SVM で NAS イベントを監査します

ONTAP 9

NetApp
April 24, 2024

目次

SVM で NAS イベントを監査します

SMB および NFS の監査とセキュリティトレース

SMB プロトコルと NFS プロトコルで使用できるファイルアクセス監査機能は、 ONTAP で使用できます。たとえば、 FPolicy を使用した標準の監査やファイルポリシー管理などです。

SMB と NFS のファイルアクセスイベントの監査は、次のような状況で設計および実装する必要があります。

- SMB および NFS プロトコルの基本的なファイルアクセスが設定されている。
- 次のいずれかの方法で監査の設定を作成して管理する。
  - ONTAP の標準機能
  - 外部 FPolicy サーバ

SVM で NAS イベントを監査します

NASイベントの監査は、Storage Virtual Machine（SVM）で特定のSMBおよびNFSイベントを追跡してログに記録できるセキュリティ対策です。これは、潜在的なセキュリティの問題を追跡するのに役立ち、セキュリティ違反が発生した場合の証拠になります。Active Directory の集約型アクセスポリシーのステージングおよび監査によってこれらを実装した場合の結果を確認することもできます。

SMBイベント

次のイベントを監査できます。

- SMB ファイルおよびフォルダのアクセスイベント

  監査が有効になっている SVM に属する FlexVol ボリュームに格納されているオブジェクトに対する SMB によるファイルおよびフォルダアクセスイベントを監査できます。

- SMBロクオンオヨヒログオフイベント

  SVM上のSMBサーバでのSMBログオンおよびログオフイベントを監査できます。

- 集約型アクセスポリシーのステージングイベント

  提案された集約型アクセスポリシーによって適用された権限を使用して、SMBサーバ上のオブジェクトの有効なアクセスを監査できます。集約型アクセスポリシーのステージングによって監査を行うと、集約型アクセスポリシーを導入する前に、その影響を確認できます。

  集約型アクセスポリシーのステージングによる監査は、 Active Directory の GPO を使用してセットアップされます。ただし、 SVM の監査の設定は、集約型アクセスポリシーステージングイベントを監査するように設定されている必要があります。

  SMB サーバでダイナミックアクセス制御を有効にせずに、監査の設定で集約型アクセスポリシーのステージングを有効にすることはできますが、集約型アクセスポリシーのステージングイベントが生成されるのは、ダイナミックアクセス制御が有効になっている場合のみです。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。

NFSイベント

ファイルおよびディレクトリイベントを監査するには、SVMに格納されているオブジェクトでNFSv4 ACLを使用します。

監査の仕組み

監査の基本概念

ONTAP の監査について理解するために、監査の基本概念を確認しておく必要があります。

- * ステージングファイル *

  統合および変換の前に監査レコードが格納される、個々のノード上の中間バイナリファイル。ステージングファイルはステージングボリュームに格納されます。

- * ステージングボリューム *

  ステージングファイルを格納するために ONTAP によって作成される専用ボリューム。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。ステージングボリュームは、そのアグリゲート内のデータボリュームを対象としたデータアクセスの監査レコードを格納するために、監査が有効なすべての Storage Virtual Machine （ SVM ）で共有されます。各 SVM の監査レコードは、ステージングボリューム内の個別のディレクトリに格納されます。

  クラスタ管理者はステージングボリュームに関する情報を表示できますが、それ以外のほとんどのボリューム操作は実行できません。ステージングボリュームを作成できるのは ONTAP のみです。ONTAP では、ステージングボリュームに自動的に名前が割り当てられます。すべてのステージングボリューム名はで始まります `MDV_aud_` そのあとに、ステージングボリュームを含むアグリゲートのUUID（例：`MDV_aud_1d0131843d4811e296fc123478563412.`）

- * システムボリューム *

  ファイルサービスや監査ログのメタデータなど、特別なメタデータを格納する FlexVol ボリューム。システムボリュームの所有者は管理 SVM であり、システムボリュームはクラスタ全体で表示されます。ステージングボリュームはシステムボリュームの一種です。

- * 統合タスク *

  監査が有効になったときに作成されるタスク。各 SVM で長時間にわたって実行されるこのタスクは、SVM のメンバーノード全体のステージングファイルから監査レコードを取得します。このタスクは、監査レコードを時間順にソートされた状態でマージしたうえで、これらのレコードを監査の設定で指定されたユーザが読解可能なイベントログ形式に変換します。変換されたイベントログは、 SVM 監査の設定で指定された監査イベントログディレクトリに格納されます。

ONTAP 監査プロセスの仕組み

ONTAP の監査プロセスは、 Microsoft の監査プロセスとは異なります。監査を設定する前に、 ONTAP の監査プロセスの仕組みについて理解しておく必要があります。

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。ある SVM で監査が有効になると、すべてのメンバーノードでその SVM のステージングファイルが保持されます。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。

ある **SVM** で監査が有効になっている場合の処理

監査は、 SVM でのみ有効にできます。ストレージ管理者が SVM で監査を有効にすると、監査サブシステムによってステージングボリュームが存在するかどうかが確認されます。ステージングボリュームは、 SVM に所有されているデータボリュームを含むアグリゲートごとに必要です。存在しない場合は、監査サブシステムによって必要なステージングボリュームが作成されます。

また、監査が有効になる前に、前提条件となるその他のタスクが実行されます。

- 監査サブシステムによって、ログディレクトリのパスが使用可能でシンボリックリンクが含まれていないことが検証されます。

  ログディレクトリは、 SVM のネームスペース内のパスとしてすでに存在している必要があります。監査ログファイルを格納する新しいボリュームまたは qtree を作成することを推奨します。監査サブシステムは、デフォルトのログファイルの場所を割り当てません。監査の設定で指定されているログディレクトリのパスが有効なパスでない場合は、で監査の設定の作成に失敗します `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` エラー。

  ディレクトリは存在するがシンボリックリンクが含まれている場合は、設定の作成に失敗します。

- 監査によって統合タスクがスケジュールされます。

  このタスクがスケジュールされると、監査が有効になります。SVMの監査の設定とログファイルは、リブート後も、NFSサーバまたはSMBサーバが停止したり再起動したりしても維持されます。

イベントログの統合

ログの統合は、監査が無効になるまで定期的に実行されるスケジュール済みタスクです。監査が無効になると、統合タスクによって残りのすべてのログが統合されたことが検証されます。

監査の保証

デフォルトでは、監査が保証されています。ONTAP では、あるノードが利用できない場合でも、監査可能なファイルアクセスイベント（設定された監査ポリシーの ACL で指定されている）がすべて記録されることが保証されます。要求されたファイル操作は、その操作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のディスクにコミットできない場合は、クライアント処理が拒否されます。

> 管理者または権限レベルのアクセス権を持つアカウントユーザは、 NetApp Manageability SDK または REST API を使用してファイル監査ログ処理を省略できます。NetApp Manageability SDKまたはREST APIを使用してファイル操作が行われたかどうかを確認するには、に格納されているコマンド履歴ログを確認します `audit.log` ファイル。
>
> コマンド履歴監査ログの詳細については、の「管理アクティビティの監査ログの管理」セクションを参照してください "システム管理"。

ノードが利用できない場合の統合プロセス

監査が有効になっている SVM に属するボリュームを含むノードが利用できない場合、監査の統合タスクの動作は、そのノードのストレージフェイルオーバー（ SFO ）パートナー（ 2 ノードクラスタの場合は HA パートナー）が利用可能かどうかによって異なります。

- ステージングボリュームが SFO パートナーを介して利用可能な場合は、ノードから最後に報告されたステージングボリュームがスキャンされ、統合が正常に行われます。
- SFO パートナーが利用できない場合は、タスクによって部分的なログファイルが作成されます。

  あるノードにアクセスできない場合は、統合タスクによって、その SVM の利用可能な他のノードの監査レコードが統合されます。完了していないことを識別するために、サフィックスが追加されます `.partial` を統合ファイル名に変更します。

