SVMでのNASイベントの監査

ONTAP 9

NetApp
February 12, 2026

目次

SVMでのNASイベントの監査

SMB プロトコルと NFS プロトコルの両方で ONTAP を使用してファイル アクセスを監査する方法について説明します。

SMBプロトコルとNFSプロトコルに対応したファイル アクセス監査機能（標準の監査、FPolicyを使用したファイル ポリシー管理など）をONTAPで使用することができます。

SMBおよびNFSのファイル アクセス イベントの監査の設計と実装は、次のような状況で行うことを想定しています。

- SMBプロトコルおよび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。
- 監査設定を次のいずれかの方法で作成して管理する。
  - ONTAPの標準機能
  - 外部FPolicyサーバ

SVMでのNASイベントの監査

NASイベントの監査はセキュリティ対策の1つで、Storage Virtual Machine（SVM）上の特定のSMBおよびNFSイベントを追跡してログに記録することができます。潜在的なセキュリティの問題を追跡するのに役立つほか、セキュリティ違反が発生した場合の証拠にもなります。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を使用すれば、実際に実施した場合の結果を予想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 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上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ログオンおよびログオフ イベント

  SVM上にある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たSMBサーバ上のオブジェクトへ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（DAC）を有効にしていなくても監査設定では集約型アクセス

ポリシー ステージングを有効にすることができますが、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しか生成されません。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 イベントおよびディレクトリのイベントを監査するには、SVM上に格納されているオブジェクト対してNFSv4 ACLを使用します。

監査の仕組み

ONTAP監査の基本的な概念を学ぶ

ONTAPでの監査を理解するには、いくつかの基本的な監査の概念を知っておく必要があります。

- ステージングファイル

  統合および変換前の監査レコードが保存される、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

  ONTAPがステージングファイルを保存するために作成する専用ボリュームです。ステージングボリュームは、アグリゲートごとに1つ存在します。ステージングボリュームは、監査が有効なすべてのStorage Virtual Machine（SVM）によって共有され、その特定のアグリゲート内のデータボリュームのデータアクセスに関する監査レコードを保存します。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保存されます。

  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、その他のボリューム操作のほとんどは許可されていません。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はステージングボリュームに自動的に名前を割り当てます。すべてのステージングボリューム名は`MDV_aud_`で始まり、その後にその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（例：`MDV_aud_1d0131843d4811e296fc123478563412`）。

- システムボリューム

  ファイルサービス監査ログのメタデータなど、特別なメタデータを含むFlexVolボリューム。管理SVMはシステムボリュームを所有し、クラスタ全体で参照可能です。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

  監査が有効化されると作成されるタスクです。各SVM上で実行されるこの長時間実行タスクは、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、監査レコードを時系列順にマージし、監査設定で指定されたユーザーが判読可能なイベントログ形式（EVTXまたはXMLファイル形式）に変換します。変換されたイベントログは、SVM監査設定で指定された監査イベントログディレクトリに保存されます。

ONTAP監査プロセスの機能について学習します

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にパスとして既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ための新しいボリュームまたはqtreeを作成することをお勧めします。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。監査設定で指定されたログディレクトリのパスが有効なパスでない場合、監査設定の作成は `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"`エラーで失敗します。

  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、構成の作成は失敗します。

- 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たあと、監査が有効になります。SVMの監査設定とログ 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た場合も維持されます。

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）はすべて記録されます。要求されたファイル処理は、その処理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ディスクのステージング ファイルにコミットできない場合、クライアント処理は拒否されます。

管理者、または特権レベルのアクセス権を持つアカウントユーザーは、NetApp Manageability SDKまたはREST APIを使用して、ファイル監査ログ操作をバイパスできます。NetApp Manageability SDKまたはREST APIを使用してファイル操作が実行されたかどうかは、`audit.log`ファイルに保存されているコマンド履歴ログを確認することで判断できます。

コマンド履歴監査ログの詳細については、"システム管理"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。

ノードが利用できない場合の統合処理

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、ノードから最後にレポート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。

  ノードにアクセスできない場合、統合タスクは、そのSVMの他の利用可能なノードからの監査レコードを統合します。統合が完了していないことを示すため、タスクはサフィックス `.partial`を統合ファイル名に追加します。

- 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に、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の監査設定を無効にしても、監査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。ユーザが監査の統合ジョブを削除することはできません。

