이벤트입니다 • 보안 그룹 관리 이벤트입니다 • 인증 정책 변경 이벤트입니다 기본값은 파일 액세스 및 SMB 로그온 및 로그오프 이벤트를 감사하는 것입니다. • 참고: * "cap-staging"을 이벤트 범주로 지정하려면 SVM에 SMB 서버가 있어야 합니다. SMB 서버에서 동적 액세스 제어를 사용하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만, 동적 액세스 제어를 설정한 경우에만 중앙 액세스 정책 스테이징 이벤트가 생성됩니다. 동적 액세스 제어는 SMB 서버 옵션을 통해 활성화됩니다. 기본적으로 활성화되어 있지 않습니다.	'- events'{'file-ops'	'cifs-logon-logoff'	'cap-staging'	'file-share'
'audit-policy-change'	'user-account'	'security-group'	'authorization-policy-change'	아니요

		_로그 파일 출력 형식 _ 감사 로그의 출력 형식을 결정합니다. 출력 형식은 ONTAP 관련 'XML' 또는 Microsoft Windows 'evtx' 로그 형식일 수 있습니다. 기본적으로 출력 형식은 evtx입니다.	'-format '{'xml'	'evtx'}

아니요			_ 로그 파일 회전 제한 _ 가장 오래된 로그 파일을 회전하기 전에 유지할 감사 로그 파일 수를 결정합니다. 예를 들어 5를 입력하면 마지막 5개의 로그 파일이 유지됩니다. 0 값은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.	회전한계 정수

감사 이벤트 로그를 회전할 시기를 결정하는 데 사용되는 매개 변수입니다

- 로그 크기에 따라 로그를 회전합니다 *

기본값은 크기에 따라 감사 로그를 회전하는 것입니다.

- 기본 로그 크기는 100MB입니다
- 기본 로그 회전 방법과 기본 로그 크기를 사용하려면 로그 회전을 위한 특정 매개 변수를 구성할 필요가 없습니다.
- 로그 크기만을 기준으로 감사 로그를 회전하려면 다음 명령을 사용하여 '-rotate-schedule-minute' 매개 변수를 'vserver audit modify -vs0 -destination/-rotate-schedule -minute-'로 설정하십시오

기본 로그 크기를 사용하지 않으려면 '-rotate-size' 매개 변수를 구성하여 사용자 지정 로그 크기를 지정할 수 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다	포함	당신의 가치

_로그 파일 크기 제한 _ 감사 로그 파일 크기 제한을 결정합니다.	'-rotate-size'{'integer'[KB	MB	GB	TB

- 일정에 따라 로그를 회전합니다 *

일정에 따라 감사 로그를 회전하도록 선택한 경우 시간 기반 회전 매개 변수를 조합하여 로그 회전을 예약할 수 있습니다.

- 시간 기반 회전을 사용하는 경우 '-rotate-schedule-minute' 매개변수는 필수입니다.
- 다른 모든 시간 기반 회전 매개변수는 옵션입니다.
- 회전 일정은 모든 시간 관련 값을 사용하여 계산됩니다.

  예를 들어, '-rotate-schedule-minute' 매개 변수만 지정하면 감사 로그 파일은 모든 연도의 모든 월에 지정된 모든 요일에 지정된 분을 기준으로 회전합니다.

- 시간 기반 회전 매개 변수(예: '-rotate-schedule-month' 및 '-rotate-schedule-minutes')를 하나 또는 두 개만 지정하는 경우 모든 시간 동안 모든 요일에 지정한 분 값을 기준으로 로그 파일이 회전되며 지정된 개월 동안에만 회전됩니다.

  예를 들어 월요일, 수요일 및 토요일은 오전 10시 30분에 월, 3월, 8월 중 감사 로그를 회전하도록 지정할 수 있습니다

- '-rotate-schedule-dayOfWeek' 및 '-rotate-schedule-day' 값을 모두 지정하면 독립적으로 간주됩니다.

  예를 들어, `-rotate-schedule-dayOfWeek'를 금요일로 지정하고 '-rotate-schedule-day'를 13일로 지정하면 13일에 금요일이 아니라 지정한 달의 13일에 감사 로그가 회전합니다.

- 일정에 따라 감사 로그를 회전하려면 다음 명령을 사용하여 '-rotate-size' 매개 변수를 unset한다. 'vserver audit modify -vs0 -destination/-rotate -size-

다음 사용 가능한 감사 매개 변수 목록을 사용하여 감사 이벤트 로그 순환에 대한 일정을 구성하는 데 사용할 값을 결정할 수 있습니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다	포함	당신의 가치
_로그 순환 스케줄: 월 _ 감사 로그 순환에 대한 월별 일정을 결정합니다. 유효한 값은 '1월'과 '모두'를 통해 '1월'입니다. 예를 들어 월 1월, 3월 및 8월 동안 감사 로그를 회전하도록 지정할 수 있습니다.	'-rotate-schedule-month' chron_month'입니다	아니요		

_Log 순환 스케줄: 요일 _ 감사 로그 회전에 대한 일별(요일) 일정을 결정합니다. 유효한 값은 '어타데이', '올데이'입니다. 예를 들어 감사 로그를 화요일과 금요일 또는 모든 요일에 회전하도록 지정할 수 있습니다.	'-rotate-schedule-dayOfWeek"chron_DayOfWeek'	아니요		
_ 로그 순환 스케줄: 일 _ 감사 로그 회전에 대한 월 일정 날짜를 결정합니다. 유효한 값은 1부터 31까지입니다. 예를 들어 감사 로그가 한 달의 10일과 20일 또는 한 달의 모든 일에 회전되도록 지정할 수 있습니다.	'-rotate-schedule-day"chron_dayofmonth'	아니요		
_ 로그 순환 스케줄: 시간 _ 감사 로그를 회전하기 위한 시간별 스케줄을 결정합니다. 유효한 값의 범위는 0(자정)에서 23(오후 11:00)까지입니다. All을 지정하면 감사 로그가 1시간마다 회전합니다. 예를 들어 감사 로그를 6(오전 6) 및 18(오후 6:00)에 회전하도록 지정할 수 있습니다.	'-rotate-schedule-hour"chron_hour'	아니요		
_ 로그 회전 스케줄: 분 _ 감사 로그를 회전하기 위한 분 일정을 결정합니다. 유효한 값의 범위는 0에서 59까지입니다. 예를 들어 30분에 감사 로그를 회전하도록 지정할 수 있습니다.	'-rotate-schedule-minute"chron_minute'	예, 스케줄 기반 로그 회전을 구성하는 경우, 그렇지 않으면 아니요		

- 로그 크기 및 일정에 따라 로그 회전 *

'-rotate-size' 매개변수와 시간 기반 회전 매개변수를 조합하여 로그 크기와 일정에 따라 로그 파일을 회전하도록 선택할 수 있습니다. 예를 들어, '-rotate-size'를 10MB로 설정하고 '-rotate-schedule-minute'를 15로 설정하면 로그 파일 크기가 10MB에 도달하거나 매 시간 15분(둘 중 먼저 발생하는 이벤트)에 도달할 때 로그 파일이 회전합니다.