- 利用できないノードが利用可能になったら、そのノードの監査レコードが、その時点における他のノードの監査レコードと統合されます。
- 監査レコードはすべて維持されます。

イベントログのローテーション

監査イベントログファイルは、設定されたログサイズしきい値に達した場合、または設定されたスケジュールに従ってローテーションされます。イベントログファイルがローテーションされると、スケジュールされた統合タスクによって、まず、アクティブな変換済みファイルの名前がタイムスタンプのあるアーカイブファイルに変更され、そのあとで新しいアクティブな変換済みイベントログファイルが作成されます。

SVM で監査が無効になっている場合の処理

SVM で監査が無効になると、もう一度統合タスクがトリガーされます。未処理の記録済みの監査レコードはすべて、ユーザが読解可能な形式でログに記録されます。SVM で監査が無効になっても、イベントログディレクトリに格納されている既存のイベントログは削除されず、参照が可能です。

その SVM の既存のステージングファイルがすべて統合されたら、スケジュールから統合タスクが削除されます。SVM の監査の設定を無効にしても、監査の設定は削除されません。ストレージ管理者は、監査をいつでも再度有効にできます。

監査の統合ジョブは、監査が有効になったときに作成され、統合タスクを監視して、統合タスクがエラーによって終了した場合に統合タスクを再作成します。ユーザは監査の統合ジョブを削除できません。

監査の要件と考慮事項

Storage Virtual Machine （ SVM ）で監査を設定して有効にする前に、一定の要件と考慮事項について理解しておく必要があります。

- 監査を有効にしたSVMの最大サポート数は、ONTAPのバージョンによって異なります。

ONTAPバージョン	最大
9.8以前	50です
9.9.1 以降	400

- 監査は、 SMB または NFS のライセンスとは関係ありません。

  クラスタにSMBとNFSのライセンスがインストールされていない場合でも、監査を設定して有効にすることができます。

- NFS 監査では、セキュリティ ACE （タイプ U ）をサポートしています。
- NFS 監査では、モードビットと監査 ACE の間のマッピングはありません。

  ACL をモードビットに変換する場合、監査 ACE はスキップされます。モードビットを ACL に変換する場合、監査 ACE は生成されません。

- 監査の設定で指定するディレクトリが存在している必要があります。

  存在しない場合、監査の設定を作成するコマンドは失敗します。

- 監査の設定で指定するディレクトリは、次の要件を満たしている必要があります。
  - ディレクトリにシンボリックリンクを含めることはできません。

    監査の設定で指定するディレクトリにシンボリックリンクが含まれている場合、監査の設定を作成するコマンドは失敗します。

  - 絶対パスを使用してディレクトリを指定する必要があります。

    相対パスは指定しないでください（例：）。 `/vs1/../`。

- 監査は、ステージングボリューム内に利用可能なスペースがあるかどうかに依存します。

  監査対象のボリュームを含むアグリゲートのステージングボリュームに十分なスペースを確保できるよう注意する必要があります。

- 監査は、変換されたイベントログの格納先ディレクトリを含むボリューム内に利用可能なスペースがあるかどうかに依存します。

  イベントログの格納に使用するボリュームに十分なスペースを確保できるよう注意する必要があります。を使用して、監査ディレクトリに保持するイベントログの数を指定できます `-rotate-limit` 監査の設定を作成する際のパラメータ。これは、ボリューム内のイベントログ用に十分なスペースを確保するのに役立ちます。

- 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を生成するには、ダイナミックアクセス制御を有効にする必要があります。

  ダイナミックアクセス制御は、デフォルトでは有効になっていません。

監査を有効にする際のアグリゲートスペースに関する考慮事項

監査の設定が作成されていてクラスタ内の少なくとも 1 つの Storage Virtual Machine （ SVM ）で監査が有効になっている場合、監査サブシステムは、既存のすべてのアグリゲートと、作成されるすべての新しいアグリゲートにステージングボリュームを作成します。クラスタ上で監査を有効にする際は、アグリゲートスペースに関する考慮事項に注意する必要があります。

アグリゲートに十分な空き容量がない場合、ステージングボリュームの作成に失敗することがあります。これは、監査の設定を作成したときに、既存のアグリゲートにステージングボリュームを格納するための十分なスペースがない場合に発生することがあります。

SVM で監査を有効にする前に、既存のアグリゲート上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する必要があります。

ステージングファイルの監査レコードのサイズに関する制限

ステージングファイルの監査レコードのサイズは、 32KB 以下にする必要があります。

大規模な監査レコードが発生する可能性がある場合

次のいずれかのシナリオで、管理の監査時に大規模な監査レコードが発生することがあります。

- 多数のユーザを含むグループに対してユーザを追加または削除する。
- 多数のファイル共有ユーザを含むファイル共有に対して、ファイル共有アクセス制御リスト（ ACL ）を追加または削除する。
- その他のシナリオ。

この問題を回避するには、管理監査を無効にしてください。これを行うには、監査設定を変更し、監査イベントタイプのリストから次の項目を削除します。

- ファイル共有
- ユーザアカウント
- セキュリティグループ
- 認証ポリシー変更

  削除すると、ファイルサービスの監査サブシステムで監査されなくなります。

大きすぎる監査レコードの影響

- 監査レコードのサイズが大きすぎる（ 32KB を超える）場合、監査レコードは作成されず、監査サブシステムによって次のような Event Management System （ EMS ；イベント管理システム）メッセージが生成されます。

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  監査が保証されている場合は、監査レコードを作成できないためにファイル処理が失敗します。

- 監査レコードのサイズが 9 、 999 バイトを超える場合は、上記と同じ EMS メッセージが表示されます。部分的な監査レコードが作成され、指定した値よりも大きな値が欠落します。
- 監査レコードが 2 、 000 文字を超えている場合は、実際の値ではなく次のエラーメッセージが表示されます。

  ```
  The value of this field was too long to display.
  ```

サポートされる監査イベントログの形式

変換された監査イベントログでサポートされるファイル形式はです EVTX および XML ファイル形式。

監査の設定を作成する際には、ファイル形式の種類を指定できます。デフォルトでは、ONTAP はバイナリログをに変換します EVTX ファイル形式。

監査イベントログを表示する

監査イベントログを使用して、ファイルセキュリティが適切であるかどうか、ファイルやフォルダへの不適切なアクセス試行がなかったかどうかを確認できます。に保存された監査イベントログを表示および処理できます EVTX または XML ファイル形式。

- EVTX ファイル形式

  変換されたを開くことができます EVTX Microsoftイベントビューアを使用して、保存されたファイルとしてイベントログを監査します。

  イベントビューアでイベントログを表示する際に使用できるオプションは 2 つあります。

  - 全般表示

    イベントレコードには、すべてのイベントに共通する情報が表示されます。このバージョンの ONTAP では、イベントレコードに関するイベント固有のデータは表示されません。詳細表示を使用して、イベント固有のデータを表示できます。

  - 詳細ビュー

    フレンドリ表示と XML 表示を使用できます。フレンドリ表示と XML 表示には、すべてのイベントに共通の情報とイベントレコードのイベント固有のデータの両方が表示されます。

- XML ファイル形式

  表示と処理が可能です XML をサポートする他社製アプリケーションの監査イベントログ XML ファイル形式。XML スキーマと XML フィールドの定義に関する情報があれば、 XML 表示ツールを使用して監査ログを表示できます。XML スキーマおよび定義の詳細については、を参照してください "ONTAP 監査スキーマリファレンス"。

イベントビューアを使用したアクティブな監査ログの表示方法

クラスタで監査の統合プロセスを実行している場合、統合プロセスにより、監査を有効にした SVM のアクティブな監査ログファイルに新しいレコードが追加されます。このアクティブな監査ログは、 SMB 共有でアクセスして Microsoft イベントビューアで開くことができます。

