# S3イベントの監査

ONTAP 9

NetApp
December 20, 2024

# 目次

# S3イベントの監査

## S3イベントの監査

ONTAP 9 .10.1以降では、ONTAP S3環境でデータイベントと管理イベントを監査できます。S3の監査機能は既存のNASの監査機能と同様で、S3とNASの監査機能はクラスタ内に共存できます。

SVMでS3監査の設定を作成して有効にすると、S3イベントがログファイルに記録されます。ログに記録するイベントを指定できます。

### リリース別のオブジェクトアクセス（データ）イベント

9.11.1：

- ListBucketVersions
- ListBucket（9.10.1のListObjectからこの名前に変更）
- ListAllMyBuckets（9.10.1のListBucketsはこの名前に変更）

9.10.1：

- ヘッドオブジェクト
- GetObject
- PutObject
- deleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- リストアップロード
- ListParts

### リリース別の管理イベント

9.15.1：

- GetBucketCORS

- PutBucketCORS
- DeleteBucketCORS

9.14.1：

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1：

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1：

- GetBucketPolicy
- CopyObject
- パーツコピーをアップロード
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1：

- GetBucketVersioning
- PutBucketVersioning

9.10.1：

- ヘッドバケット
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

ログの形式はJavaScript Object Notation（JSON）です。

S3とNFSの監査設定の合計数は、クラスタあたり50 SVMです。

次のライセンスが必要です。

- ONTAP S3プロトコルおよびストレージ向けのONTAP ONE（旧Core Bundleに含まれていたもの）

詳細については、を参照してください "ONTAP監査プロセスの仕組み"。

### 監査の保証

デフォルトでは、S3とNASの監査が保証されます。ONTAPでは、あるノードを使用できない場合でも、監査可能なバケットアクセスイベントがすべて記録されることが保証されます。要求されたバケット処理は、その処理の監査レコードが永続的ストレージのステージングボリュームに保存されるまで完了できません。スペース不足やその他の問題が原因で監査レコードをステージングファイルでコミットできない場合は、クライアント処理が拒否されます。

### カンサヨウノスヘエスヨウケン

ONTAP監査システムでは、監査レコードは最初に個 々 のノード上のバイナリステージングファイルに格納されます。定期的に統合され、ユーザが読解可能なイベントログに変換されて、SVMの監査イベントログディレクトリに格納されます。

ステージングファイルは専用のステージングボリュームに格納されます。このボリュームは、監査設定の作成時にONTAPによって作成されます。各アグリゲートに1つのステージングボリュームがあります。

監査の設定に十分な使用可能スペースがあることを計画する必要があります。

- 監査対象バケットを含むアグリゲート内のステージングボリューム。
- （変換されたイベントログが格納されるディレクトリを含むボリューム）。

S3監査の設定を作成するときに次の2つの方法のいずれかを使用して、イベントログの数とボリュームの利用可能なスペースを制御できます。

- 最大数値。パラメータは、 `-rotate-limit`保持する必要がある監査ファイルの最小数を制御します。
- 時間制限。パラメータは、ファイルを保持できる最大期間を制御します。 `-retention-duration`

どちらのパラメータでも、構成済みの監査ファイルを超えると、古い監査ファイルを削除して新しい監査ファイル用のスペースを確保できます。両方のパラメータの値は0で、すべてのファイルを維持する必要があることを示します。したがって、十分なスペースを確保するためには、いずれかのパラメータをゼロ以外の値に設定することを推奨します。

監査が保証されるため、ローテーション制限の前に監査データに使用できるスペースがなくなると、新しい監査データを作成できなくなり、クライアントがデータにアクセスできなくなります。したがって、この値と監査に割り当てられるスペースは慎重に選択する必要があり、監査システムからの使用可能なスペースに関する警告に対応する必要があります。

詳細については、を参照してください "監査の基本概念"。

# S3監査の設定を計画する

S3監査の設定にはいくつかのパラメータを指定するか、デフォルトを受け入れる必要があります。特に、適切な空きスペースを確保するのに役立つログローテーションパラメータを検討する必要があります。