SVM에 파일 및 디렉토리 감사 구성을 생성합니다

감사 구성을 만듭니다

SVM(Storage Virtual Machine)에서 파일 및 디렉토리 감사 구성을 생성하는 작업에는 사용 가능한 구성 옵션 이해, 구성 계획 수립, 구성 구성 및 활성화 등이 포함됩니다. 그런 다음 감사 구성에 대한 정보를 표시하여 결과 구성이 원하는 구성인지 확인할 수 있습니다.

파일 및 디렉토리 이벤트 감사를 시작하려면 먼저 SVM(스토리지 가상 머신)에 감사 구성을 생성해야 합니다.

시작하기 전에

중앙 액세스 정책 스테이징에 대한 감사 구성을 생성하려는 경우 SVM에 SMB 서버가 있어야 합니다.

- SMB 서버에서 동적 액세스 제어를 사용하지 않고 감사 구성에서 중앙 액세스 정책 스테이징을 설정할 수 있지만, 동적 액세스 제어를 설정한 경우에만 중앙 액세스 정책 스테이징 이벤트가 생성됩니다.

  동적 액세스 제어는 SMB 서버 옵션을 통해 활성화됩니다. 기본적으로 활성화되어 있지 않습니다.

- 필드, 중복 항목 및 존재하지 않는 항목에 대한 잘못된 입력 등 명령에서 필드의 인수가 잘못된 경우 감사 단계 전에 명령이 실패합니다.

  이러한 실패는 감사 기록을 생성하지 않습니다.

이 작업에 대해

SVM이 SVM 재해 복구 소스인 경우 타겟 경로가 루트 볼륨에 있을 수 없습니다.

단계

1. 계획 워크시트의 정보를 사용하여 감사 구성을 만들어 로그 크기 또는 일정에 따라 감사 로그를 회전합니다.

감사 로그를 회전하려면…	입력…
로그 크기	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
일정	``vserver audit create-vserver_name-destination path-events[{file-ops
cifs-logon-logoff	cap-staging}][-format{xml

예

다음 예제에서는 크기 기반 회전을 사용하여 파일 작업 및 SMB 로그온 및 로그오프 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그 형식은 evtx(기본값)입니다. 로그는 '/audit_log' 디렉토리에 저장됩니다. 로그 파일 크기 제한은 200MB입니다. 로그 크기는 200MB에 도달하면 회전됩니다.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

다음 예에서는 크기 기반 회전을 사용하여 파일 작업 및 SMB 로그온 및 로그오프 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그 형식은 입니다 `EVTX` (기본값). 로그는 에 저장됩니다 `/cifs_event_logs` 디렉토리. 로그 파일 크기 제한은 입니다 `100 MB` (기본값), 로그 회전 제한은 입니다 `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

다음 예에서는 파일 작업, CIFS 로그온 및 로그오프 이벤트 및 시간 기반 회전을 사용하여 중앙 액세스 정책 스테이징 이벤트를 감사하는 감사 구성을 생성합니다. 로그 형식은 evtx(기본값)입니다. 감사 로그는 매월 오후 12시 30분에 순환됩니다 일주일 내내. 로그 회전 제한은 "5"입니다.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

관련 정보

- "SVM에 대한 감사를 설정합니다"
- "감사 구성을 확인합니다"

SVM에 대한 감사를 설정합니다

감사 구성 설정을 마쳤으면 SVM(스토리지 가상 머신)에 대한 감사를 활성화해야 합니다.

시작하기 전에

SVM 감사 구성이 이미 존재해야 합니다.

이 작업에 대해

SVM 재해 복구 ID 폐기 구성이 SnapMirror 초기화가 완료된 후 먼저 시작되고 SVM에 감사 구성이 있으면 ONTAP에서 감사 구성을 자동으로 비활성화합니다. 스테이징 볼륨이 가득 차는 것을 방지하기 위해 읽기 전용 SVM에서 감사가 비활성화됩니다. SnapMirror 관계가 부러지고 SVM이 읽기-쓰기 상태가 된 후에만 감사를 활성화할 수 있습니다.

단계

1. SVM에 대한 감사 활성화:

   'vserver audit enable - vserver vserver_name'

'vserver audit enable - vserver vs1'

관련 정보

- "감사 구성을 만듭니다"
- "감사 구성을 확인합니다"

감사 구성을 확인합니다

감사 구성을 완료한 후에는 감사가 올바르게 구성되어 있고 활성화되어 있는지 확인해야 합니다.

단계

1. 감사 구성을 확인합니다.

   'vserver audit show-instance-vserver vserver_name'

   다음 명령은 SVM(Storage Virtual Machine) VS1 에 대한 모든 감사 구성 정보를 목록으로 표시합니다.

   'vserver audit show-instance-vserver vs1'

```
                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops
                          Log Format: evtx
                  Log File Size Limit: 200MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
            Log Files Rotation Limit: 0
```

관련 정보

- "감사 구성을 만듭니다"
- "SVM에 대한 감사를 설정합니다"

파일 및 폴더 감사 정책을 구성합니다

파일 및 폴더 감사 정책을 구성합니다

파일 및 폴더 액세스 이벤트에 대한 감사를 구현하는 과정은 두 단계로 구성됩니다. 먼저 SVM(스토리지 가상 시스템)에서 감사 구성을 생성하고 활성화해야 합니다. 둘째, 모니터링할 파일과 폴더에 대해 감사 정책을 구성해야 합니다. 성공한 액세스 시도와 실패한 액세스 시도를

모두 모니터링하도록 감사 정책을 구성할 수 있습니다.