イベントビューアには、既存の監査レコードが表示されるだけでなく、コンソールウィンドウの内容を更新するオプションもあります。アクティブな監査ログにアクセスするために使用される共有で oplock が有効になっているかどうかに応じて、新たに追加されたログをイベントビューアで表示できるかどうかが異なります。

共有での oplock の設定	動作
有効	その時点までに書き込まれたイベントを含むログがイベントビューアに表示されます。更新処理を実行してもログは更新されず、統合プロセスで追加された新しいイベントは表示されません。
無効	その時点までに書き込まれたイベントを含むログがイベントビューアに表示されます。更新処理を実行すると、ログが更新され、統合プロセスで追加された新しいイベントが表示されます。

この情報は、にのみ適用されます `EVTX` イベントログ。 `XML` イベントログは、SMBを介してブラウザで、または任意のXMLエディタまたはビューアを使用してNFSで表示できます。

監査できる SMB イベント

監査できる SMB イベントの概要

ONTAP は、ファイルおよびフォルダのアクセスイベント、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などの SMB イベントを監査できます。どのようなアクセスイベントを監査できるか理解しておくと、イベントログの結果を解釈するときに役立ちます。

ONTAP 9.2 以降では、次の SMB イベントが監査対象として追加されました。

イベント ID （ EVT / EVTX ）	イベント	説明	カテゴリ
4670	オブジェクト権限が変更されました	オブジェクトアクセス：権限が変更された。	ファイルアクセス
4907	オブジェクトの監査設定が変更されました	オブジェクトアクセス：監査設定が変更された。	ファイルアクセス
4913	オブジェクトの集約型アクセスポリシーが変更されました	オブジェクトへのアクセス： CAP が変更された。	ファイルアクセス

ONTAP 9.0 以降では、次の SMB イベントを監査できます。

イベント ID （ EVT / EVTX ）	イベント	説明	カテゴリ
540/4624	アカウントがログオンに成功しました	ログオン/ログオフ：ネットワーク（SMB）ログオン。	ログオンおよびログオフ

529/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザ名が不明またはパスワードが無効です。	ログオンおよびログオフ
530/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：アカウントログオンの時間制限です。	ログオンおよびログオフ
531/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：アカウントは現在無効になっています。	ログオンおよびログオフ
532/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザアカウントの有効期限が切れています。	ログオンおよびログオフ
533/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザはこのコンピュータにログオンできません。	ログオンおよびログオフ
534/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザはログオンを許可されていません。	ログオンおよびログオフ
535/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：ユーザのパスワードが期限切れです。	ログオンおよびログオフ
537/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：上記以外の理由でログオンが失敗しました。	ログオンおよびログオフ
539/4625	アカウントがログオンに失敗しました	ログオン / ログオフ：アカウントのロックアウト。	ログオンおよびログオフ
538/4634	アカウントがログオフされました	ログオン / ログオフ：ローカルまたはネットワークユーザのログオフ。	ログオンおよびログオフ
560/4656	オブジェクトを開く / オブジェクトを作成	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）が開きます。	ファイルアクセス
563/4659.	削除するためにオブジェクトを開く	オブジェクトへのアクセス：削除するためにオブジェクト（ファイルまたはディレクトリ）へのハンドルが要求された。	ファイルアクセス
564 / 4660	オブジェクトを削除します	オブジェクトへのアクセス：オブジェクト（ファイルまたはディレクトリ）を削除します。ONTAP は、Windows クライアントがオブジェクト（ファイルまたはディレクトリ）の削除を試みるとこのイベントを生成します。	ファイルアクセス

567/4663	オブジェクトの読み取り / オブジェクトの書き込み / オブジェクトの属性の取得 / オブジェクトの属性の設定	オブジェクトへのアクセス：オブジェクトへのアクセスの試み（読み取り、書き込み、属性の取得、属性の設定）。 • 注： * このイベントでは、ONTAP はオブジェクトに対する最初の SMB 読み取り操作と SMB 書き込み操作（の成功または失敗）を監査します。これにより、 1 つのクライアントが、あるオブジェクトを開き、そのオブジェクトに対して連続的に多数の読み取りまたは書き込みを行っても、 ONTAP が余計にログエントリを書き込むことがなくなります。	ファイルアクセス
NA / 4664	ハードリンク	オブジェクトへのアクセス：ハードリンクの作成が試行されました。	ファイルアクセス
NA / 4818	提案された集約型アクセスポリシーでは、現在の集約型アクセスポリシーと同じアクセス権限が付与されません	オブジェクトへのアクセス：集約型アクセスポリシーのステージング。	ファイルアクセス
NA / NA Data ONTAP イベント ID 9999	オブジェクト名を変更します	オブジェクトへのアクセス：オブジェクトの名前変更。これは ONTAP イベントです。Windows では現在、単一イベントとしてサポートされていません。	ファイルアクセス
NA/NA Data ONTAP イベントID 9998	オブジェクトのリンク解除	オブジェクトへのアクセス：オブジェクトのリンクが解除される。これは ONTAP イベントです。Windows では現在、単一イベントとしてサポートされていません。	ファイルアクセス

イベント **4656** に関する追加情報

。 `HandleID` 監査でタグを付けます `XML` イベントには、アクセスされたオブジェクト（ファイルまたはディレクトリ）のハンドルが含まれます。。 `HandleID` EVTX 4656イベントのタグには、オープンイベントが新しいオブジェクトを作成するためのものか、既存のオブジェクトを開くためのものかによって、異なる情報が含まれます。

- openイベントが新しいオブジェクト（ファイルまたはディレクトリ）を作成するためのオープン要求である場合は、 `HandleID` 監査XMLイベントのタグに空が表示されます `HandleID` （例： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。

。 HandleID が空の理由は、（新しいオブジェクトを作成するための）OPEN要求が、実際のオブジェクトの作成が行われる前、およびハンドルが存在する前に監査されるためです。同じオブジェクトの後続の監査対象イベントは、で適切なオブジェクトハンドルを持ちます HandleID タグ。

- オープンイベントが既存のオブジェクトを開くためのオープン要求である場合、監査イベントには、でそのオブジェクトの割り当てられたハンドルが割り当てられます HandleID タグ（例： <Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data> ）。

監査対象オブジェクトへの完全なパスを決定します

に出力されたオブジェクトパス <ObjectName> 監査レコードのタグには、ボリュームの名前（かっこ内）と、そのボリュームを含むボリュームのルートからの相対パスが表示されます。ジャンクションパスを含む監査対象オブジェクトの完全パスを決定する場合には、実行する必要がある特定の手順があります。

手順

1. を参照して、ボリューム名と監査対象オブジェクトへの相対パスを確認します <ObjectName> 監査イベントのタグ。

   この例では、ボリューム名は「data1」で、ファイルへの相対パスはです /dir1/file.txt：

   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>

2. 前の手順で確認したボリューム名を使用して、監査対象オブジェクトが含まれているボリュームのジャンクションパスを確認します。

   この例では、ボリューム名は「data1」、監査対象オブジェクトが含まれるボリュームのジャンクションパスはです /data/data1：

   volume show -junction -volume data1

   ```
   
                                   Junction                     Junction
   Vserver   Volume       Language Active    Junction Path     Path Source
   --------- ------------ -------- --------  ----------------- -----------
   vs1       data1        en_US.UTF-8
                                   true      /data/data1       RW_volume
   ```

3. で見つかった相対パスを追加して、監査対象オブジェクトへの完全パスを決定します <ObjectName> ボリュームのジャンクションパスにタグを付けます。

   この例では、ボリュームのジャンクションパスは次のようになります。

   /data/data1/dir1/file.text

シンボリックリンクおよびハードリンクを監査する際の考慮事項

シンボリックリンクおよびハードリンクを監査する場合は、一定の考慮事項に注意する

必要があります。

監査レコードには、で識別される監査対象オブジェクトへのパスなど、監査対象オブジェクトに関する情報が含まれます `ObjectName` タグ。シンボリックリンクおよびハードリンクのパスがにどのように記録されるかを確認しておく必要があります `ObjectName` タグ。

