# SVMでファイルとディレクトリの監査設定を作成します。

ONTAP 9

NetApp
December 20, 2024

# 目次

# SVMでファイルとディレクトリの監査設定を作成します。

## 監査の設定を作成する

Storage Virtual Machine（SVM）上でファイルとディレクトリの監査の設定を作成するには、使用可能な設定オプションについて理解し、設定を計画し、設定を行って有効にします。その後、監査の設定に関する情報を表示して、設定した設定が適切かどうかを確認できます。

ファイルおよびディレクトリイベントの監査を開始する前に、監査の設定をStorage Virtual Machine（SVM）で作成する必要があります。

開始する前に

集約型アクセスポリシーステージングの監査の設定を作成する場合は、SVM上にSMBサーバが存在している必要があります。

- 監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントはダイナミックアクセス制御が有効になっている場合にのみ生成されます。

  ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。

- コマンドのフィールドの引数が無効な場合（フィールドのエントリが無効である、エントリが重複している、エントリがないなど）、コマンドは監査フェーズの前に失敗します。

  この場合、監査レコードは生成されません。

タスクの内容

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。

ステップ

1. 計画ワークシートの情報を使用して、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ための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 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]}]` |
| スケジュール | `vserver audit create -vserver vserver_name -destination path -events [{file-ops |
| cifs-logon-logoff | cap-staging}] [-format {xml |

例

次の例は、サイズに基づくローテーションを使用してファイル操作とSMBログオンおよびログオフイベント（デフォルト）を監査する監査の設定を作成します。ログ形式は（デフォルト）です `EVTX`。ログはディレクトリに保存され `/audit_log`ます。ログファイルの最大サイズはです `200 MB`。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ファイル操作とSMBログオンおよびログオフイベント（デフォルト）を監査する監査の設定を作成します。ログ形式は（デフォルト）です `EVTX`。ログはディレクトリに保存され `/cifs_event_logs`ます。ログファイルのサイズの上限は `100 MB`（デフォルト）、ログのローテーションの上限は次のとおり `5`です。

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

次の例は、時間に基づくローテーションを使用してファイル操作、CIFSのログオンおよびログオフイベント、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。ログ形式は（デフォルト）です `EVTX`。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の上限は次のとおりです `5`。

```
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
```

関連情報

- "SVMで監査を有効にする"
- "監査の設定を確認する"

# SVMで監査を有効にする

監査の設定が完了したら、 Storage Virtual Machine （ SVM ）で監査を有効にする必要があります。

開始する前に

SVM の監査設定がすでに存在している必要があります。

タスクの内容

SVM ディザスタリカバリ ID 破棄の設定が（ SnapMirror 初期化完了後に）初めて開始され、 SVM に監査の設定がある場合、 ONTAP は監査の設定を自動的に無効にします。読み取り専用 SVM では、ステージングボリュームがいっぱいにならないように監査が無効になっています。SnapMirror 関係が解除されて SVM が読み書き可能になったあとでないと、監査を有効にすることはできません。

手順

1. SVM で監査を有効にします。

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

関連情報

- "監査の設定を作成する"
- "監査の設定を確認する"

# 監査の設定を確認する

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する必要があります。

手順

1. 監査の設定を確認します。

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   次のコマンドは、Storage Virtual Machine（SVM）vs1のすべての監査の設定情報をリスト形式で表示します。

   ```
   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
```

関連情報

- "監査の設定を作成する"
- "SVMで監査を有効にする"

## 著作権に関する情報



## 商標に関する情報