S3 이벤트를 감사합니다

ONTAP 9

NetApp
April 24, 2024

목차

S3 이벤트를 감사합니다

S3 이벤트를 감사합니다

ONTAP 9.10.1부터 ONTAP S3 환경에서 데이터 및 관리 이벤트를 감사할 수 있습니다. S3 감사 기능은 기존의 NAS 감사 기능과 유사하며, S3 및 NAS 감사가 클러스터에 공존할 수 있습니다.

SVM에서 S3 감사 구성을 생성하고 활성화하면 S3 이벤트가 로그 파일에 기록됩니다. 에서 로깅할 다음 이벤트를 지정할 수 있습니다.

- 개체 액세스(데이터) 이벤트입니다

  GetObject , PutObject 및 DeleteObject 를 참조하십시오

- 관리 이벤트

  PutBucket 및 DeleteBucket

로그 형식은 JSON(JavaScript Object Notation)입니다.

S3 및 NFS 감사 구성의 경우 결합된 제한은 클러스터당 50개의 SVM입니다.

다음 라이센스 번들이 필요합니다.

- 코어 번들, ONTAP S3 프로토콜 및 스토리지용

자세한 내용은 을 참조하십시오 "ONTAP 감사 프로세스의 작동 방식".

감사 보장

기본적으로 S3 및 NAS 감사가 보장됩니다. ONTAP는 노드를 사용할 수 없는 경우에도 감사 가능한 모든 버킷 액세스 이벤트를 기록할 수 있도록 보장합니다. 해당 작업에 대한 감사 레코드가 영구 스토리지의 스테이징 볼륨에 저장될 때까지 요청된 버킷 작업을 완료할 수 없습니다. 공간이 부족하거나 다른 문제로 인해 스테이징 파일에 감사 레코드를 커밋할 수 없는 경우 클라이언트 작업이 거부됩니다.

감사를 위한 공간 요구 사항

ONTAP 감사 시스템에서는 감사 레코드가 처음에는 개별 노드의 이진 스테이징 파일에 저장됩니다. 주기적으로 이러한 로그는 통합되어 사용자가 읽을 수 있는 이벤트 로그로 변환되며, SVM의 감사 이벤트 로그 디렉토리에 저장됩니다.

스테이징 파일은 감사 구성이 생성될 때 ONTAP에서 생성하는 전용 스테이징 볼륨에 저장됩니다. 애그리게이트당 하나의 스테이징 볼륨이 있습니다.

감사 구성에서 사용 가능한 충분한 공간을 계획해야 합니다.

- 감사된 버킷을 포함하는 애그리게이트에서 스테이징 볼륨의 경우
- 변환된 이벤트 로그가 저장되는 디렉토리가 포함된 볼륨입니다.

S3 감사 구성을 생성할 때 다음 두 가지 방법 중 하나를 사용하여 이벤트 로그 수와 볼륨의 사용 가능한 공간을 제어할 수 있습니다.

- 숫자 제한, '-rotate-limit' 매개변수는 보존되어야 하는 최소 감사 파일 수를 제어합니다.
- 시간 제한: '-retention-duration' 매개변수는 파일을 보존할 수 있는 최대 기간을 제어합니다.

두 매개 변수 모두에서 구성된 값을 초과하면 오래된 감사 파일을 삭제하여 새 감사 파일을 저장할 공간을 만들 수 있습니다. 두 매개 변수 모두 값이 0이면 모든 파일이 유지되어야 함을 나타냅니다. 따라서 충분한 공간을 확보하기 위해 매개 변수 중 하나를 0이 아닌 값으로 설정하는 것이 좋습니다.

감사 보장 때문에 감사 데이터에 사용할 수 있는 공간이 회전 제한 전에 초과되면 최신 감사 데이터를 생성할 수 없으므로 클라이언트가 데이터에 액세스하지 못합니다. 따라서 이 값과 감사에 할당된 공간을 신중하게 선택해야 하며 감사 시스템의 사용 가능한 공간에 대한 경고에 응답해야 합니다.

자세한 내용은 을 참조하십시오 "기본 감사 개념".