シンボリックリンク

シンボリックリンクとは、ターゲットと呼ばれるデスティネーションオブジェクトの場所へのポインタを含む、独立した inode を持つファイルです。シンボリックリンクを介してオブジェクトにアクセスする際、ONTAP は、シンボリックリンクを自動的に解釈し、ボリューム内のターゲットオブジェクトへの、プロトコルに依存しない本来のパスに従います。

次の出力例には、2つのシンボリックリンクがあり、どちらもという名前のファイルを指しています `target.txt`。一方のシンボリックリンクは相対シンボリックリンクであり、他方は絶対シンボリックリンクです。どちらかのシンボリックリンクが監査された場合は、が実行されます `ObjectName` 監査イベントのタグにファイルへのパスが含まれています `target.txt`：

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

ハードリンク

ハードリンクは、ファイルシステム上の既存のファイルに名前を関連付けるディレクトリエントリです。ハードリンクは元のファイルの inode の場所を指しています。ONTAP ONTAP は、シンボリックリンクの解釈方法と同様に、ハードリンクを解釈し、ボリューム内のターゲットオブジェクトへの本来のパスに従います。ハードリンクオブジェクトへのアクセスが監査されると、監査イベントはこの正規の絶対パスをに記録します `ObjectName` ハードリンクパスではなくタグを付けます。

代替 **NTFS** データストリームを監査する際の考慮事項

NTFS 代替データストリームを持つファイルを監査する場合は、一定の考慮事項に注意する必要があります。

監査対象のオブジェクトの場所は、2つのタグ（）を使用してイベントレコードに記録されます `ObjectName` タグ（パス）および `HandleID` タグ（ハンドル）。ログに記録されるストリーム要求を適切に識別するには、 NTFS 代替データストリームでこれらのフィールドに記録される ONTAP レコードを把握しておく必要があります。

- EVTX ID ： 4656 のイベント（オープンおよび作成の監査イベント）
  - 代替データストリームのパスはに記録されます `ObjectName` タグ。
  - 代替データストリームのハンドルはに記録されます `HandleID` タグ。
- EVTX ID ： 4663 のイベント（読み取り、書き込み、属性の取得など、その他すべての監査イベント）

- 代替データストリームではなく、ベースファイルのパスがに記録されます `ObjectName` タグ。
- 代替データストリームのハンドルはに記録されます `HandleID` タグ。

例

次の例は、を使用して代替データストリームのEVTX ID：4663イベントを特定する方法を示しています `HandleID` タグ。にもかかわらず `ObjectName` 読み取り監査イベントで記録されるタグ（パス）は、ベースファイルパスであるへのパスです `HandleID` タグを使用すると、イベントを代替データストリームの監査レコードとして識別できます。

ストリームファイル名はの形式になります `base_file_name:stream_name`。この例では、を使用しています `dir1` ディレクトリには、次のパスを持つ代替データストリームを持つベースファイルが含まれています。

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

> 次のイベント例の出力はご覧のように省略されています。この出力にはイベントで使用可能なすべての出力タグが表示されているわけではありません。

EVTX ID 4656（オープン監査イベント）の場合、代替データストリームの監査レコード出力に代替データストリーム名が記録されます `ObjectName` タグ：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

EVTX ID 4663（読み取り監査イベント）の場合、同じ代替データストリームの監査レコード出力にベースファイル名が記録されます `ObjectName` タグ。ただし、のハンドル `HandleID` タグは代替データストリームのハンドルであり、このイベントを代替データストリームと関連付けるために使用できます。

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

監査できる NFS ファイルおよびディレクトリのアクセスイベント

ONTAP は、特定の NFS ファイルおよびディレクトリへのアクセスイベントを監査できます。どのようなアクセスイベントを監査できるか理解しておくと、変換された監査イベントログの結果を解釈するときに役立ちます。

次の NFS ファイルおよびディレクトリへのアクセスイベントを監査できます。

- 読み取り
- を開きます
- を閉じます
- ディレクトリの読み取り
- 書き込み
- 属性の設定
- 作成
- リンク
- 属性を開く（ OPENATTR ）
- 取り外します
- 属性の取得
- 確認します
- 非検証
- 名前を変更する

NFS の名前変更イベントを確実に監査するには、ファイルではなくディレクトリに監査 ACE を設定する必要があります。これは、ディレクトリへのアクセス権がある場合に、名前変更の操作でファイルのアクセス権が確認されないためです。

監査の設定を計画

Storage Virtual Machine （ SVM ）で監査を設定する前に、使用可能な設定オプションを理解し、各オプションに設定する値を計画する必要があります。この情報は、ビジネスニーズを満たす監査の設定に役立ちます。

すべての監査の設定に共通する設定パラメータがあります。

また、統合および変換された監査ログのローテーション時に使用する方法を指定するために使用できるパラメータもあります。監査の設定を行う際には、次の 3 つの方法のいずれかを指定できます。

- ログサイズに基づいてログをローテーションします

  ログのローテーションに使用されるデフォルトの方法です。

- スケジュールに基づいたログのローテーション
- ログのサイズとスケジュール（先にイベントが発生した方）に基づいてログのローテーションを実行 F

ログローテーションの方法を少なくとも 1 つ設定する必要があります。

すべての監査設定に共通するパラメータ

監査の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、指定できるオプションのパラメータが 3 つあります。

情報のタイプ	オプション	必須	含める	値を入力します
SVM 名 _ 監査の設定を作成する SVM の名前。SVM はすでに存在している必要があります。	`-vserver vserver_name`	はい。	はい。	

_ ログデスティネーションパス _ 変換された監査ログを格納するディレクトリを指定します。通常は専用のボリュームまたは qtree です。パスは SVM ネームスペースにすでに存在している必要があります。 パスには、最大 864 文字の文字列を指定できます。パスには読み取り / 書き込みアクセス権が必要です。 パスが有効でない場合、監査の設定コマンドは失敗します。 SVM が SVM ディザスタリカバリソースである場合、ログのデスティネーションパスをルートボリュームにすることはできません。これは、ルートボリュームのコンテンツがディザスタリカバリ先にレプリケートされないためです。 FlexCache ボリュームをログのデスティネーション（ ONTAP 9.7 以降）として使用することはできません。	`-destination text`	はい。	はい。	

_ 監査するイベントのカテゴリ _ 監査するイベントのカテゴリを指定します。監査できるイベントカテゴリは次のとおりです。 • ファイルアクセスイベント（ SMB と NFSv4 の両方） • SMBロクオンオヨヒログオフイヘント • 集約型アクセスポリシーのステージングイベント 集約型アクセスポリシーのステージングイベントは、Windows Server 2012 Active Directoryドメイン以降で使用できます。 • ファイル共有カテゴリイベント • ポリシー変更イベントの監査 • ローカルユーザアカウント管理イベント • セキュリティグループ管理イベント • 認証ポリシー変更イベント デフォルトでは、ファイルアクセスイベントとSMBログオンおよびログオフイベントが監査されます。 *注：*を指定する前に `cap-staging` イベントカテゴリとしては、SVMにSMBサーバが存在している必要があります。SMBサーバでダイナミックアクセス制御を有効にせずに、監査の設定で集約型アクセスポリシーのステージングを有効にすることはできますが、集約型アクセスポリシーのステージングイベントが生成されるのは、ダイナミックアクセス制御が有効になっている場合のみです。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。	`-events {file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change}`	いいえ

		_ ログファイル出力形式 _ 監査ログの出力形式を指定します。出力形式にはONTAP固有のものを指定できます XML またはMicrosoft Windows EVTX ログ形式。デフォルトの出力形式はです EVTX。	-format {xml	evtx}

