監査の設定を管理します
ONTAP 9

NetApp
April 24, 2024

目次

監査の設定を管理します

監査イベントログの手動ローテーションを行います

監査イベントログは、表示する前に、ユーザが読解可能な形式に変換する必要があります。ONTAP によるログの自動ローテーション前に、特定の Storage Virtual Machine （ SVM ）のイベントログを表示する場合は、その SVM で監査イベントログの手動ローテーションを行うことができます。

ステップ

1. を使用して、監査イベントログのローテーションを行います `vserver audit rotate-log` コマンドを実行します

   ```
   vserver audit rotate-log -vserver vs1
   ```

   監査イベントログは、監査の設定で指定されている形式で、SVMの監査イベントログディレクトリに保存されます (`XML` または `EVTX`）をクリックし、適切なアプリケーションを使用して表示できます。

SVM での監査を有効または無効にします

Storage Virtual Machine （ SVM ）での監査を有効または無効にすることができます。必要に応じて、監査を無効にすることで、ファイルおよびディレクトリの監査を一時的に停止できます。監査はいつでも有効にできます（監査の設定が存在する場合）。

必要なもの

SVM で監査を有効にするには、 SVM の監査の設定がすでに存在している必要があります。

"監査の設定を作成します"

このタスクについて

監査を無効にしても、監査の設定は削除されません。

手順

1. 適切なコマンドを実行します。

監査の設定	入力するコマンド
有効	`vserver audit enable -vserver vserver_name`
無効	`vserver audit disable -vserver vserver_name`

2. 監査が目的の状態になっていることを確認します。

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

例

次の例は、 SVM vs1 で監査を有効にします。

```
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
```

次の例は、 SVM vs1 で監査を無効にします。

```
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
```

監査の設定に関する情報を表示します

監査の設定に関する情報を表示できます。この情報は、各 SVM で適切な設定が使用されているかどうか確認するのに役立ちます。また、表示される情報から、監査の設定が

有効になっているかどうかを確認することもできます。

このタスクについて

すべての SVM の監査の設定に関する詳細情報を表示することも、オプションのパラメータを指定して、出力に表示される情報をカスタマイズすることもできます。オプションのパラメータを何も指定しない場合、次の情報が表示されます。

- 監査の設定が適用される SVM の名前
- 監査の状態。になります `true` または `false`

  監査の状態がの場合 `true`監査が有効になっています。監査の状態がの場合 `false`監査は無効になっています。

- 監査するイベントのカテゴリ
- 監査ログの形式
- 統合および変換された監査ログが監査サブシステムによって格納されるターゲットディレクトリ

ステップ

1. を使用して、監査の設定に関する情報を表示します `vserver audit show` コマンドを実行します

   コマンドの使用の詳細については、マニュアルページを参照してください。

例

次の例は、すべての SVM の監査の設定の概要を表示したものです。

```
cluster1::> vserver audit show

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

次の例は、すべての SVM の監査の設定情報をリスト形式で表示したものです。

```
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
```

監査の設定を変更するコマンド

監査設定を変更する場合は、ログのデスティネーションパスおよび形式の変更、監査するイベントのカテゴリの変更、ログファイルの自動保存方法、保存するログファイルの最大数の指定など、現在の設定をいつでも変更できます。

状況	使用するコマンド
ログデスティネーションパスを変更します	`vserver audit modify` を使用 `-destination` パラメータ
監査するイベントのカテゴリを変更します	`vserver audit modify` を使用 `-events` パラメータ 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には、Dynamic Access Control（DAC；ダイナミックアクセス制御）SMBサーバオプションがStorage Virtual Machine（SVM）で有効になっている必要があります。
ログ形式を変更します	`vserver audit modify` を使用 `-format` パラメータ
内部的な一時ログファイルサイズに基づいた自動保存の有効化	`vserver audit modify` を使用 `-rotate-size` パラメータ

時間間隔に基づいた自動保存の有効化	`vserver audit modify` を使用 `-rotate-schedule-month`、 `-rotate-schedule-dayofweek`、 `-rotate-schedule-day`、 `-rotate-schedule-hour`および `-rotate-schedule-minute` パラメータ
保存されるログファイルの最大数の指定	`vserver audit modify` を使用 `-rotate-limit` パラメータ

監査の設定を削除します

Storage Virtual Machine （ SVM ）でのファイルおよびディレクトリイベントの監査が必要なくなり、 SVM で監査の設定を維持する必要がなくなった場合は、監査の設定を削除できます。

手順

1. 監査の設定を無効にします。

   ```
   vserver audit disable -vserver vserver_name
   ```

   ```
   vserver audit disable -vserver vs1
   ```

2. 監査の設定を削除します。

   ```
   vserver audit delete -vserver vserver_name
   ```

   ```
   vserver audit delete -vserver vs1
   ```

クラスタリバートの影響を理解する

クラスタのリバートを予定している場合は、監査が有効になっている Storage Virtual Machine （ SVM ）がクラスタ内に存在するときに ONTAP が従うリバートのプロセスに注意する必要があります。リバートを行う前に特定の操作を実行する必要があります。

SMBのログオンおよびログオフ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の監査をサポートしていないバージョンの**ONTAP**へのリバート

SMBのログオンおよびログオフ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のサポートは、clustered Data ONTAP 8.3から開始されました。これらのイベントタイプをサポートしていないバージョンの ONTAP へのリバートを予定していて、これらのイベントタイプを監視する監査が設定されている場合は、リバートを行う前に、監査が有効になっている SVM の監査の設定を変更する必要があります。設定は、ファイル操作イベントのみが監査されるように変更する必要があります。