S3イベントの監査

ONTAP 9

NetApp
February 12, 2026

目次

S3イベントの監査 . . . 1
- ONTAP S3イベントの監査について学ぶ . . . 1
  - リリース別のオブジェクト アクセス（データ）イベント . . . 1
  - リリース別の管理イベント . . . 1
  - 監査の保証 . . . 3
  - 監査のスペース要件 . . . 3
- ONTAP S3監査構成を計画する . . . 3
  - 一般パラメータ . . . 4
  - 監査ログのローテーション パラメータ . . . 5
- ONTAP S3監査設定を作成して有効にする . . . 6
- ONTAP S3監査用のバケットを選択する . . . 8
- ONTAP S3監査設定を変更する . . . 8
- ONTAP S3監査設定を表示する . . . 9

S3イベントの監査

ONTAP S3イベントの監査について学ぶ

ONTAP 9.10.1以降では、ONTAP S3環境のデータ イベントや管理イベントを監査できます。S3の監査機能は既存のNASの監査機能とほぼ同じであり、クラスタ内でS3とNASの監査を同時に使用できます。

SVMでS3の監査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。ログに記録できるイベントは次のとおりです。

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から名称変更）
- ListAllMyBuckets（9.10.1のListBucketsから名称変更）

9.10.1：

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- ListUploads
- 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
- UploadPartCopy
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1：

- GetBucketVersioning
- PutBucketVersioning

9.10.1：

- HeadBucket
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

ログ形式はJavaScript Object Notation（JSON）です。

クラスタごとに監査可能なSVM数は、S3とNFSの監査設定を合わせて最大400個です。

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（以前はCore Bundleに付属）

詳細については、"ONTAP監査プロセスの仕組み"を参照してください。

監査の保証

デフォルトでは、S3とNASの監査はどちらも保証されます。ONTAPでは、あるノードが利用できない場合でも、監査可能なバケット アクセス イベントはすべて記録されます。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。スペース不足またはその他の問題が原因で監査レコードをステージング ファイルにコミットできない場合、クライアント処理は拒否されます。

監査のスペース要件

ONTAPの監査システムでは、監査レコードは最初に個々のノードのバイナリ 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。

監査設定を作成するにあたっては、以下の項目について十分な使用可能スペースを確保する必要があります。

- 監査対象バケットを格納する、アグリゲート内のステージング ボリューム。
- 変換後のイベント ログの格納先ディレクトリを含むボリューム。

S3の監査設定を作成する際には、次のどちらかの方法を使用して、イベント ログの数、そして結果的にボリューム内の使用可能スペースを制御できます。

- 数値制限。 `-rotate-limit`パラメータは、保存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。 `-retention-duration`パラメータは、ファイルを保存できる最大期間を制御します。

どちらのパラメータも、設定値を超えると古い監査ファイルが削除されて新しい監査ファイル用のスペースが確保されます。どちらのパラメータも、0を指定するとすべてのファイルが保持されます。したがって、十分なスペースを確保するためには、どちら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。

監査の保証により、ローテーションの制限に達する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ず、クライアントはデータにアクセスできなくなります。そのため、このパラメータに指定する値と監査に割り当てるスペースを慎重に決定し、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適切に対処する必要があります。

詳細については、"監査の基本概念"を参照してください。

ONTAP S3監査構成を計画する

S3の監査設定では、いくつかのパラメータを指定する必要があります（デフォルトを受け入れることもできます）。特に、ログ ローテーションのパラメータについては、十分な空きスペースを確保できるように検討が必要です。

`vserver object-store-server audit create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-object-store-server-audit-create.html["ONTAPコマンド リファレンス
"^]をご覧ください。

一般パラメータ

監査設定の作成時に指定する必要がある2つの必須パラメータがあります。また、オプションのパラメータが3つあります。

情報の種類	オプション	必須
SVM 名 監査設定を作成するSVMの名前。 S3対応の既存のSVMを指定する必要があります。	`-vserver` *svm_name*	はい
ログの保存先パス 変換された監査ログを格納する場所を指定します。SVM上の既存のパスを指定する必要があります。 パスは864文字以内で、読み取り / 書き込みアクセス権が設定されている必要があります。 パスが有効でない場合、監査設定コマンドは失敗します。	`-destination` *text*	はい
監査対象イベントのカテゴリー 監査できるイベント カテゴリは次のとおりです。 • データGetObject、PutObject、DeleteObjectイベント • 管理 PutBucket および DeleteBucket イベント 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、次のどちらかのパラメータを入力します。値を入力しないと、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制限 最も古いログファイルをローテーションする前に保持する監査ログファイルの数を決定します。たとえば、値に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。 値を0に設定すると、すべてのログ ファイルが保持されます。デフォルト値は0です。	`-rotate-limit` *integer*	いいえ
ログファイルの保存期間制限 ログ ファイルを削除するまでの保持期間を指定します。たとえば、「5d0h0m」という値を入力すると、5日以上経過したログが削除されます。 値を0に設定すると、すべてのログ ファイルが保持されます。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 パラメータ

監査ログは、サイズまたはスケジュールに基づいてローテーションできます。デフォルトでは、サイズに基づいて監査ログがローテーションされます。

ログ サイズに基づいた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法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に関する特別な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100 MBです。