SMB 및 NFS 감사 정책을 모두 구성할 수 있습니다. SMB 및 NFS 감사 정책은 다양한 구성 요구사항 및 감사 기능을 갖습니다.

적절한 감사 정책이 구성된 경우 ONTAP는 SMB 또는 NFS 서버가 실행 중인 경우에만 감사 정책에 지정된 SMB 및 NFS 액세스 이벤트를 모니터링합니다.

NTFS 보안 스타일 파일 및 디렉터리에 대한 감사 정책을 구성합니다

파일 및 디렉터리 작업을 감사하려면 감사 정보를 수집할 파일 및 디렉터리에 대한 감사 정책을 구성해야 합니다. 감사 구성을 설정 및 활성화하는 것 외에 다른 기능도 있습니다. Windows 보안 탭을 사용하거나 ONTAP CLI를 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

Windows 보안 탭을 사용하여 **NTFS** 감사 정책 구성

Windows 속성 창의 * Windows 보안 * 탭을 사용하여 파일 및 디렉터리에 대한 NTFS 감사 정책을 구성할 수 있습니다. 이는 Windows 클라이언트에 있는 데이터에 대한 감사 정책을 구성할 때 사용되는 것과 동일한 방법으로, 익숙한 GUI 인터페이스를 사용할 수 있습니다.

시작하기 전에

감사는 SACL(시스템 액세스 제어 목록)을 적용하는 데이터가 포함된 SVM(스토리지 가상 시스템)에서 구성해야 합니다.

이 작업에 대해

NTFS 감사 정책 구성은 NTFS 보안 설명자와 연결된 NTFS SACL에 항목을 추가하여 수행됩니다. 그런 다음 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다. 이러한 작업은 Windows GUI에서 자동으로 처리됩니다. 보안 설명자는 파일 및 폴더 액세스 권한을 적용하기 위한 DACL(임의 액세스 제어 목록), 파일 및 폴더 감사를 위한 SACL 또는 SACL 및 DACL을 모두 포함할 수 있습니다.

Windows 보안 탭을 사용하여 NTFS 감사 정책을 설정하려면 Windows 호스트에서 다음 단계를 수행하십시오.

단계

1. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
2. 네트워크 드라이브 매핑 * 상자를 완료합니다.

   a. 드라이브 * 문자를 선택합니다.

   b. 폴더 * 상자에 감사할 데이터와 공유 이름을 가지고 있는 공유가 포함된 SMB 서버 이름을 입력합니다.

      SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

      SMB 서버 이름이 "smb_server"이고 공유 이름이 "hay1"인 경우 \\smb_server\share1"을 입력해야 합니다.

   c. 마침 * 을 클릭합니다.

   선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

3. 감사 액세스를 설정할 파일 또는 디렉토리를 선택합니다.
4. 파일 또는 디렉터리를 마우스 오른쪽 단추로 클릭한 다음 * 속성 * 을 선택합니다.

5. 보안 * 탭을 선택합니다.
6. 고급 * 을 클릭합니다.
7. 감사 * 탭을 선택합니다.
8. 원하는 작업을 수행합니다.

원하는 경우	다음을 수행합니다
새 사용자 또는 그룹에 대한 감사를 설정합니다	a. 추가 * 를 클릭합니다. b. 선택할 개체 이름을 입력하십시오. 상자에 추가할 사용자 또는 그룹의 이름을 입력합니다. c. 확인 * 을 클릭합니다.
사용자 또는 그룹에서 감사를 제거합니다	a. 선택할 개체 이름을 입력하십시오. 상자에서 제거할 사용자 또는 그룹을 선택합니다. b. 제거 * 를 클릭합니다. c. 확인 * 을 클릭합니다. d. 이 절차의 나머지 부분을 건너뜁니다.
사용자 또는 그룹에 대한 감사 변경	a. 선택할 개체 이름을 입력하십시오. 상자에서 변경할 사용자 또는 그룹을 선택합니다. b. 편집 * 을 클릭합니다. c. 확인 * 을 클릭합니다.

사용자 또는 그룹에 대한 감사를 설정하거나 기존 사용자 또는 그룹에 대한 감사를 변경하는 경우 <object>에 대한 감사 항목 상자가 열립니다.

9. 적용 대상 * 상자에서 이 감사 항목을 적용할 방법을 선택합니다.

   다음 중 하나를 선택할 수 있습니다.

   - * 이 폴더, 하위 폴더 및 파일 *
   - * 이 폴더 및 하위 폴더 *
   - * 이 폴더만 *
   - * 이 폴더 및 파일 *
   - * 하위 폴더 및 파일만 *
   - * 하위 폴더만 *
   - * 파일만 * 단일 파일에 대한 감사를 설정하는 경우 * 적용 대상 * 상자가 활성화되지 않습니다. 적용 대상 * 상자 설정은 기본적으로 * 이 개체만 * 으로 설정됩니다.

   > 감사는 SVM 리소스를 사용하기 때문에 보안 요구사항을 충족하는 감사 이벤트를 제공하는 최소 수준만 선택하십시오.

10. Access* 상자에서 감사할 내용과 성공한 이벤트, 실패 이벤트 또는 둘 모두를 감사할지 여부를 선택합니다.
    - 성공한 이벤트를 감사하려면 성공 상자를 선택합니다.
    - 실패 이벤트를 감사하려면 실패 상자를 선택합니다.

      보안 요구 사항을 충족하기 위해 모니터링해야 하는 작업만 선택합니다. 이러한 감사 가능한 이벤트에 대한 자세한 내용은 Windows 설명서를 참조하십시오. 다음 이벤트를 감사할 수 있습니다.

    - * 완전 제어 *
    - * 폴더 트래버스/파일 실행 *
    - * 폴더 나열/데이터 읽기 *
    - * 읽기 속성 *
    - * 확장 속성 읽기 *
    - * 파일 생성/데이터 쓰기 *
    - * 폴더 생성/데이터 추가 *
    - * 속성 쓰기 *
    - * 확장 속성 쓰기 *
    - * 하위 폴더 및 파일 삭제 *
    - * 삭제 *
    - * 읽기 권한 *
    - * 권한 변경 *
    - * 소유권 가져오기 *
11. 감사 설정이 원본 컨테이너의 후속 파일 및 폴더에 전파되지 않도록 하려면 * 이 감사 항목을 이 컨테이너 내의 개체 및/또는 컨테이너에 적용 * 상자를 선택합니다.
12. 적용 * 을 클릭합니다.
13. 감사 항목 추가, 제거 또는 편집을 마친 후 * 확인 * 을 클릭합니다.

    object>에 대한 감사 항목 상자가 닫힙니다.

