



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	1
監査イベントログの手動ローテーションを行います	1
SVM での監査を有効または無効にします	1
監査の設定に関する情報を表示します	2
監査の設定を変更するコマンド	4
監査の設定を削除します	5
クラスタリバートの影響を理解する	5

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	<code>vserver audit enable -vserver vserver_name</code>
無効	<code>vserver audit disable -vserver vserver_name</code>

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     evttx      /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	<code>vserver audit modify</code> を使用 <code>-destination</code> パラメータ
監査するイベントのカテゴリを変更します	<div>  <p>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。</p> </div> <div> <code>vserver audit modify</code> を使用 <code>-events</code> パラメータ </div>
ログ形式を変更します	<code>vserver audit modify</code> を使用 <code>-format</code> 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	<code>vserver audit modify</code> を使用 <code>-rotate-size</code> パラメータ

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

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。