デフォルトのログ サイズを使用しない場合は、 `-rotate-size` パラメータを構成してカスタム ログ サイズを指定できます。

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 `-rotate-schedule-minute`パラメータの設定を解除します：

```
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いて監査ログをローテーションすることを選択した場合は、時間ベースの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。

- 時間ベースの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。
- それ以外の時間に基づくローテーション 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、すべての時間関連値を使用して計算されます。たとえば、 `-rotate-schedule-minute`パラメータのみを指定した場合、監査ログ ファイルは、年間を通じてすべての月のすべての時間帯において、すべての曜日で指定された分に基づいてローテーションされます。
- 時間ベースのローテーション パラメータを 1 つまたは 2 つだけ指定すると（たとえば、 `-rotate-schedule-month`および `-rotate-schedule-minutes`）、指定した月のみ、すべての曜日、すべての時間帯で指定した分の値に基づいてログ ファイルがローテーションされます。

  たとえば、監査ログを1月、3月、8月のすべての月曜日、水曜日、土曜日の午前10：30にローテーションするように指定できます。

- `-rotate-schedule-dayofweek`と `-rotate-schedule-day`の両方に値を指定した場合、それらは独立して考慮されます。

  たとえば、 `-rotate-schedule-dayofweek`を金曜日、 `-rotate-schedule-day`を13と指定した場合、監査ログは13日の金曜日だけでなく、毎週金曜日と指定した月の13日にローテーションされます。

- 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 `-rotate-size parameter`の設定を解除します：

  ```
  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

-rotate-size パラメータと時間ベースのローテーション パラメータを任意の組み合わせで設定することで、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できます。例： `-rotate-size`が10 MBに設定され、 `-rotate-schedule-minute`が15に設定されている場合、ログ ファイルのサイズが10 MBに達したとき、または毎時15分（どちらか早い方のイベント）にログ ファイルがローテーションされます。

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

ONTAP S3監査設定を作成して有効にする

S3の監査を実装するには、S3対応SVMに永続的オブジェクト ストアの監査設定を作成し、その設定を有効にします。

開始する前に

- S3 対応の SVM があります。
- ローカル階層にステージング ボリューム用の十分なスペースがあることを確認します。

タスク概要

監査対象のS3バケットを含むSVMごとに監査設定が必要です。新規または既存のS3サーバーでS3監査を有効にできます。監査設定は、*vserver object-store-server audit delete*コマンドで削除されるまでS3環境に保持されます。

S3の監査設定は、監査対象として選択したSVM内のすべてのバケットに適用されます。監査を有効にしたSVMには、監査対象のバケットだけでなく、監査対象外のバケットも含めることができます。

S3監査では、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ローテーションを行うように設定することをお勧めします。自動ログローテーションを設定しない場合は、デフォルトですべてのログファイルが保

持されます。*vserver object-store-server audit rotate-log*コマンドを使用して、S3ログファイルを手動でローテーションすることもできます。

SVMがSVMディザスタ リカバリ ソースである場合、デスティネーション パスをルート ボリューム上に設定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をローテーションする監査設定を作成します。

監査ログのローテーションの基準	入力する内容
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* `-rotate-schedule-minute`パラメータは、時間ベースの監査ログのローテーションを構成する場合に必須です。

2. S3の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 サイズの上限は200MBです。ログのサイズが200MB以上になると、ログが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）を監査する監査設定を作成します。ログ ファイルの最大サイズは100MB（デフォルト）で、5日経過すると削除されます。

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

以下の例では、時間ベースの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設定を作成します。監査ログは毎月、毎日午後12：30にローテーションされます。ログローテーションの上限は5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
```

ONTAP S3監査用のバケットを選択する

監査が有効なSVMから監査対象のバケットを指定する必要があります。

開始する前に

- S3 監査が有効になっている SVM があります。

タスク概要

S3監査設定はSVMごとに有効化されますが、監査が有効になっている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、その新しいバケットを監査対象とする場合は、この手順でバケットを選択する必要があります。また、S3監査が有効になっているSVM内に監査対象外のバケットを含めることもできます。

監査構成は、 `vserver object-store-server audit event-selector delete` コマンドによって削除されるまでバケットに対して保持されます。

手順

1. S3の監査対象にするバケットを選択します。

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

ONTAP S3監査設定を変更する

個々のバケット、またはSVM内で監査対象として選択されているすべてのバケットについて、監査設定を変更することができます。

監査設定を変更する対象	入力する内容
個々のバケット	`vserver object-store-server audit event-selector modify -vserver` *svm_name* [`-bucket` *bucket_name*] [*parameters to modify*]
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、書き込み専用のアクセス 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
```

次の例では、SVM 内のすべてのバケットの監査設定を変更して、ログ サイズの制限を 10MB に変更し、ローテーション前に 3 つのログ ファイルを保持するようにしています。

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

ONTAP S3監査設定を表示する

監査設定が完成したら、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。クラスタ内のすべてのオブジェクト ストアの監査設定に関する情報を表示することもできます。

タスク概要

バケットとSVMの監査設定に関する情報を表示できます。

- バケット： `vserver object-store-server audit event-selector show`コマンドを使用する

  このコマンドをパラメータなしで実行すると、オブジェクト ストアの監査設定があるクラスタ内のすべてのSVMのバケットについて、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： `vserver object-store-server audit show`コマンドを使用する

  このコマンドをパラメータなしで実行すると、オブジェクト ストアの監査設定があるクラスタ内のすべてのSVMについて、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

> `-fields`パラメータを指定して、表示する監査構成情報を指定できます。

手順

S3の監査設定に関する情報を表示します。

変更対象	入力する内容
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のすべて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

     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、イベントの種類、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、および監査ログの詳細情報を表示します。

```
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