14. 감사 * 상자에서 이 폴더의 상속 설정을 선택합니다.

    보안 요구 사항을 충족하는 감사 이벤트를 제공하는 최소 수준만 선택합니다. 다음 중 하나를 선택할 수 있습니다.

    - 이 개체의 부모 상자에서 상속 가능한 감사 항목 포함 을 선택합니다.
    - 모든 하위 항목의 기존 상속 가능한 감사 항목을 이 개체의 상속 가능한 감사 항목으로 바꾸기 상자를 선택합니다.
    - 두 상자를 모두 선택합니다.
    - 어느 상자도 선택하지 않습니다. 단일 파일에 대해 SACL을 설정하는 경우 모든 하위 항목에 대해 상속 가능한 기존 감사 항목을 이 개체의 상속 가능한 감사 항목으로 바꾸기 상자는 감사 상자에 없습니다.
15. 확인 * 을 클릭합니다.

    감사 상자가 닫힙니다.

ONTAP CLI를 사용하여 **NTFS** 감사 정책을 구성합니다

ONTAP CLI를 사용하여 파일 및 폴더에 대한 감사 정책을 구성할 수 있습니다. 따라서 Windows 클라이언트에서 SMB 공유를 사용하여 데이터에 연결할 필요 없이 NTFS 감사 정책을 구성할 수 있습니다.

'vserver security file-directory' 명령 제품군을 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

CLI를 사용하는 NTFS SACL만 구성할 수 있습니다. 이 ONTAP 명령 제품군에는 NFSv4 SACL 구성이 지원되지 않습니다. 이러한 명령을 사용하여 파일과 폴더에 NTFS SACL을 구성 및 추가하는 방법에 대한 자세한 내용은 man 페이지를 참조하십시오.

UNIX 보안 스타일 파일 및 디렉토리에 대한 감사를 구성합니다

NFSv4.x ACL에 감사 ACE를 추가하여 UNIX 보안 스타일 파일 및 디렉토리에 대한 감사를 구성합니다. 이를 통해 보안을 위해 특정 NFS 파일 및 디렉토리 액세스 이벤트를 모니터링할 수 있습니다.

이 작업에 대해

NFSv4.x의 경우 임의 ACE와 시스템 ACE가 모두 동일한 ACL에 저장됩니다. 이 파일은 별도의 DACL 및 SACL에 저장되지 않습니다. 따라서 기존 ACL을 덮어쓰거나 잃지 않도록 기존 ACL에 감사 ACE를 추가할 때는 주의해야 합니다. 감사 ACE를 기존 ACL에 추가하는 순서는 중요하지 않습니다.

단계

1. nfs4_getfacl 또는 이와 동등한 명령을 사용하여 파일 또는 디렉토리의 기존 ACL을 검색합니다.

   ACL을 조작하는 방법에 대한 자세한 내용은 NFS 클라이언트의 man 페이지를 참조하십시오.

2. 원하는 감사 ACE를 추가합니다.
3. nfs4_setfacl 또는 이와 동등한 명령을 사용하여 파일 또는 디렉토리에 업데이트된 ACL을 적용합니다.

파일 및 디렉토리에 적용된 감사 정책에 대한 정보를 표시합니다

Windows 보안 탭을 사용하여 감사 정책에 대한 정보를 표시합니다

Windows 속성 창의 보안 탭을 사용하여 파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시할 수 있습니다. 이는 Windows 서버에 있는 데이터에 사용되는 것과 동일한 방법으로, 고객이 익숙한 GUI 인터페이스를 사용할 수 있습니다.

이 작업에 대해

파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시하면 지정된 파일 및 폴더에 적절한 SACL(시스템 액세스 제어 목록)이 설정되어 있는지 확인할 수 있습니다.

NTFS 파일 및 폴더에 적용된 SACL에 대한 정보를 표시하려면 Windows 호스트에서 다음 단계를 수행하십시오.

단계

1. Windows 탐색기의 * Tools * 메뉴에서 * Map network drive * 를 선택합니다.
2. 네트워크 드라이브 연결 * 대화 상자를 완료합니다.

a. 드라이브 * 문자를 선택합니다.

b. 폴더 * 상자에 감사할 데이터와 공유 이름을 둘 다 포함하는 공유가 포함된 SVM(스토리지 가상 시스템)의 IP 주소 또는 SMB 서버 이름을 입력합니다.

   SMB 서버 이름이 "smb_server"이고 공유 이름이 "hay1"인 경우 \\smb_server\share1"을 입력해야 합니다.

   SMB 서버 이름 대신 SMB 서버에 대한 데이터 인터페이스의 IP 주소를 지정할 수 있습니다.

c. 마침 * 을 클릭합니다.

선택한 드라이브가 마운트되고 공유 내에 포함된 파일 및 폴더를 표시하는 Windows 탐색기 창이 준비됩니다.

3. 감사 정보를 표시할 파일 또는 디렉터리를 선택합니다.
4. 파일 또는 디렉토리를 마우스 오른쪽 버튼으로 클릭하고 * 속성 * 을 선택합니다.
5. 보안 * 탭을 선택합니다.
6. 고급 * 을 클릭합니다.
7. 감사 * 탭을 선택합니다.
8. 계속 * 을 클릭합니다.

   감사 상자가 열립니다. 감사 항목 * 상자에는 SACL이 적용된 사용자 및 그룹의 요약이 표시됩니다.

9. 감사 항목 * 상자에서 SACL 항목을 표시할 사용자 또는 그룹을 선택합니다.
10. 편집 * 을 클릭합니다.

    object>에 대한 감사 항목이 열립니다.

11. Access* 상자에서 선택한 개체에 적용된 현재 SACL을 확인합니다.
12. 객체> * 에 대한 * 감사 항목을 닫으려면 * 취소 * 를 클릭합니다.
13. 취소 * 를 클릭하여 * 감사 * 상자를 닫습니다.