S3 감사 구성 계획

S3 감사 구성에 대해 여러 매개 변수를 지정하거나 기본값을 그대로 사용해야 합니다. 특히 적절한 여유 공간을 확보하는 데 도움이 되는 로그 회전 매개 변수를 고려해야 합니다.

구문 정보는 * 'vserver object-store-server audit create' * man 페이지를 참조하십시오.

일반 매개변수

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

정보 유형입니다	옵션을 선택합니다	필수 요소입니다
_SVM 이름 _ 감사 구성을 생성할 SVM의 이름입니다. S3에 대해 SVM이 이미 존재하고 사용하도록 설정해야 합니다.	'-verserver_svm_name_'	예
_로그 대상 경로 _ 변환된 감사 로그를 저장할 위치를 지정합니다. SVM에 경로가 이미 있어야 합니다. 경로는 최대 864자까지 가능하며 읽기-쓰기 권한이 있어야 합니다. 경로가 유효하지 않으면 감사 구성 명령이 실패합니다.	'-destination_text_'	예

_ 감사할 이벤트의 범주 _ 다음 이벤트 범주를 감사할 수 있습니다. • Data GetObject , PutObject 및 DeleteObject 이벤트 • 관리 PutBucket 및 DeleteBucket 이벤트 기본값은 데이터 이벤트만 감사하는 것입니다.	'-events{data|management},…'	아니요

다음 매개 변수 중 하나를 입력하여 감사 로그 파일 수를 제어할 수 있습니다. 값을 입력하지 않으면 모든 로그 파일이 유지됩니다.

정보 유형입니다	옵션을 선택합니다	필수 요소입니다
_ 로그 파일 회전 제한 _ 가장 오래된 로그 파일을 회전하기 전에 유지할 감사 로그 파일 수를 결정합니다. 예를 들어 값을 5로 입력하면 마지막 5개의 로그 파일이 유지됩니다. 값 0은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.	'-rotate-limit_integer _'	아니요
_로그 파일 지속 시간 제한 _ 로그 파일을 삭제하기 전에 보존할 수 있는 기간을 결정합니다. 예를 들어 5d0h0m 값을 입력하면 5일 이상 지난 로그가 삭제됩니다. 값 0은 모든 로그 파일이 보존됨을 나타냅니다. 기본값은 0입니다.	'-retention duration_integer_time_'	아니요

감사 로그 회전을 위한 매개 변수입니다

크기 또는 일정에 따라 감사 로그를 회전할 수 있습니다. 기본값은 크기에 따라 감사 로그를 회전하는 것입니다.

로그 크기에 따라 로그를 회전합니다

기본 로그 회전 방법과 기본 로그 크기를 사용하려면 로그 회전을 위한 특정 매개 변수를 구성할 필요가 없습니다. 기본 로그 크기는 100MB입니다.

기본 로그 크기를 사용하지 않으려면 '-rotate-size' 매개변수를 구성하여 사용자 정의 로그 크기를 지정할 수 있습니다.

로그 크기만을 기준으로 회전을 재설정하려면 다음 명령을 사용하여 '-rotate-schedule-minute' 매개 변수를 설정 해제합니다.

'vserver audit modify -vserver_svm_name_-destination/-rotate-schedule-minute -'

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.
  - '-rotate-schedule-month'입니다
  - '-rotate-schedule-DayOfWeek'
  - '-rotate-schedule-day'
  - '-rotate-schedule-hour'
- 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.
- 일정만 기준으로 회전을 재설정하려면 다음 명령을 사용하여 '-rotate-size 매개 변수'를 해제합니다.

  'vserver audit modify -vserver_svm_name_-destination/-rotate-size-'

로그 크기 및 일정에 따라 로그를 회전합니다

모든 조합의 -rotate-size 매개 변수와 시간 기반 회전 매개 변수를 모두 설정하여 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.

S3 감사 구성을 생성하고 설정합니다

S3 감사를 구현하려면 먼저 S3 기반 SVM에서 영구 오브젝트 저장소 감사 구성을 생성한 다음 구성을 활성화합니다.