*`vserver object-store-server audit create`構文の詳細については、*のマニュアルページを参照してください。

## 一般パラメータ

監査の設定を作成するときに指定する必要がある必須パラメータが2つあります。また、指定できるオプションのパラメータも3つあります。

| 情報の種類 | オプション | 必須 |
|---|---|---|
| SVM 名 _<br><br>監査設定を作成するSVMの名前。<br><br>SVMがすでに存在し、S3に対して有効になっている必要があります。 | `-vserver` *`svm_name`* | ○ |
| _ ログデスティネーションパス _<br><br>変換された監査ログを格納する場所を指定します。SVM上にすでに存在しているパスを指定する必要があります。<br><br>パスは最大864文字で、読み取り/書き込み権限が必要です。<br><br>パスが無効な場合、監査設定コマンドは失敗します。 | `-destination` *`text`* | ○ |
| _ 監査するイベントのカテゴリ _<br><br>監査できるイベントカテゴリは次のとおりです。<br><br>• データGetObject、PutObject、およびDeleteObjectイベント<br>• 管理PutBucketイベントおよびDeleteBucketイベント<br><br>デフォルトでは、データイベントのみが監査されます。 | `-events {data\|management}, …` | いいえ |

監査ログファイルの数を制御するには、次のいずれかのパラメータを入力します。値を入力しない場合は、すべてのログファイルが保持されます。

| 情報の種類 | オプション | 必須 |
|---|---|---|
| ログファイルのローテーションの上限 _<br><br>保持する監査ログファイルの数を指定します。この数を超えると、最も古いログファイルがローテーションから除外されます。たとえば、値5を入力すると、最後の5つのログファイルが保持されます。<br><br>値0は、すべてのログファイルが保持されることを示します。デフォルト値は0です。 | `-rotate-limit` *`integer`* | いいえ |

| | | |
|---|---|---|
| ログファイル継続時間制限<br><br>ログファイルが削除されるまでの保持期間を指定します。たとえば、5d0h0mと入力すると、5日以上経過したログが削除されます。<br><br>値0は、すべてのログファイルが保持されることを示します。デフォルト値は0です。 | `-retention duration` *integer_time* | いいえ |

## 監査ログのローテーションのパラメータ

サイズまたはスケジュールに基づいて監査ログのローテーションを実行できます。デフォルトでは、監査ログのローテーションはサイズに基づいて行われます。

### ログサイズに基づくログのローテーション

デフォルトのログローテーション方式とデフォルトのログサイズを使用する場合は、ログローテーションのパラメータを設定する必要はありません。デフォルトのログサイズは100MBです。

デフォルトのログサイズを使用しない場合は、カスタムログサイズを指定するようにパラメータを設定できます `-rotate-size`。

ログサイズのみに基づいてローテーションをリセットする場合は、次のコマンドを使用してパラメータの設定を解除し `-rotate-schedule-minute`ます。

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

### スケジュールに基づいたログのローテーション

スケジュールに基づく監査ログのローテーションを選択した場合は、時間に基づくローテーションパラメータを任意の組み合わせで使用して、ログのローテーションをスケジュールできます。

- 時間に基づくローテーションを使用する場合、 `-rotate-schedule-minute`パラメータは必須です。
- その他の時間ベースのローテーションパラメータはすべてオプションです。
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- ローテーションスケジュールは、時間に関連するすべての値を使用して計算されます。たとえば、パラメータのみを指定する `-rotate-schedule-minute`と、監査ログファイルのローテーションは、毎月のすべての曜日の毎時間、指定した分に行われます。
- 時間に基づくローテーションパラメータを1つか2つだけ指定した場合（、など `-rotate-schedule -month -rotate-schedule-minutes`）、ログファイルのローテーションは、指定した月にのみ、すべての曜日の毎時間、指定した分に行われます。