CLI를 사용하여 FlexVol 볼륨의 NTFS 감사 정책에 대한 정보를 표시합니다

FlexVol 볼륨에서 보안 스타일 및 효과적인 보안 스타일의 정의, 적용되는 권한 및 시스템 액세스 제어 목록에 대한 정보를 포함하여 NTFS 감사 정책에 대한 정보를 표시할 수 있습니다. 이 정보를 사용하여 보안 구성을 확인하거나 감사 문제를 해결할 수 있습니다.

이 작업에 대해

파일 및 디렉터리에 적용된 감사 정책에 대한 정보를 표시하면 지정된 파일 및 폴더에 적절한 SACL(시스템 액세스 제어 목록)이 설정되어 있는지 확인할 수 있습니다.

SVM(스토리지 가상 시스템)의 이름과 감사 정보를 표시할 파일 또는 폴더의 경로를 제공해야 합니다. 출력을 요약 양식 또는 상세 목록으로 표시할 수 있습니다.

- NTFS 보안 스타일 볼륨 및 qtree는 감사 정책에 NTFS SACL(시스템 액세스 제어 목록)만 사용합니다.
- NTFS 효과적인 보안이 적용된 혼합 보안 스타일 볼륨의 파일과 폴더에 NTFS 감사 정책이 적용될 수 있습니다.

혼합 보안 스타일 볼륨 및 qtree에는 모드 비트 또는 NFSv4 ACL, NTFS 파일 권한을 사용하는 일부 파일 및 디렉토리 등 UNIX 파일 권한을 사용하는 일부 파일과 디렉토리가 포함될 수 있습니다.

- 혼합 보안 형식 볼륨의 최상위 수준에는 UNIX 또는 NTFS의 효과적인 보안이 포함될 수 있으며 NTFS SACL이 포함될 수도 있고 포함되지 않을 수도 있습니다.
- 볼륨 루트 또는 qtree의 효과적인 보안 스타일이 UNIX인 경우에도 스토리지 레벨 액세스 가드 보안을 혼합 보안 스타일 볼륨 또는 qtree로 구성할 수 있으므로 Storage-Level Access Guard가 구성된 볼륨 또는 qtree 경로의 출력에는 일반 파일 및 폴더 NFSv4 SACL 및 Storage-Level Access Guard NTFS SACL이 모두 표시될 수 있습니다.
- 명령에 입력한 경로가 NTFS 유효 보안을 사용하는 데이터인 경우 해당 파일 또는 디렉토리 경로에 동적 액세스 제어가 구성되어 있으면 동적 액세스 제어 ACE에 대한 정보도 출력에 표시됩니다.
- NTFS 유효 보안이 있는 파일 및 폴더에 대한 보안 정보를 표시할 때 UNIX 관련 출력 필드에는 표시 전용 UNIX 파일 권한 정보가 포함됩니다.

  NTFS 보안 스타일 파일 및 폴더는 파일 액세스 권한을 결정할 때 NTFS 파일 권한과 Windows 사용자 및 그룹만 사용합니다.

- ACL 출력은 NTFS 또는 NFSv4 보안이 설정된 파일 및 폴더에만 표시됩니다.

  모드 비트 권한만 적용된 UNIX 보안을 사용하는 파일 및 폴더의 경우 이 필드는 비어 있습니다(NFSv4 ACL 없음).

- ACL 출력의 소유자 및 그룹 출력 필드는 NTFS 보안 설명자의 경우에만 적용됩니다.

단계

1. 파일 및 디렉터리 감사 정책 설정을 원하는 수준으로 표시합니다.

정보를 표시하려면…	다음 명령을 입력합니다…
요약 양식	'vserver security file-directory show -vserver vserver_name -path path path'
를 참조하십시오	'vserver security file-directory show -vserver vserver_name -path path path -expand-mask true'

예

다음 예에서는 SVM VS1 경로의 /Corp 경로에 대한 감사 정책 정보를 표시합니다. 경로에 NTFS 유효 보안이 있습니다. NTFS 보안 설명자는 성공 및 성공/실패 SACL 항목을 모두 포함합니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

다음 예제는 SVM VS1 경로의 /datavol1 경로에 대한 감사 정책 정보를 표시합니다. 이 경로에는 일반 파일 및 폴더 SACL과 Storage-Level Access Guard SACL이 모두 포함됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

파일 보안 및 감사 정책에 대한 정보를 표시하는 방법

와일드카드 문자(*)를 사용하여 지정된 경로 또는 루트 볼륨 아래에 있는 모든 파일 및 디렉토리의 파일 보안 및 감사 정책에 대한 정보를 표시할 수 있습니다.

와일드카드 문자(*)는 모든 파일 및 디렉터리의 정보를 표시할 아래의 지정된 디렉터리 경로의 마지막 하위 구성 요소로 사용할 수 있습니다.

"*"로 명명된 특정 파일 또는 디렉토리의 정보를 표시하려면 큰따옴표("") 안에 전체 경로를 제공해야 합니다.

예

와일드카드 문자를 사용하여 다음 명령을 실행하면 SVM VS1 경로의 '/1/' 아래에 있는 모든 파일 및 디렉토리에 대한 정보가 표시됩니다.

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
                Unix User Id: 0
               Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
                Unix User Id: 0
               Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

다음 명령을 실행하면 SVM VS1 의 path '/vol1/a' 아래에 " * "로 명명된 파일의 정보가 표시됩니다. 경로는 큰따옴표(" ")로 묶습니다.

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                  Vserver: vs1
                File Path: "/vol1/a/*"
           Security Style: mixed
          Effective Style: unix
           DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
             Unix User Id: 1002
            Unix Group Id: 65533
           Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

감사할 수 있는 **CLI** 변경 이벤트입니다

감사할 수 있는 **CLI** 변경 이벤트 개요

ONTAP는 특정 SMB 공유 이벤트, 특정 감사 정책 이벤트, 특정 로컬 보안 그룹 이벤트, 로컬 사용자 그룹 이벤트 및 인증 정책 이벤트를 비롯한 특정 CLI 변경 이벤트를 감사할 수 있습니다. 감사할 수 있는 변경 이벤트를 이해하면 이벤트 로그의 결과를 해석할 때 도움이 됩니다.