いいえ			ログファイルのローテーションの上限 _ 保持する監査ログファイルの数を指定します。これにより、その数からあふれた最も古いログファイルがローテーションから外されます。たとえば、の値を入力した場合などです `5`では、最後の5つのログファイルが保持されます。 の値 `0` すべてのログファイルが保持されることを示します。デフォルト値は0です。	`-rotate-limit integer`

監査イベントログのローテーションをいつ行うかを決定するためのパラメータ

- ログサイズに基づいてログを回転 *

デフォルトでは、サイズに基づいた監査ログのローテーションが行われます。

- デフォルトのログサイズは 100MB です。

- 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、ログローテーションに関する特定のパラメータを設定する必要はありません。
- ログサイズのみに基づいて監査ログのローテーションを行う場合は、次のコマンドを使用しての設定を解除します `-rotate-schedule-minute` パラメータ： `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

デフォルトのログサイズを使用しない場合は、を設定できます `-rotate-size` カスタムログサイズを指定するパラメータ：

情報のタイプ	オプション	必須	含める	値を入力します
_ ログファイルサイズ制限 _ 監査ログファイルの最大サイズを指定します。	`-rotate-size` {`integer`[KB	MB	GB	TB

- スケジュールに基づいてログを回転 *

スケジュールに基づいた監査ログのローテーションを選択した場合は、時間に基づくローテーションパラメータを任意に組み合わせて使用することで、ログのローテーションをスケジュールすることができます。

- 時間に基づくローテーションを使用する場合は、 `-rotate-schedule-minute` パラメータは必須です。
- それ以外の時間ベースのローテーションパラメータは、すべてオプションです。
- ローテーションスケジュールは、時間に関連するすべての値を使用して計算されます。

  たとえば、のみを指定した場合 `-rotate-schedule-minute` パラメータを指定すると、監査ログファイルのローテーションは、毎月のすべての曜日の毎時間、指定した分に行われます。

- 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つだけ指定した場合（例： `-rotate-schedule -month` および `-rotate-schedule-minutes`）を指定すると、ログファイルのローテーションは、指定した月にのみ、すべての曜日の毎時間、指定した分に行われます。

  たとえば、監査ログのローテーションを、 1 月、 3 月、 8 月の毎週月曜日、水曜日、土曜日の 10 時 30 分に実行するように指定できます

- 両方に値を指定する場合は `-rotate-schedule-dayofweek` および `-rotate-schedule-day`では、これらは独立して考慮されます。

  たとえば、を指定した場合などです `-rotate-schedule-dayofweek` 金曜日およびとして `-rotate -schedule-day` 13と指定すると、監査ログのローテーションは、13日の金曜日だけでなく、毎週金曜日と指定した月の13日にも実行されます。

- スケジュールのみに基づいて監査ログのローテーションを行う場合は、次のコマンドを使用しての設定を解除します `-rotate-size` パラメータ： `vserver audit modify -vserver vs0 -destination / -rotate-size -`

次に示す使用可能な監査パラメータのリストを使用して、監査イベントログのローテーションのスケジュール設定に使用する値を決定できます。

情報のタイプ	オプション	必須	含める	値を入力します
ログローテーションスケジュール：Month_ 監査ログのローテーションを実行する月を指定します。 有効な値はです `January` から `December`および `all`。たとえば、監査ログのローテーションが 1 月、 3 月、 8 月に行われるように指定できます。	`-rotate-schedule-month chron_month`	いいえ		
ログローテーションスケジュール：曜日 _ 監査ログのローテーションを実行する日（曜日）を指定します。 有効な値はです `Sunday` から `Saturday`および `all`。たとえば、監査ログのローテーションを火曜日と金曜日に、またはすべての曜日に実行するように指定できます。	`-rotate-schedule -dayofweek chron_dayofweek`	いいえ		
ログローテーションスケジュール： Day _ 監査ログのローテーションを実行する日にちを指定します。 指定できる値の範囲は、です `1` から `31`。たとえば、監査ログのローテーションを毎月 10 日と 20 日に、またはすべての日に実行するように指定できます。	`-rotate-schedule-day chron_dayofmonth`	いいえ		
ログローテーションスケジュール： Hour _ 監査ログのローテーションを実行する時間を決めます。 指定できる値の範囲は、です `0` （午前0時）から `23` （午後11時）。を指定します `all` 監査ログのローテーションを1時間ごとに実行します。たとえば、監査ログのローテーションが 6 （午前 6 時）と 18 （午後 6 時）に行われるように指定できます。	`-rotate-schedule-hour chron_hour`	いいえ		

ログローテーションスケジュール：分 _ 監査ログのローテーションを実行する分を決めます。 指定できる値の範囲は、です `0` 終了：`59`。たとえば、監査ログのローテーションが 30 分に行われるように指定できます。	`-rotate-schedule-minute chron_minute`	スケジュールベースのログローテーションを設定している場合は Yes 、それ以外の場合は No にします		

- ログサイズとスケジュールに基づいてログを回転 *

両方のを設定すると、ログサイズとスケジュールに基づいてログファイルのローテーションを行うことができます `-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指定できます。例：if `-rotate-size` は10 MBに設定されており `-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10MBに達したとき、または1時間15分ごと（いずれか早い方）にログファイルがローテーションされます。

SVM 上にファイルとディレクトリの監査の設定を作成します

監査の設定を作成します

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作業には、使用可能な設定オプションの理解、設定の計画、設定の実行および有効化が含まれます。その後、監査の設定に関する情報を表示して、設定した内容が適切であることを確認できます。

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。

作業を開始する前に

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。

- SMB サーバでダイナミックアクセス制御を有効にせずに、監査の設定で集約型アクセスポリシーのステージングを有効にすることはできますが、集約型アクセスポリシーのステージングイベントが生成されるのは、ダイナミックアクセス制御が有効になっている場合のみです。

  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。

- コマンド内のフィールドの引数が無効な場合、たとえばフィールドの無効なエントリ、重複するエントリ、存在しないエントリなどが考えられます。その場合、監査フェーズの前にコマンドが失敗します。

  この場合、監査レコードは生成されません。

このタスクについて

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。ログの形式はです `EVTX` （デフォルト）。ログはに保存されます `/audit_log` ディレクトリ。ログファイルの最大サイズはです `200 MB`。ログのサイズが 200MB になると、ログのローテーションが実行されます。

```
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。ログの形式はです `EVTX` （デフォルト）。ログはに保存されます `/cifs_event_logs` ディレクトリ。ログファイルの最大サイズはです `100 MB` （デフォルト）。ログのローテーションの上限はです `5`：

```
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 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。ログの形式はです `EVTX` （デフォルト）。監査ログのローテーションが毎月、午後 12 時 30 分に実行されますそして毎日、午後 12 ： 30 に実行されます。ログのローテーションの上限はです `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
```

SVM で監査を有効にします

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。

必要なもの

SVM の監査設定がすでに存在している必要があります。

このタスクについて

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。

ステップ

1. SVM で監査を有効にします。

   ```
   vserver audit enable -vserver vserver_name
   ```

   ```
   vserver audit enable -vserver vs1
   ```

監査の設定を確認します

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の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
   ```

ファイルおよびフォルダの監査ポリシーを設定

ファイルおよびフォルダの監査ポリシーを設定

ファイルおよびフォルダのアクセスイベントの監査は、 2 つのステップで実装します。まず、 Storage Virtual Machine （ SVM ）で監査設定を作成し、有効にする必要があります。次に、監視するファイルとフォルダに対して監査ポリシーを設定する必要があります。成功したアクセス試行と失敗したアクセス試行の両方を監視するように監査ポリシーを設定できます。

SMB と NFS の両方の監査ポリシーを設定できます。SMB と NFS の監査ポリシーでは、設定の要件や監査の機能が異なります。

適切な監査ポリシーが設定されている場合、 ONTAP は、 SMB または NFS サーバの稼働中に限り、監査ポリシーでの指定に従って SMB および NFS アクセスイベントを監視します。