  たとえば、監査ログのローテーションを、1月、3月、8月の月曜日、水曜日、土曜日の午前10時30分に実行するように指定できます。

- との `-rotate-schedule-day`両方に値を指定すると `-rotate-schedule-dayofweek`、それらは独立して考慮されます。

  たとえば、にFridayを指定し、 `-rotate-schedule-day`に13を指定する `-rotate-schedule-dayofweek`と、監査ログのローテーションは、13日の金曜日だけでなく、毎週金曜日、および指定した月の13日にも実行されます。

- スケジュールのみに基づいてローテーションをリセットする場合は、次のコマンドを使用しての設定を解除します `-rotate-size parameter`。

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

ログサイズとスケジュールに基づいたログのローテーション

ログサイズとスケジュールに基づいてログファイルをローテーションするように選択するには、-rotate-sizeパラメータと時間ベースのローテーションパラメータの両方を任意の組み合わせで設定します。たとえば、が10MBに設定され、 `-rotate-schedule-minute`が15に設定されている場合 `-rotate-size`、ログファイルのサイズが10MBに達したとき、または1時間ごとの15分（いずれか早い方）にログファイルがローテーションされます。

# S3監査の設定を作成して有効にする

S3監査を実装するには、まずS3対応のSVMで永続的なオブジェクトストアの監査設定を作成してから、設定を有効にします。

必要なもの

- S3対応のSVM。
- アグリゲートにステージングボリューム用の十分なスペースが必要です。

タスクの内容

監査の設定は、監査対象のS3バケットを含むSVMごとに必要です。新規または既存のS3サーバでS3監査を有効にすることができます。監査の設定は、 * vserver object-store-server audit delete * コマンドで削除されるまで S3 環境で維持されます。

S3監査の設定は、監査用に選択したSVM内のすべてのバケットに適用されます。監査が有効なSVMには、監査対象バケットと未監査バケットを含めることができます。

ログサイズまたはスケジュールに基づいて自動的にログがローテーションされるようにS3監査を設定することを推奨します。ログの自動ローテーションを設定しない場合、すべてのログファイルがデフォルトで保持されます。S3 ログファイルのローテーションは、 * vserver object-store-server audit rotate-log * コマンドを使用して手動で実行することもできます。

SVMがSVMディザスタリカバリのソースである場合、デスティネーションパスをルートボリュームに配置することはできません。

手順

1. ログサイズまたはスケジュールに基づいて監査ログのローテーションを行うには、監査の設定を作成します。

| 監査ログのローテーションの基準 | 入力するコマンド |
| --- | --- |
| ログサイズ | `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][_integers]]} [-rotate-size {`*integer*`[KB\|MB\|GB\|TB\|PB]}]` |
| スケジュール | `vserver object-store-server audit create -vserver` *svm_name* `-destination path [[-events] {data\|management}, …] {[-rotate-limit` *integer*`] \| [-retention-duration [`*integerd*`][`*integerh*`] [`*integerm*`][`*integers*`]] } [-rotate-schedule-month` *chron_month*`] [-rotate-schedule-dayofweek` *chron_dayofweek*`] [-rotate-schedule-day` *chron_dayofmonth*`] [-rotate-schedule-hour` *chron_hour*`] -rotate-schedule-minute` *chron_minute*<br><br>`-rotate-schedule-minute`時間に基づく監査ログのローテーションを設定する場合、パラメータは必須です。 |

2. S3監査を有効にします。

   `vserver object-store-server audit enable -vserver` *svm_name*

例

次の例は、サイズに基づくローテーションを使用してすべてのS3イベント（デフォルト）を監査する監査の設定を作成します。ログは/audit_logディレクトリに格納されます。ログファイルのサイズの上限は200MBです。ログは、サイズが200MBに達するとローテーションされます。

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

次の例は、サイズに基づくローテーションを使用してすべてのS3イベント（デフォルト）を監査する監査の設定を作成します。ログファイルのサイズの上限は100MB（デフォルト）で、ログは5日間保持されてから削除されます。