감사 로그를 수동으로 회전하고, 감사를 설정 또는 비활성화하고, 변경 이벤트 감사 정보를 표시하고, 변경 이벤트 감사 및 감사 변경 이벤트를 수정하여, CLI 변경 이벤트를 감사하여 스토리지 가상 시스템(SVM) 감사 CLI 변경 이벤트를 관리할 수 있습니다.

관리자 권한으로 SMB-share, 로컬 사용자 그룹, 로컬 보안 그룹, 인증 정책 및 감사 정책 이벤트와 관련된 구성을 변경하기 위해 명령을 실행하는 경우 레코드가 생성되고 해당 이벤트가 감사됩니다.

감사 범주	이벤트	이벤트 ID입니다	이 명령 실행…
Mhost 감사	정책 변경	[4719] 감사 구성이 변경되었습니다	'vserver audit disable

enable	modify'	파일 공유	[5142] 네트워크 공유가 추가되었습니다
'vserver cifs share create	[5143] 네트워크 공유가 수정되었습니다	'vserver cifs share modify"vserver cifs share create	modify
delete"vserver cifs share add	remove'	[5144] 네트워크 공유가 삭제되었습니다	'vserver cifs share delete
감사	사용자 계정	[4720] 로컬 사용자가 생성되었습니다	'vserver cifs users-and-groups local-user create"vserver services name-service unix-user create'를 참조하십시오
[4722] 로컬 사용자가 활성화되었습니다	'vserver cifs users-and-groups local-user create	modify'를 참조하십시오	[4724] 로컬 사용자 암호 재설정
'vserver cifs users-and-groups local-user set-password	[4725] 로컬 사용자가 비활성화되었습니다	'vserver cifs users-and-groups local-user create	modify'를 참조하십시오
[4726] 로컬 사용자가 삭제되었습니다	'vserver cifs users-and-groups local-user delete"vserver services name-service unix-user delete"를 선택합니다	[4738] 로컬 사용자 변경	'vserver cifs users-and-groups local-user modify"vserver services name-service unix-user modify"를 선택합니다
[4781] 로컬 사용자 이름 바꾸기	'vserver cifs users-and-groups local-user rename'을 선택합니다	보안 그룹	[4731] 로컬 보안 그룹이 생성되었습니다
'vserver cifs users-and-groups local-group create"vserver services name-service unix-group create'를 참조하십시오	[4734] 로컬 보안 그룹이 삭제되었습니다	SVM CIFS 사용자-그룹 로컬-그룹 삭제 SVM 서비스 이름-서비스 UNIX-그룹 삭제	[4735] 로컬 보안 그룹이 수정되었습니다
vserver cifs users-and-groups local-group rename	modify ``vserver services name-service unix-group modify''라는 이름의 가상 서버 사용자 및 그룹 로컬 그룹 이름 변경	[4732] 사용자가 로컬 그룹에 추가되었습니다	가상 CIFS 사용자 및 그룹 로컬 그룹 추가 멤버 가상 서버 서비스 이름 서비스 unix 그룹 추가 사용자
[4733] 사용자가 로컬 그룹에서 제거되었습니다	SVM CIFS 사용자-그룹 local-group remove-멤버들 vserver services name-service unix-group deluser	authorization-policy-change를 참조하십시오	[4704] 사용자 권한이 할당되었습니다

'vserver cifs users-and-groups Privilege add-privilege'	[4705] 사용자 권한이 제거되었습니다	'vserver cifs users-and-groups Privilege remove-Privilege	reset-Privilege

파일 공유 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 파일 공유 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다. 파일 공유 이벤트는 SMB 네트워크 공유가 'vserver cifs share' 관련 명령을 사용하여 수정될 때 생성됩니다.

이벤트 ID 5142, 5143 및 5144와 파일 공유 이벤트는 SVM에 대해 SMB 네트워크 공유를 추가, 수정 또는 삭제할 때 생성됩니다. SMB 네트워크 공유 구성은 'CIFS share access control create | modify | delete' 명령을 사용하여 수정합니다.

다음 예에서는 'audit_dest'라는 공유 객체가 생성될 때 ID 5143이 생성된 파일 공유 이벤트를 표시합니다.

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Audit-Policy-Change 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 감사 정책 변경 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다. Audit-policy-change 이벤트는 'vserver audit' 관련 명령어를 이용하여 Audit 정책을 수정할 때 발생한다.

이벤트 ID 4719를 사용하는 감사 정책 변경 이벤트는 감사 정책이 사용 안 함, 사용 또는 수정될 때마다 생성되며 사용자가 트랙을 커버하기 위해 감사를 비활성화하려고 시도하는 시점을 식별하는 데 도움이 됩니다. 기본적으로 구성되어 있으며 비활성화하려면 진단 권한이 필요합니다.

다음 예제에서는 감사가 비활성화된 경우 ID 4719가 생성된 감사 정책 변경 이벤트를 표시합니다.

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

사용자 계정 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 사용자 계정 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4720, 4722, 4724, 4725, 4726, 4738 및 4781은 로컬 SMB 또는 NFS 사용자가 시스템에서 생성 또는 삭제되거나, 로컬 사용자 계정이 활성화, 비활성화 또는 수정되고, 로컬 SMB 사용자 암호가 재설정 또는 변경될 때 생성됩니다. 사용자 계정 이벤트는 사용자 계정이 'vserver cifs users-and-groups_<local user>_' 및 'vserver services name-service_<unix user>_' 명령을 사용하여 수정될 때 생성됩니다.

다음 예에서는 로컬 SMB 사용자가 생성될 때 ID 4720이 생성된 사용자 계정 이벤트를 표시합니다.

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

다음 예제에서는 앞의 예제에서 만든 로컬 SMB 사용자의 이름이 변경된 경우 ID 4781이 생성된 사용자 계정 이벤트를 표시합니다.

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

보안 그룹 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 보안 그룹 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4731, 4732, 4733, 4734 및 4735가 포함된 보안 그룹 이벤트는 로컬 SMB 또는 NFS 그룹이 시스템에서 생성 또는 삭제되고 로컬 사용자가 그룹에서 추가 또는 제거될 때 생성됩니다. 사용자 계정이 'vserver cifs users-and-groups_<local-group>_' 및 'vserver services name-service_<unix-group>_' 명령을 사용하여 수정될 때 security-group-events가 생성됩니다.

다음 예에서는 로컬 UNIX 보안 그룹이 생성될 때 ID 4731이 생성된 보안 그룹 이벤트를 표시합니다.