ONTAP監査の前提条件

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。

- NFS および S3 監査対応 SVM の合計制限は ONTAP のバージョンによって異なります：

ONTAPのバージョン	最大
9.8以前	50
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。

  SMBとNFSのライセンスがクラスタに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、監査設定を作成するコマンドは失敗します。

- 監査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。

    相対パスを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。

  イベントログを保存するために使用するボリュームに十分な空き容量があることを認識し、その確保のための計画を立てておく必要があります。監査設定を作成する際に `-rotate-limit`パラメータを使用して、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。これにより、ボリューム内にイベントログ用の十分な空き容量を確保できます。

- 監査設定では、SMBサーバでDynamic Access Control（DAC;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しておく必要があります。

  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。

監査を有効化する場合のアグリゲート スペースの考慮事項

監査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。監査を構成しても、既存のアグリゲートにステージング ボリュームの格納に必要な空き容量がない場合に、このエラーが起きることがあります。

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空き容量があることを確認する必要があります。

ONTAP監査レコードのステージングファイルのサイズ制限

ステージング ファイルの監査レコードのサイズは最大32KBです。

監査レコードが肥大化する状況

監査レコードの肥大化は、管理監査における次のシナリオでおきる可能性があります。

- 多数のユーザで構成されるグループに対するユーザの追加または削除。
- 多数のユーザが共有するファイル共有に対するアクセス制御リスト（ACL）の追加または削除。
- その他のシナリオ。

この問題を回避するには、管理の監査を無効にしてください。これを行うには、監査の設定を変更し、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
- ユーザーアカウント
- セキュリティグループ
- 承認ポリシーの変更

  削除した項目はファイル サービスの監査サブシステムで監査されなくなります。

監査レコードの肥大化による影響

- 監査レコードが肥大化（32KB超）すると、監査レコードは作成されなくなり、監査サブシステムによって次のようなイベント管理システム（EMS）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、監査レコードを作成できないため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バイトを超えると、上記と同じEMSメッセージが表示されます。監査レコ

ードは作成されますが、大きなキー値は省略されます。

- 監査レコードが2,000文字を超える場合、実際の値の代わりに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.`

ONTAP監査イベントログでサポートされている形式について学習します

変換された監査イベント ログでサポートされているファイル形式は、 `EVTX`および`XML`のファイル形式です。

監査設定を作成する際に、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`EVTX`ファイル形式に変換します。

ONTAP監査イベントログの表示と処理

監査イベント ログを使用すると、ファイルのセキュリティが適切かどうか、またファイルやフォルダへの不適切なアクセス試行があったかどうかを判断できます。 `EVTX`または `XML`ファイル形式で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` ファイル形式

  変換された `EVTX`監査イベント ログは、Microsoft Event Viewer を使用して保存されたファイルとして開くことができます。

  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2つのオプションがあります。

  - 全般表示

    イベント レコードに対し、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。詳細表示を使用すると、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表示が利用できます。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

  > `XML`監査イベント ログは、`XML`ファイル形式をサポートするサードパーティ製アプリケーションで表示および処理できます。`XML` スキーマと `XML` フィールドの定義情報があれば、`XML` 表示ツールを使用して監査ログを表示できます。`XML` スキーマと定義の詳細については、`https://library.netapp.com/ecm/ecm_get_file/ECMLP2875022["ONTAP 監査スキーマ リファレンス"]`を参照してください。

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でき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、新たに追加されたレコードをイベント ビューアで表示できるかどうかが異なります。

共有のOplocks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。更新操作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。更新操作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 `EVTX`イベント ログにのみ適用されます。 `XML`イベント ログは、ブラウザで SMB 経由で、または任意の XML エディタまたはビューアを使用して NFS 経由で表示できます。