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

次の例は、時間に基づくローテーションを使用してS3管理イベントと集約型アクセスポリシーのステージングイベントを監査する監査の設定を作成します。監査ログのローテーションは、毎月、すべての曜日の午後12時30分に実行されます。ログのローテーション回数の上限は5回です。

```
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監査のバケットを選択

監査が有効なSVMでは、監査対象のバケットを指定する必要があります。

必要なもの

- S3監査が有効になっているSVM。

タスクの内容

S3 監査の設定は SVM 単位で有効になりますが、監査用に有効になっている SVM 内のバケットを選択する必要があります。SVMにバケットを追加し、新しいバケットを監査する場合は、この手順でバケットを選択する必要があります。SVMの監査で未監査のバケットをS3監査用に有効にすることもできます。

監査の設定は、コマンドで削除するまでバケットの設定が維持され `vserver object-store-server audit event-selector delete`ます。

手順

S3監査のバケットを選択：

```
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}]
```

- `-access`-監査対象のイベントアクセスのタイプ（、 `write-only`または） `all`を指定します `read-only`（デフォルトは `all`）。
- `-permission`-監査するイベント権限のタイプ（、 `deny-only`または） `all`を指定します。 `allow-only` `all`

例

次の例は、読み取り専用アクセスで許可されたイベントのみをログに記録するバケットの監査設定を作成します。

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

# S3監査の設定を変更する

SVMでは、個 々 のバケットの監査パラメータや、監査対象として選択したすべてのバケットの監査の設定を変更できます。

| 監査設定を変更する対象 | 入力するコマンド |
| --- | --- |
| 個々のバケット | `vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`]` `[`*`parameters to modify`*`]` |

| 監査設定を変更する対象 | 入力するコマンド |
| --- | --- |
| SVM内のすべてのバケット | `vserver object-store-server audit modify -vserver` *svm_name* [*parameters to modify*] |

例

次の例は、書き込み専用アクセスイベントのみを監査するように、個 々 のバケットの監査設定を変更します。

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

次の例は、 SVM 内のすべてのバケットの監査の設定を変更して、ログサイズの上限を 10MB に変更し、 3 つのログファイルを保持するように変更します。

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

# S3監査の設定を表示します。

監査の設定が完了したら、監査が適切に設定されて有効になっていることを確認できます。また、クラスタ内のすべてのオブジェクトストアの監査の設定に関する情報を表示することもできます。

タスクの内容

バケットとSVMの監査の設定に関する情報を表示できます。

- バケット–コマンドを使用します。 `vserver object-store-server audit event-selector show`

  パラメータを指定せずにコマンドを実行すると、オブジェクトストアの監査が設定されたクラスタ内のすべてのSVM内のバケットに関する次の情報が表示されます。

  - SVM名
  - バケット名
  - アクセスと権限の値
- SVM–コマンドを使用します。 `vserver object-store-server audit show`

  パラメータを指定せずにコマンドを実行すると、オブジェクトストアの監査が設定されたクラスタ内のすべてのSVMに関する次の情報が表示されます。

  - SVM名
  - 監査の状態

- ターゲットディレクトリ

パラメータを指定すると、表示する監査設定情報を指定できます `-fields`。

手順

S3監査の設定に関する情報を表示します。

| 設定を変更する対象 | 入力するコマンド |
| --- | --- |
| バケット | `vserver object-store-server audit event-selector show [-vserver svm_name] [parameters]` |
| SVM | `vserver object-store-server audit show [-vserver svm_name] [parameters]` |

例

次の例は、単一のバケットの情報を表示します。

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

次の例は、SVM上のすべてのバケットに関する情報を表示します。

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

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

次の例は、すべてのSVMの名前、監査の状態、イベントタイプ、ログ形式、およびターゲットディレクトリを表示します。

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

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

次の例は、すべてのSVMの名前と監査ログに関する詳細を表示します。

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

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

次の例は、すべてのSVMに関するすべての監査設定情報をリスト形式で表示します。

```
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
```

## 著作権に関する情報



## 商標に関する情報