



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。	1
監査の設定を作成する	1
SVMで監査を有効にする	3
監査の設定を確認する	3

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

- 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	<code>`vserver audit create -vserver vserver_name -destination path -events [{file-ops</code>
cifs-logon-logoff	<code>cap-staging</code>
file-share	<code>authorization-policy-change</code>
user-account	<code>security-group</code>

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分に行われます。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

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。