필요한 것

- S3 지원 SVM:
- Aggregate에서 볼륨을 스테이징할 수 있는 충분한 공간입니다.

이 작업에 대해

감사 구성은 감사하려는 S3 버킷을 포함하는 각 SVM에 필요합니다. 신규 또는 기존 S3 서버에서 S3 감사를 활성화할

수 있습니다. 감사 구성은 * vserver object-store-server audit delete * 명령을 통해 제거될 때까지 S3 환경에서 지속됩니다.

S3 감사 구성은 감사를 위해 선택한 SVM의 모든 버킷에 적용됩니다. 감사 가능 SVM에는 감사되고 감사되지 않은 버킷이 포함될 수 있습니다.

로그 크기 또는 일정에 따라 자동 로그 회전에 대해 S3 감사를 구성하는 것이 좋습니다. 자동 로그 회전을 구성하지 않으면 기본적으로 모든 로그 파일이 유지됩니다. vserver object-store-server audit rotate -log * 명령을 사용하여 S3 로그 파일을 수동으로 회전할 수도 있습니다.

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

절차를 참조하십시오

1. 감사 구성을 생성하여 로그 크기 또는 일정에 따라 감사 로그를 회전합니다.

감사 로그를 회전하려면...	입력...
로그 크기	'vserver object-store-server audit create-vserver_svm_name_-destination_path_[[- events]{data| management},…] {[-rotate-limit_integer_]|[-retention-duration[*integer_d][_integer_h][_integer_m]]}[-rotate-size{_integer*[KB|MB|GB|TB|PB]}]']'
일정	'vserver object-store-server audit create-vserver_svm_name_-destination path[[- events]{data| management},…] {[-rotate-limit_integer_]|[-retention-duration[*integerd*][*integerh*][*integerm*]}[-rotate-schedule -month_chron_month_][-rotate_schedule -DayOfWeek_chron_dayOfWeek_] [-rotate_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_dayron_month 시간 기반 감사 로그 회전을 구성하려면 '-rotate-schedule-minute' 매개변수가 필요합니다.

2. S3 감사 활성화:

   'vserver object-store-server audit enable-vserver_svm_name_'

예

다음 예제에서는 크기 기반 회전을 사용하여 모든 S3 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그는 /audit_log 디렉토리에 저장됩니다. 로그 파일 크기 제한은 200MB입니다. 로그 크기가 200MB에 도달하면 로그가 회전합니다.

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

다음 예제에서는 크기 기반 회전을 사용하여 모든 S3 이벤트(기본값)를 감사하는 감사 구성을 만듭니다. 로그 파일 크기 제한은 100MB(기본값)이며, 로그 삭제 전 5일 동안 보존됩니다.

'cluster1::> vserver audit create - vserver vs1-destination/audit_log-retention-duration 5d0h0m'

다음 예제에서는 시간 기반 회전을 사용하여 S3 관리 이벤트와 중앙 액세스 정책 스테이징 이벤트를 감사하는 감사 구성을 만듭니다. 감사 로그는 매월 오후 12시 30분에 순환됩니다 일주일 내내. 로그 회전 제한은 5입니다.

'cluster1:> vserver audit create - vserver vs1-destination/audit_log-events management-rotate-schedule -month all-rotate-schedule -dayOfWeek all-rotate-schedule-hour 12-rotate-schedule-minute 30-rotate-limit 5'

S3 감사에 사용할 버킷을 선택합니다

감사 가능 SVM에서 감사할 버킷은 지정해야 합니다.

필요한 것

- S3 감사를 위해 SVM 지원

이 작업에 대해

S3 감사 구성은 SVM별로 활성화되지만 감사를 위해 SVM에서 버킷을 선택해야 합니다. SVM에 버킷을 추가하고 새 버킷을 감사하려면 이 절차를 사용하여 해당 버킷을 선택해야 합니다. S3 감사를 위해 SVM에서 감사하지 않은 버킷을 포함할 수도 있습니다.

감사 구성은 'vserver object-store-server audit object-select delete' 명령으로 제거될 때까지 버킷에 대해 유지됩니다.