監査できる**SMB**イベント

ONTAPが監査して結果を解釈できる**SMB**イベントについて学習します

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。

次の追加の SMB イベントを監査できます：

イベント ID（EVT/EVTX）	イベント	概要	カテゴリ
4670	オブジェクト権限の変更	オブジェクト アクセス：権限が変更されました。	ファイル アクセス
4907	オブジェクトの監査設定の変更	オブジェクト アクセス：監査設定が変更されました。	ファイル アクセス
4913	オブジェクトの集約型アクセス ポリシーの変更	オブジェクト アクセス：CAP が変更されました。	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	概要	カテゴリ
540/4624	アカウントがログオンに成功	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	ログオン/ログオフ：ユーザー名が不明であるか、パスワードが間違っています。	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	ログオン/ログオフ：アカウントのログオン時間の制限。	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	LOGON/LOGOFF：アカウントは現在無効です。	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	ログオン/ログオフ：ユーザー 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	ログオン/ログオフ：ユーザーはこのコンピューター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	ログオン/ログオフ：ここではユーザーにログオン タイプが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	ログオン/ログオフ：ユーザーのパスワードの有効期限が切れています。	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	LOGON/LOGOFF：上記以外の理由によりログオンに失敗しました。	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	ログオン/ログオフ：アカウントがロックアウトされています。	ログオンおよびログオフ
538/4634	アカウントがログオフ	ログオン/ログオフ：ローカルまたはネットワーク ユーザーのログオフ。	ログオンおよびログオフ
560/4656	オブジェクトのオープン / オブジェクトの作成	オブジェクト アクセス：オブジェクト（ファイルまたはディレクトリ）が開いています。	ファイル アクセス

563/4659	削除するためのオブジェクトのオープン	オブジェクト アクセス：削除の意図を持ってオブジェクト（ファイルまたはディレクトリ）へのハンドルが要求されました。	ファイル アクセス
564/4660	オブジェクトの削除	オブジェクト アクセス：オブジェクト（ファイルまたはディレクトリ）の削除。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）を削除しようとしたときに、ONTAP は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 アクセス：オブジェクト アクセスの試行（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読み取り操作と最初のSMB書き込み操作（成功または失敗）のみを監査します。これにより、単一のクライアントがオブジェクトを開き、同じオブジェクトに対して多数の読み取りまたは書き込み操作を連続して実行した場合に、ONTAPが過剰なログエントリを作成することを回避できます。	ファイル アクセス
NA / 4664	ハード リンク	オブジェクト アクセス：ハード リンクを作成しようとしました。	ファイル アクセス
NA / 4818	提案された集約型アクセス ポリシーで現在の集約型アクセス ポリシーと同じアクセス権限が許可されない	オブジェクト アクセス：Central Access Policy 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	オブジェクトの名前変更	オブジェクトアクセス：オブジェクト名が変更されました。これはONTAPイベントです。現在、Windowsでは単一のイベントとしては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 アクセス：オブジェクトのリンクが解除されました。これは ONTAP イベントです。現在、Windows では単一のイベントとしてはサポートされていません。	ファイル アクセス

イベント**4656**に関する補足情報

監査 `XML`イベントの `HandleID`タグには、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。EVTX 4656イベントの `HandleID`タグには、オープンイベントが新しいオブジェクトの作成用か、既存のオブジェクトを開く用かによって異なる情報が含まれます。

- オープン 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、監査 XML イベント内の `HandleID`タグには空の `HandleID`が表示されます（例： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`）。

  > `HandleID`は空です。これは、`OPEN`（新しいオブジェクトを作成するための）要求が、実際のオブジェクト作成が発生する前、およびハンドルが存在する前に監査されるためです。同じオブジェクトに対する後続の監査イベントには、`HandleID`タグ内に正しいオブジェクトハンドルがあります。

- 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、そのオブジェクトの割り当てられたハンドルが `HandleID`タグ内に含まれます（例： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`）。

ONTAP監査対象オブジェクトへの完全パスを決定する

監査レコードの `<ObjectName>`タグに出力されるオブジェクトパスには、ボリューム名（括弧内）と、そのボリュームのルートからの相対パスが含まれます。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特定するには、いくつかの手順を実行する必要があります。

手順

1. 監査イベントの `<ObjectName>`タグを調べて、ボリューム名と監査対象オブジェクトへの相対パスを決定します。

   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 `/dir1/file.txt`：

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

2. 前の手順で決定したボリューム名を使用して、監査対象オブジェクトを含むボリュームのジャンクションパスを決定します：

   この例では、ボリューム名は「`data1`」であり、監査対象オブジェクトを含むボリュームのジャンクション パスは `/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. `<ObjectName>`タグで見つかった相対パスをボリュームのジャンクション パスに追加して、監査対象オブジェクトへの完全パスを決定します。

   この例では、ボリュームのジャンクション パスは次のとおりです：

   ```
   /data/data1/dir1/file.text
   ```

ONTAPのシンボリックリンクとハードリンクの監査について学ぶ

シンボリックリンクとハードリンクを監査する際には、留意すべき特定の考慮事項があります。

監査レコードには、監査対象オブジェクトに関する情報（`ObjectName`タグで識別される監査対象オブジェクトへのパスを含む）が含まれます。シンボリックリンクとハードリンクのパスが`ObjectName`タグにどのように記録されるかを知っておく必要があります。