NTFS セキュリティ形式のファイルおよびディレクトリに監査ポリシーを設定する

ファイルおよびディレクトリ操作を監査する前に、監査情報を収集するファイルおよびディレクトリに対して監査ポリシーを設定する必要があります。これは、監査の設定と有効化に加えて行います。NTFS 監査ポリシーを設定するには、 Windows のセキュリティタブを使用するか、 ONTAP の CLI を使用します。

Windows のセキュリティタブを使用した NTFS 監査ポリシーの設定

Windows の [プロパティ] ウィンドウの [Windows セキュリティ *] タブを使用して、ファイルおよびディレクトリの NTFS 監査ポリシーを構成できます。これは Windows クライアント上に存在するデータの監査ポリシーを設定する場合と同じ方法であり、ユーザは使い慣れたものと同じ GUI インターフェイスを使用できます。

必要なもの

監査は、 System Access Control List （ SACL ；システムアクセス制御リスト）を適用するデータが格納されている Storage Virtual Machine （ SVM ）で設定する必要があります。

このタスクについて

NTFS 監査ポリシーの設定は、 NTFS セキュリティ記述子に関連付けられている NTFS SACL にエントリを追加することによって行います。その後、セキュリティ記述子を NTFS ファイルおよびディレクトリに適用します。これらのタスクは Windows GUI によって自動的に処理されます。セキュリティ記述子には、ファイルやフォルダのアクセス権を適用するための Discretionary Access Control List （ DACL ；随意アクセス制御リスト）、ファイルやフォルダを監査するための SACL 、または SACL と DACL の両方を含めることができます。

Windows のセキュリティタブを使用して NTFS 監査ポリシーを設定するには、 Windows ホストで次の手順を実行します。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
2. [ネットワークドライブの割り当て *] ボックスに入力します。

   a. ドライブ文字を選択します。

   b. [* フォルダ *] ボックスに、監査するデータと共有名を保持して、共有を含む SMB サーバー名を入力します。

      SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

      SMBサーバ名が「smb_server」で、共有の名前が「share1」の場合は、と入力します `\\SMB_SERVER\share1`。

   c. [完了] をクリックします。

   選択したドライブがマウントされて使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

3. アクセスの監査を有効にするファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。

5. [* セキュリティ *] タブを選択します。
6. 「 * 詳細設定 * 」をクリックします。
7. [監査 *] タブを選択します。
8. 次のうち必要な操作を実行します。

状況	実行する処理
新しいユーザまたはグループの監査を設定します	a. [追加（ Add ）] をクリックします。 b. [選択するオブジェクト名を入力してください] ボックスに、追加するユーザーまたはグループの名前を入力します。 c. [OK] をクリックします。
ユーザまたはグループから監査を削除します	a. [選択するオブジェクト名を入力してください] ボックスで、削除するユーザーまたはグループを選択します。 b. [削除（ Remove ）] をクリックします。 c. [OK] をクリックします。 d. この手順の残りの部分はスキップします。
ユーザまたはグループの監査を変更します	a. [選択するオブジェクト名を入力してください] ボックスで、変更するユーザーまたはグループを選択します。 b. [編集（ Edit ）] をクリックします。 c. [OK] をクリックします。

ユーザーまたはグループの監査を設定したり、既存のユーザーまたはグループの監査を変更したりする場合は、 [< オブジェクト > の監査エントリ] ボックスが開きます。

9. [* 適用先 *] ボックスで、この監査エントリの適用方法を選択します。

   次のいずれかを選択できます。

   - * このフォルダ、サブフォルダ、ファイル *
   - * このフォルダとサブフォルダ *
   - * このフォルダのみ *
   - * このフォルダとファイル *
   - * サブフォルダとファイルのみ *
   - * サブフォルダのみ *
   - ファイルのみ 単一ファイルに対して監査を設定している場合、*適用先*ボックスはアクティブになりません。[* 適用先 * （ Apply to * ）] ボックスの設定は、デフォルトで * このオブジェクトのみ * に設定されています。

   監査では SVM リソースが使用されるので、セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。

10. [* アクセス *] ボックスで、監査する対象と、成功したイベント、失敗イベント、またはその両方を監査するかどうかを選択します。
    - 成功したイベントを監査するには、成功ボックスを選択します。
    - 障害イベントを監査するには、 [障害] ボックスを選択します。

      セキュリティ要件を満たすために監視する必要がある操作のみを選択してください。これらの監査可能なイベントの詳細については、 Windows のマニュアルを参照してください。次のイベントを監査できます。

    - * フルコントロール *
    - * フォルダの移動 / ファイルの実行 *
    - * フォルダのリスト / データの読み取り *
    - * 属性の読み取り *
    - * 拡張属性の読み取り *
    - * ファイルの作成 / データの書き込み *
    - * フォルダの作成 / データの追加 *
    - * 属性の書き込み *
    - * 拡張属性の書き込み *
    - * サブフォルダとファイルの削除 *
    - * 削除 *
    - * 読み取り許可 *
    - * 権限の変更 *
    - * 所有権を取りなさい *
11. 監査設定を元のコンテナの後続のファイルとフォルダに反映させない場合は、 [このコンテナ内のオブジェクトまたはコンテナにのみ監査エントリを適用する *] ボックスを選択します。
12. [適用（ Apply ）] をクリックします。
13. 監査エントリの追加、削除、または編集が完了したら、 **OK** をクリックします。

    [Auditing Entry for <object>] ボックスが閉じます。

14. [監査 *] ボックスで、このフォルダの継承設定を選択します。

    セキュリティ要件を満たす監査イベントにするために必要な最小レベルを選択してください。次のいずれかを選択できます。

    - このオブジェクトの親から継承可能な監査エントリを含めるボックスを選択します
    - [このオブジェクトから継承可能な監査エントリをすべての子の既存の継承可能な監査エントリをすべて置換する] ボックスをオンにします
    - 両方のボックスを選択します。
    - どちらのボックスも選択しない。 1 つのファイルに SACL を設定する場合は '[このオブジェクトから継承可能な監査エントリをすべての子の既存のすべての監査エントリを置換] ボックスが [監査] ボックスに表示されません

15. [OK] をクリックします。

    [監査] ボックスが閉じます。

ONTAP CLI を使用して **NTFS** 監査ポリシーを設定する

ONTAP CLI を使用して、ファイルおよびフォルダに対して監査ポリシーを設定できます。これにより、Windows クライアントで SMB 共有を使用してデータに接続することなく NTFS 監査ポリシーを設定できます。

を使用してNTFS監査ポリシーを設定できます `vserver security file-directory` コマンドファミリー。

CLI で設定できるのは NTFS SACL だけです。NFSv4 SACL の設定は、この ONTAP コマンドファミリーではサポートされていません。これらのコマンドを使用して NTFS SACL を設定し、ファイルおよびフォルダに追加する方法については、マニュアルページを参照してください。

UNIX セキュリティ形式のファイルおよびディレクトリの監査を設定します

UNIX セキュリティ形式のファイルおよびディレクトリの監査を設定するには、NFSv4.x ACL に監査 ACE を追加します。これにより、セキュリティの目的で特定の NFS ファイルおよびディレクトリのアクセスイベントを監視できます。

このタスクについて

NFSv4.x では、随意 ACE とシステム ACE の両方が同じ ACL に格納されます。個別の DACL と SACL には格納されません。したがって、既存の ACL に監査 ACE を追加する場合は、既存の ACL を上書きして失われることがないように、細心の注意を払う必要があります。既存の ACL に監査 ACE を追加する順序は重要ではありません。

手順

1. を使用して、ファイルまたはディレクトリの既存のACLを取得します `nfs4_getfacl` または同等のコマンド。

   ACL の操作の詳細については、 NFS クライアントのマニュアルページを参照してください。

2. 目的の監査 ACE を追加します。
3. を使用して、更新したACLをファイルまたはディレクトリに適用します `nfs4_setfacl` または同等のコマンド。