절차를 참조하십시오

S3 감사에 사용할 버킷 선택:

'vserver object-store-server audit event-selector create-vserver_svm_name_-bucket_bucket_name_[[-access]{read-only|write-only|all}][[- permission]{allow-only|deny-only|all}]'입니다

- '-access' - 감사할 이벤트 액세스 유형을 'read-only', 'write-only', 'all'(기본값은 모두)로 지정합니다.
- '-permission'-'allow-only'', 'deny-only', 'all'(기본값: all')으로 감사할 이벤트 권한 유형을 지정합니다.

예

다음 예제에서는 읽기 전용 액세스로 허용된 이벤트만 기록하는 버킷 감사 구성을 만듭니다.

'cluster1::> vserver object-store-server audit event-selector create-vserver vs1-bucket test-bucket-access read-only-permission allow-only'

S3 감사 구성을 수정합니다

개별 버킷의 감사 매개 변수 또는 SVM에서 감사를 위해 선택한 모든 버킷의 감사 구성을 수정할 수 있습니다.

에 대한 감사 구성을 수정하려면...	입력...
개별 버킷	'vserver object-store-server audit event-selector modify -vserver_svm_name_[-bucket_bucket_name_][_parameters to modify _]'
SVM의 모든 버킷	'vserver object-store-server audit modify -vserver_svm_name_[_parameters to modify _]'

예

다음 예에서는 쓰기 전용 액세스 이벤트만 감사하도록 개별 버킷 감사 구성을 수정합니다.

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

다음 예에서는 SVM의 모든 버킷에 대한 감사 구성을 수정하여 로그 크기 제한을 10MB로 변경하고 회전 전에 로그 파일 3개를 보존합니다.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

S3 감사 구성을 표시합니다

감사 구성을 완료한 후 감사가 올바르게 구성되어 있고 활성화되어 있는지 확인할 수 있습니다. 또한 클러스터의 모든 오브젝트 저장소 감사 구성에 대한 정보를 표시할 수도 있습니다.

이 작업에 대해

버킷 및 SVM 감사 구성에 대한 정보를 표시할 수 있습니다.

- 버킷 - 'vserver object-store-server audit event-selector show' 명령어를 사용한다

  매개 변수 없이 명령을 실행하면 오브젝트 저장소 감사 구성이 포함된 클러스터의 모든 SVM에 있는 버킷에 대한 다음 정보가 표시됩니다.

  - SVM 이름
  - 버킷 이름
  - 액세스 및 권한 값

- SVM – 'vserver object-store-server audit show' 명령을 사용합니다

  매개 변수 없이 명령을 실행하면 오브젝트 저장소 감사 구성이 포함된 클러스터의 모든 SVM에 대한 다음 정보가 표시됩니다.

  - SVM 이름
  - 감사 상태
  - 대상 디렉토리

'-fields' 파라미터를 지정하여 표시할 감사 구성 정보를 지정할 수 있습니다.

절차를 참조하십시오

S3 감사 구성에 대한 정보 표시:

에 대한 구성을 수정하려면...	입력...
버킷	'vserver object-store-server audit event-selector show[-vserver_svm_name_][*parameters*]'

에 대한 구성을 수정하려면...	입력...
SVM	'vserver object-store-server audit show[-vserver_svm_name_][*parameters*]'

예

다음 예는 단일 버킷에 대한 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

다음 예는 SVM의 모든 버킷에 대한 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

다음 예에서는 모든 SVM에 대한 이름, 감사 상태, 이벤트 유형, 로그 형식, 타겟 디렉토리를 표시합니다.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

다음 예에서는 SVM 이름과 모든 SVM의 감사 로그에 대한 세부 정보를 표시합니다.

```
cluster1::> vserver object-store-server audit show -log-save-details

                   Rotation                           Rotation
      Vserver     File Size Rotation Schedule        Limit
      ----------- --------- ------------------------ --------
      vs1         100MB     -                        0
```

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

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                           Log Format: json
                  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
                  Log Retention Time: 0s
```