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

authorization-policy-change 이벤트를 관리합니다

SVM(스토리지 가상 시스템)에 대해 인증 정책 변경 이벤트가 구성되고 감사가 활성화된 경우 감사 이벤트가 생성됩니다.

이벤트 ID 4704 및 4705의 권한 부여 정책 변경 이벤트는 SMB 사용자 및 SMB 그룹에 대해 권한 부여 권한이 부여되거나 취소될 때마다 생성됩니다. authorization-policy-change 이벤트는 vserver cifs users-and-groups 권한 관련 명령을 사용하여 권한 부여 권한이 할당되거나 취소될 때 생성됩니다.

다음 예에서는 SMB 사용자 그룹에 대한 인증 권한이 할당된 경우 ID 4704가 생성된 인증 정책 이벤트를 표시합니다.

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

감사 구성을 관리합니다

감사 이벤트 로그를 수동으로 회전합니다

감사 이벤트 로그를 보려면 먼저 로그를 사용자가 읽을 수 있는 형식으로 변환해야 합니다. ONTAP이 로그를 자동으로 회전하기 전에 특정 SVM(스토리지 가상 시스템)의 이벤트 로그를 보려는 경우 SVM에서 감사 이벤트 로그를 수동으로 회전할 수 있습니다.

단계

1. vserver audit rotate -log 명령을 사용하여 감사 이벤트 로그를 회전합니다.

   'vserver audit rotate-log-vserver vs1'

   감사 이벤트 로그는 SVM 감사 이벤트 로그 디렉토리에 감사 구성('XML' 또는 'evtx')에 지정된 형식으로 저장되며, 적절한 애플리케이션을 사용하여 볼 수 있습니다.

SVM에서 감사를 설정 및 해제합니다

SVM(스토리지 가상 머신)에 대한 감사를 설정하거나 해제할 수 있습니다. 감사를 비활성화하여 파일 및 디렉터리 감사를 일시적으로 중지할 수 있습니다. 감사 구성이 있는 경우 언제든지 감사를 활성화할 수 있습니다.

필요한 것

SVM에 대한 감사를 활성화하려면 먼저 SVM의 감사 구성이 이미 존재해야 합니다.

"감사 구성을 만듭니다"

이 작업에 대해

감사를 사용하지 않도록 설정해도 감사 구성은 삭제되지 않습니다.

단계

1. 적절한 명령을 수행합니다.

감사를 원하는 경우...	명령 입력...
활성화됨	'vserver audit enable - vserver vserver_name'
사용 안 함	'vserver audit disable-vserver vserver_name'

2. 감사가 원하는 상태인지 확인합니다.

   'vserver audit show -vserver vserver_name'

예

다음 예에서는 SVM VS1 에 대한 감사를 설정합니다.

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

다음 예에서는 SVM VS1 에 대한 감사를 해제합니다.

```
cluster1::> vserver audit disable -vserver vs1

                                Vserver: vs1
                       Auditing state: false
                 Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                            Log Format: evtx
                   Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
           Log Rotation Schedule: Day: -
          Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 10
```

감사 구성에 대한 정보를 표시합니다

감사 구성에 대한 정보를 표시할 수 있습니다. 이 정보를 통해 각 SVM에 대해 구성이 현재 위치에서 원하는 것인지 확인할 수 있습니다. 표시된 정보를 사용하여 감사 구성이 설정되었는지 여부를 확인할 수도 있습니다.

이 작업에 대해

모든 SVM의 감사 구성에 대한 자세한 정보를 표시하거나 선택적 매개 변수를 지정하여 출력에 표시되는 정보를 사용자 지정할 수 있습니다. 선택적 매개 변수를 지정하지 않으면 다음 항목이 표시됩니다.

- 감사 구성이 적용되는 SVM 이름입니다
- 진실 허위일 수 있는 감사 상태

  감사 상태가 true이면 감사가 활성화됩니다. 감사 상태가 false이면 감사가 비활성화됩니다.

- 감사할 이벤트의 범주입니다
- 감사 로그 형식입니다
- 감사 하위 시스템이 통합 및 변환된 감사 로그를 저장하는 대상 디렉토리입니다

단계

1. vserver audit show 명령을 사용하여 감사 구성에 대한 정보를 표시합니다.

   명령 사용에 대한 자세한 내용은 man 페이지를 참조하십시오.

예

다음 예에서는 모든 SVM에 대한 감사 구성을 요약하여 표시합니다.

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

다음 예에서는 모든 SVM에 대한 모든 감사 구성 정보를 목록 형식으로 표시합니다.