ファイルおよびディレクトリに適用されている監査ポリシーに関する情報を表示します

Windows のセキュリティタブを使用して、監査ポリシーに関する情報を表示します

Windows のプロパティウィンドウのセキュリティタブを使用して、ファイルおよびディレクトリに適用されている監査ポリシーに関する情報を表示できます。これは Windows サーバ上に存在するデータの場合と同じ方法であり、ユーザは使い慣れたものと同じ GUI インターフェイスを使用できます。

このタスクについて

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なシステムアクセス制御リスト（ SACL ）が設定されていることを確認できます。

NTFS ファイルおよびフォルダに適用されている SACL に関する情報を表示するには、 Windows ホストで次の手順を実行します。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
2. [* ネットワークドライブの割り当て *] ダイアログボックスに入力します。

   a. ドライブ文字を選択します。

   b. [フォルダ]ボックスに、監査するデータが格納されている共有を含むStorage Virtual Machine（SVM）のIPアドレスまたはSMBサーバ名と、共有の名前を入力します。

      SMBサーバ名が「smb_server」で、共有の名前が「share1」の場合は、と入力します `\\SMB_SERVER\share1`。

      > SMBサーバ名の代わりに、SMBサーバのデータインターフェイスのIPアドレスを指定できます。

   c. [完了] をクリックします。

   選択したドライブがマウントされて使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

3. 監査情報を表示するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。
5. [* セキュリティ *] タブを選択します。
6. 「 * 詳細設定 * 」をクリックします。
7. [監査 *] タブを選択します。
8. [* Continue （続行）] をクリックします

   [監査] ボックスが開きます。[監査エントリ *] ボックスには、 SACL が適用されているユーザーとグループの概要が表示されます。

9. [* 監査エントリ *] ボックスで、 SACL エントリを表示するユーザーまたはグループを選択します。
10. [編集（ Edit ）] をクリックします。

    [< オブジェクト > の監査エントリ] ボックスが開きます。

11. [* アクセス * （ * Access * ）] ボックスで、選択したオブジェクトに適用されている現在の SACL を表示します。
12. [* キャンセル *] をクリックして、 [* 監査エントリ for < オブジェクト >*] ボックスを閉じます。
13. [* キャンセル *] をクリックして、 [* 監査 *] ボックスを閉じます。

CLI を使用して、 FlexVol の NTFS 監査ポリシーに関する情報を表示する

セキュリティ形式と有効なセキュリティ形式、適用されているアクセス権、システムアクセス制御リストに関する情報など、 FlexVol の NTFS 監査ポリシーに関する情報を表示できます。この情報を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

このタスクについて

ファイルやディレクトリに適用されている監査ポリシーに関する情報を表示すると、指定したファイルやフォルダに適切なシステムアクセス制御リスト（ SACL ）が設定されていることを確認できます。

Storage Virtual Machine （ SVM ）の名前、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、 NTFS のシステムアクセス制御リスト（ SACL ）のみが監査ポリシーに使用されます。
- NTFS 対応のセキュリティが有効な mixed セキュリティ形式のボリューム内のファイルおよびフォルダには、 NTFS 監査ポリシーを適用できます。

  mixed セキュリティ形式のボリュームおよび qtree には、 UNIX ファイル権限、モードビットまたは NFSv4 ACL 、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- mixed セキュリティ形式のボリュームの最上位では、 UNIX または NTFS 対応のセキュリティを有効にすることができ、そこには NTFS SACL が格納されている場合も、格納されていない場合もあります。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、 mixed セキュリティ形式のボリュームまたは qtree で設定できるため、 ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、通常のファイルおよびフォルダの NFSv4 SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- コマンドで入力したパスが、 NTFS 対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。
- NTFS 対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報を表示する場合、 UNIX 関連の出力フィールドには表示専用の UNIX ファイル権限情報が格納されます。

  ファイルアクセス権の決定時、 NTFS セキュリティ形式のファイルおよびフォルダでは、 NTFS ファイルアクセス権と Windows ユーザおよびグループのみが使用されます。

- ACL 出力は、 NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットのアクセス権のみ（ NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、 NTFS セキュリティ記述子の場合にのみ適用されます。

ステップ

1. ファイルおよびディレクトリ監査ポリシー設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細なリストとして	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、パスの監査ポリシーの情報を表示します `/corp` （SVM vs1）。パスで NTFS 対応のセキュリティが有効になっています。NTFS セキュリティ記述子には、 SUCCESS および SUCCESS/FAIL SACL エントリの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

次の例は、パスの監査ポリシーの情報を表示します `/datavol1` （SVM vs1）。このパスには、標準ファイルおよびフォルダの SACL とストレージレベルのアクセス保護の SACL の両方が格納されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ファイルセキュリティと監査ポリシーに関する情報を表示する方法

ワイルドカード文字（ * ）を使用すると、特定のパスまたはルートボリュームの下にあるすべてのファイルおよびディレクトリのファイルセキュリティと監査ポリシーに関す

る情報を表示できます。

ワイルドカード文字（ * ）は、すべてのファイルおよびディレクトリの情報を表示する特定のディレクトリパスの最後のサブコンポーネントとして使用できます。

という名前の特定のファイルまたはディレクトリの情報を表示する場合は、パス全体を二重引用符（ "" ）で囲む必要があります。

例

次のコマンドにワイルドカード文字を指定すると、パスの下にあるすべてのファイルとディレクトリに関する情報が表示されます `/1/` SVM vs1：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

次のコマンドは、パスの下に「*」という名前のファイルの情報を表示します `/vol1/a` SVM vs1の。パスは二重引用符（ "" ）で囲まれます。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                  Vserver: vs1
                File Path: “/vol1/a/*”
           Security Style: mixed
          Effective Style: unix
           DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
             Unix User Id: 1002
            Unix Group Id: 65533
           Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

監査できる **CLI** 変更イベント

監査可能な **CLI** 変更イベントの概要

ONTAP は、特定の SMB 共有イベント、監査ポリシーイベント、ローカルセキュリティグループイベント、ローカルユーザグループイベント、認証ポリシーイベントなどの CLI 変更イベントを監査できます。どのような変更イベントを監査できるか理解しておくと、イベントログの結果を解釈するときに役立ちます。

Storage Virtual Machine （ SVM ）で監査する CLI 変更イベントの管理作業として、手動での監査ログのローテーション、監査の有効化と無効化、監査対象変更イベントに関する情報の表示、監査対象変更イベントの変更、監査対象変更イベントの削除が可能です。

管理者が、 SMB 共有、ローカルユーザグループ、ローカルセキュリティグループ、認証ポリシー、および監査ポリシーのイベントに関連する設定を変更するコマンドを実行する場合、 レコードが生成され、対応するイベントが監査されます。

監査カテゴリ	イベント	イベント IDs	実行するコマンド
Mhost 監査	ポリシー変更	[4719] 監査設定が変更されました	`vserver audit disable

enable	modify`	ファイル共有	[5142] ネットワーク共有が追加されました
`vserver cifs share create`	[5143] ネットワーク共有の変更	`vserver cifs share modify` `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] ネットワーク共有が削除されました	`vserver cifs share delete`
監査	ユーザアカウント	[4720] ローカルユーザの作成	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] ローカルユーザの有効化	`vserver cifs users-and-groups local-user create	modify`	[4724] ローカルユーザのパスワードのリセット
`vserver cifs users-and-groups local-user set-password`	[4725] ローカルユーザの無効化	`vserver cifs users-and-groups local-user create	modify`
[4726] ローカルユーザの削除	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] ローカルユーザの変更	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] ローカルユーザの名前変更	`vserver cifs users-and-groups local-user rename`	セキュリティグループ	[4731] ローカルセキュリティグループが作成されました
`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`	[4734] ローカルセキュリティグループが削除されました	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`	[4735] ローカルセキュリティグループの変更