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
            Log Files Rotation Limit: 0
```

감사 구성을 수정하는 명령입니다

감사 설정을 변경하려면 로그 경로 대상 및 로그 형식 수정, 감사할 이벤트 범주 수정, 로그 파일을 자동으로 저장하는 방법, 저장할 최대 로그 파일 수 지정 등 언제든지 현재 구성을 수정할 수 있습니다.

원하는 작업	이 명령 사용...
로그 대상 경로를 수정합니다	'-destination' 매개 변수를 사용하여 vserver audit modify를 수행합니다
감사할 이벤트 범주를 수정합니다	'-events' 매개 변수를 사용하여 vserver audit modify를 수행합니다 ⓘ 중앙 액세스 정책 스테이징 이벤트를 감사하려면 스토리지 가상 머신(SVM)에서 DAC(Dynamic Access Control) SMB 서버 옵션을 활성화해야 합니다.
로그 형식을 수정합니다	vserver audit modify는 -format 매개 변수를 사용합니다

내부 로그 파일 크기에 따라 자동 저장을 사용하도록 설정합니다	'-rotate-size' 파라미터를 사용한 vserver audit modify
시간 간격에 따라 자동 저장을 사용하도록 설정합니다	vserver audit modify with the '-rotate-schedule-month', '-rotate-schedule-dayOfWeek', '-rotate-schedule-day', '-rotate-schedule-hour', '-rotate-schedule-minute' 매개변수를 사용합니다
저장된 로그 파일의 최대 개수를 지정합니다	'-rotate-limit' 파라미터를 사용한 vserver audit modify

감사 구성을 삭제합니다

더 이상 SVM(스토리지 가상 시스템)의 파일 및 디렉토리 이벤트를 감사하지 않고 SVM에 대한 감사 구성을 유지하고 싶지 않으면 감사 구성을 삭제할 수 있습니다.

단계

1. 감사 구성을 사용하지 않도록 설정합니다.

   'vserver audit disable-vserver vserver_name'

   'vserver audit disable - vserver vs1'

2. 감사 구성을 삭제합니다.

   'vserver audit delete - vserver vserver_name'

   'vserver audit delete - vserver vs1'

클러스터 되돌리기의 의미를 이해합니다

클러스터를 되돌리려는 경우 클러스터에 감사 기능이 설정된 SVM(스토리지 가상 머신)이 있을 때 ONTAP에서 따르는 복원 프로세스에 대해 알고 있어야 합니다. 되돌리기 전에 특정 조치를 취해야 합니다.

SMB 로그온 및 로그오프 이벤트 및 중앙 액세스 정책 스테이징 이벤트에 대한 감사를 지원하지 않는 **ONTAP** 버전으로 되돌립니다

SMB 로그온 및 로그오프 이벤트 감사 및 중앙 액세스 정책 스테이징 이벤트는 clustered Data ONTAP 8.3에서 시작됩니다. 이러한 이벤트 유형을 지원하지 않는 ONTAP 버전으로 되돌리려고 하고 이러한 이벤트 유형을 모니터링하는 감사 구성이 있는 경우, 되돌리기 전에 감사 기능이 설정된 SVM에 대한 감사 구성을 변경해야 합니다. 파일 작업 이벤트만 감사되도록 구성을 수정해야 합니다.

감사 및 스테이징 볼륨 공간 문제를 해결합니다

스테이징 볼륨 또는 감사 이벤트 로그가 포함된 볼륨에 공간이 부족할 때 문제가 발생할 수 있습니다. 공간이 부족하면 새 감사 레코드를 생성할 수 없으므로 클라이언트가 데이터에 액세스하지 못하게 되고 액세스 요청이 실패합니다. 이러한 볼륨 공간 문제를 해결하고 해결하는

방법을 알아야 합니다.

이벤트 로그 볼륨과 관련된 공간 문제를 해결합니다

이벤트 로그 파일이 포함된 볼륨의 공간이 부족한 경우 감사 기능은 로그 레코드를 로그 파일로 변환할 수 없습니다. 이로 인해 클라이언트 액세스 장애가 발생합니다. 이벤트 로그 볼륨과 관련된 공간 문제를 해결하는 방법을 알고 있어야 합니다.

- 스토리지 가상 머신(SVM) 및 클러스터 관리자는 볼륨 및 애그리게이트의 사용 및 구성에 대한 정보를 표시하여 볼륨 공간이 부족한지 여부를 확인할 수 있습니다.
- 이벤트 로그가 포함된 볼륨에 공간이 부족하면 SVM 및 클러스터 관리자가 이벤트 로그 파일 중 일부를 제거하거나 볼륨 크기를 늘려 공간 문제를 해결할 수 있습니다.

> 이벤트 로그 볼륨이 포함된 애그리게이트는 가득 찬 경우, 볼륨의 크기를 늘리려면 애그리게이트의 크기를 늘려야 합니다. 클러스터 관리자만 집계 크기를 늘릴 수 있습니다.

- 감사 구성을 수정하여 이벤트 로그 파일의 대상 경로를 다른 볼륨의 디렉토리로 변경할 수 있습니다.

> 다음과 같은 경우 데이터 액세스가 거부됩니다.
>
> - 대상 디렉토리가 삭제됩니다.
> - 대상 디렉토리를 호스팅하는 볼륨에 대한 파일 제한이 최대 레벨에 도달합니다.

자세히 알아보기:

- "볼륨에 대한 정보를 보고 볼륨 크기를 늘리는 방법".
- "Aggregate에 대한 정보를 보고 애그리게이트를 관리하는 방법".

스테이징 볼륨과 관련된 공간 문제를 해결합니다

SVM(Storage Virtual Machine)에 대한 스테이징 파일이 포함된 볼륨 중 공간이 부족한 경우 감사를 통해 로그 레코드를 스테이징 파일에 쓸 수 없습니다. 이로 인해 클라이언트 액세스 장애가 발생합니다. 이 문제를 해결하려면 SVM에 사용된 스테이징 볼륨이 볼륨 사용에 대한 정보를 표시하여 가득 찼는지 여부를 확인해야 합니다.

통합된 이벤트 로그 파일이 포함된 볼륨에 충분한 공간이 있지만 공간 부족으로 인해 여전히 클라이언트 액세스 장애가 발생하는 경우 스테이징 볼륨의 공간이 부족할 수 있습니다. SVM 관리자는 SVM을 위한 스테이징 파일이 포함된 스테이징 볼륨의 공간이 부족한지 여부를 확인하기 위해 여러분에게 연락해야 합니다. 감사 하위 시스템은 스테이징 볼륨의 공간이 부족하여 감사 이벤트를 생성할 수 없는 경우 EMS 이벤트를 생성합니다. 장치에 남은 공간이 없습니다 라는 메시지가 표시됩니다. 스테이징 볼륨에 대한 정보는 사용자만 볼 수 있으며 SVM 관리자는 볼 수 없습니다.

모든 스테이징 볼륨 이름은 mdv_AUD_ 로 시작하고 그 스테이징 볼륨을 포함하는 애그리게이트의 UUID로 시작합니다. 다음 예에서는 클러스터 내의 데이터 SVM에 대한 파일 서비스 감사 구성을 생성할 때 자동으로 생성되는 admin SVM의 시스템 볼륨 4개를 보여 줍니다.

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

스테이징 볼륨에 공간이 부족하면 볼륨 크기를 늘려 공간 문제를 해결할 수 있습니다.

> 스테이징 볼륨이 포함된 aggregate가 가득 찬 경우 볼륨의 크기를 늘리려면 애그리게이트의 크기를 늘려야 합니다. 애그리게이트의 크기를 늘릴 수 있는 것은 없으며 SVM 관리자는 불가능합니다.

하나 이상의 애그리게이트에서 사용 가능한 공간이 2GB 미만(ONTAP 9.14.1 이하) 또는 5GB(ONTAP 9.15.1부터 시작)인 경우 SVM 감사 생성이 실패합니다. SVM 감사 생성에 실패하면 생성된 스테이징 볼륨이 삭제됩니다.