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] ローカルグループへのユーザの追加	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
[4733] ローカルグループからユーザが削除されました	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`	認証ポリシー変更	[4704] ユーザ権限の割り当て
`vserver cifs users-and-groups privilege add-privilege`	[4705] ユーザ権限が削除されました	`vserver cifs users-and-groups privilege remove-privilege	reset-privilege`

ファイル共有イベントの管理

Storage Virtual Machine （ SVM ）に対してファイル共有イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。ファイル共有イベントは、を使用してSMBネットワーク共有が変更された場合に生成されます `vserver cifs share` 関連コマンド。

ファイル共有イベントは、SVMに対してSMBネットワーク共有が追加、変更、または削除されたときに生成されます。イベントIDは5142、5143、および5144です。SMBネットワーク共有の設定はを使用して変更します `cifs share access control create|modify|delete` コマンド

次の例では、「 audit_dest 」という名前の共有オブジェクトが作成され、 ID 5143 のファイル共有イベントが生成されています。

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

監査ポリシー変更イベントの管理

Storage Virtual Machine （ SVM ）に対して監査ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。監査ポリシー変更イベントは、を使用して監査ポリシーが変更されたときに生成されます `vserver audit` 関連コマンド。

監査ポリシー変更イベントは、監査ポリシーが無効化、有効化、または変更されたときに生成されます。イベント ID は 4719 です。このイベントは、ユーザが監査を無効にしようとしたときに状況を追跡するのに役立ちます。このイベントはデフォルトで設定されており、無効にするには diagnostic 権限が必要です。

次の例では、監査が無効になったときに、 ID 4719 の監査ポリシー変更イベントが生成されています。

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

ユーザアカウントイベントを管理します

Storage Virtual Machine （ SVM ）に対してユーザアカウントイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

イベントID 4720、4722、4724、4725、4726のユーザアカウントイベント 4738および4781は、ローカルSMBまたはNFSユーザがシステムから作成または削除されたとき、ローカルユーザアカウントが有効化、無効化または変更されたとき、ローカルSMBユーザパスワードがリセットまたは変更されたときに生成されます。ユーザアカウントイベントは、を使用してユーザアカウントが変更されたときに生成されます `vserver cifs users-and-groups <local user>` および `vserver services name-service <unix user>` コマンド

次の例では、ローカルSMBユーザが作成され、ID 4720のユーザアカウントイベントが生成されています。

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

次の例では、上記の例で作成されたローカルSMBユーザの名前が変更され、ID 4781のユーザアカウントイベントが生成されています。

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

セキュリティグループイベントの管理

Storage Virtual Machine （ SVM ）に対してセキュリティグループイベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

セキュリティグループイベントは、システムのローカル SMB グループまたは NFS グループが作成または削除されたとき、それらのグループのローカルユーザが追加または削除されたときに生成されます。イベント ID は 4731 、 4732 、 4733 、 4734 、および 4735 です。セキュリティグループイベントは、を使用してユーザアカウントが変更された場合に生成されます `vserver cifs users-and-groups <local-group>` および `vserver services name-service <unix-group>` コマンド

次の例では、ローカル UNIX セキュリティグループが作成され、 ID 4731 のセキュリティグループイベントが生成されています。

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

認証ポリシー変更イベントを管理します

Storage Virtual Machine （ SVM ）に対して認証ポリシー変更イベントが設定されている場合、監査を有効にしたときに、それらについての監査イベントが生成されます。

認証ポリシー変更イベントは、 SMB ユーザおよび SMB グループに対する認証権限が付与または取り消されたときに生成されます。イベント ID は 4704 および 4705 です。認証ポリシー変更イベントは、を使用して認証権限が割り当てられた場合または取り消された場合に生成されます `vserver cifs users-and-groups privilege` 関連コマンド。

次の例では、SMBユーザグループの認証権限が割り当てられている場合に、ID 4704の認証ポリシーイベントが生成されています。

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

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。

監査およびステージング用のボリュームのスペースに関する問題のトラブルシューティングを行います

ステージングボリュームや監査イベントログを格納するボリュームに十分なスペースがない場合、問題が発生することがあります。十分なスペースがないと新しい監査レコードを作成できないため、クライアントからデータにアクセスできず、アクセス要求が失敗します。ボリュームのスペースに関するこれらの問題について、トラブルシューティングを行って解決する方法を確認しておく必要があります。

イベントログボリュームに関連するスペースの問題のトラブルシューティングを行います

イベントログファイルを含むボリュームでスペースが不足すると、監査でログレコードをログファイルに変換できなくなります。その結果、クライアントアクセスに失敗します。イベントログボリュームのスペースに関する問題のトラブルシューティング方法を把握しておく必要があります。

- Storage Virtual Machine （ SVM ）管理者およびクラスタ管理者は、ボリュームとアグリゲートの使用量と設定に関する情報を表示して、ボリュームでスペースが不足していないかを確認できます。
- イベントログを含むボリュームでスペースが不足している場合、 SVM 管理者およびクラスタ管理者は、いくつかのイベントログファイルを削除するかボリュームのサイズを大きくすることで、スペースに関する問題を解決できます。

> イベントログボリュームを含むアグリゲートがいっぱいになっている場合は、ボリュームのサイズを大きくする前に、アグリゲートのサイズを大きくする必要があります。アグリゲートのサイズを大きくすることができるのは、クラスタ管理者だけです。

- 監査の設定を変更して、イベントログファイルのデスティネーションパスを別のボリューム上のディレクトリに変更できます。

> 次の場合、データアクセスは拒否されます。
>
> - デスティネーションディレクトリが削除されている場合。
> - デスティネーションディレクトリをホストするボリュームのファイルリミットが最大レベルに達している場合。

詳細情報：

- "ボリュームに関する情報の表示方法とボリュームサイズの拡張方法"。
- "アグリゲートに関する情報の表示方法とアグリゲートの管理方法"。

ステージングボリュームに関するスペースの問題のトラブルシューティングを行います

Storage Virtual Machine （ SVM ）のステージングファイルを含むボリュームのいずれかでスペースが不足すると、監査でログレコードをステージングファイルに書き込むことができなくなります。その結果、クライア

ントアクセスに失敗します。この問題のトラブルシューティングを行うには、ボリュームの使用量に関する情報を表示して、 SVM で使用されているステージングボリュームのいずれかがいっぱいになっていないかを確認する必要があります。

統合イベントログファイルを含むボリュームに十分なスペースがあるにもかかわらず、スペース不足が原因でクライアントアクセスに失敗する場合は、ステージングボリュームでスペースが不足している可能性があります。SVM 管理者は、クラスタ管理者に問い合わせて、 SVM のステージングファイルを含むステージングボリュームでスペースが不足していないかを確認する必要があります。ステージングボリュームのスペース不足が原因で監査イベントを生成できない場合は、監査サブシステムによって EMS イベントが生成されます。次のメッセージが表示されます。 `No space left on device`。ステージングボリュームに関する情報を表示できるのは、クラスタ管理者だけです。 SVM 管理者はこの操作を実行できません

すべてのステージングボリューム名はで始まります `MDV_aud_` そのあとに、ステージングボリュームを含むアグリゲートのUUIDが続きます。次に、管理 SVM 上にある 4 個のシステムボリュームの例を示します。これらのボリュームは、クラスタ内でデータ SVM のファイルサービスの監査の設定の作成時に自動的に作成されたものです。

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

ステージングボリュームでスペースが不足している場合は、ボリュームのサイズを大きくすることで、スペースに関する問題を解決できます。

> ステージングボリュームを含むアグリゲートがいっぱいになっている場合は、ボリュームのサイズを大きくする前に、アグリゲートのサイズを大きくする必要があります。アグリゲートのサイズを拡張できるのは、クラスタ管理者だけです。 SVM 管理者はこの操作を行うことができません

使用可能なスペースが 2GB 未満のアグリゲートがあると、 SVM の監査の作成に失敗します。SVM の監査の作成に失敗した場合、作成されたステージングボリュームは削除されます。