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宛先オブジェクトの位置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場合、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実際の標準的なプロトコル非依存パスをたどります。

以下の出力例には、2つのシンボリックリンクがあり、どちらも`target.txt`という名前のファイルを指しています。シンボリックリンクの1つは相対シンボリックリンクで、もう1つ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対象の場合、監査イベントの`ObjectName`タグにはファイル`target.txt`へのパスが含まれます。

```
[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

ハードリンクとは、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位置を指します。ONTAPはシンボリックリンクを解釈するのと同様に、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実際の正規パスをたどります。ハードリンクオブジェクトへのアクセスが監査される場合、監査イベントはハードリンクパスではなく、`ObjectName`タグにこの絶対正規パスを記録します。

ONTAP による代替 NTFS データストリームの監査について学ぶ

NTFS代替データ ストリームがあるファイルを監査する際には、注意が必要ないくつかの考慮事項があります。

監査対象オブジェクトの場所は、 `ObjectName`タグ（パス）と `HandleID`タグ（ハンドル）という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。ログに記録されているストリーム要求を正しく識別するには、ONTAP が NTFS 代替データストリームについて以下のフィールドに何を記録するかを把握しておく必要があります：

- EVTX ID：4656 イベント（監査イベントのオープンと作成）
  - 代替データ ストリームのパスは `ObjectName`タグに記録されます。
  - 代替データ ストリームのハンドルが `HandleID` タグに記録されます。
- EVTX ID: 4663 イベント（読み取り、書き込み、getattr などのその他の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 `ObjectName`タグに記録されます。
  - 代替データ ストリームのハンドルが `HandleID` タグに記録されます。

例

次の例は、 `HandleID`タグを使用して代替データストリームのEVTX ID: 4663イベントを識別する方法を示しています。読み取り監査イベントに記録された `ObjectName`タグ（パス）はベースファイルパスを指していますが、 `HandleID`タグを使用することで、イベントが代替データストリームの監査レコードであることを識別できます。

ストリームファイル名は `base_file_name:stream_name`という形式になります。この例では、 `dir1`ディレクトリには以下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省略されており、イベントの一部の出力タグは表示されていません。

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は、 `ObjectName`タグに代替データ ストリーム名が記録されます：

```
- <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では、`ObjectName`タグに基本ファイル名が記録されます。ただし、`HandleID`タグ内のハンドル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>
```

ONTAPによるNFSファイルおよびディレクトリアクセスイベントの監査について学習します

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。監査可能なアクセスイベントを把握しておくと、変換された監査イベントログの結果を解釈する際に役立ちます。

次に、監査できるNFSファイルおよびディレクトリへのアクセス イベントを示します。

- 注意
- OPEN
- 閉じる
- 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
- 削除
- 属性の取得
- 確認する
- 非検証
- 名前を変更

NFS RENAME イベントを確実に監査するには、ディレクトリ権限が十分であれば RENAME 操作のファイル権限はチェックされないため、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。

ONTAP SVMの監査設定を計画する

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、ビジネスニーズに合った監査設定の作成に役立ちます。

すべての監査構成に共通する特定の構成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パラメータもあります。監査設定時に次の3つの方法のいずれかを指定できます。

- ログ サイズに基づいたログのローテーション

  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 サイズとスケジュール（早い方）に基づいたログのローテーション

ログのローテーション方法は必ず指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。

情報の種類	オプション	必須	含める	値
SVM 名 監査設定を作成するSVMの名前。既存のSVMを指定する必要があります。	`-vserver vserver_name`	はい	はい	
ログの保存先パス 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。SVMネームスペース内の既存のパスを指定する必要があります。 パスは864文字以内で、読み取り / 書き込みアクセス権が設定されている必要があります。 パスが有効でない場合、監査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 ボリューム上に設定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はディザスタ 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として使用することはできません（ONTAP 9.7以降）。	`-destination text`	はい	はい	

監査対象イベントのカテゴリー 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 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。 • 非同期削除 • ファイル共有カテゴリ イベント • 監査ポリシー変更イベント • 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： `cap-staging`をイベントカテゴリとして指定するには、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しなくても、監査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サーバオプションで有効になります。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`	`async-delete}`

いいえ			ログ ファイルの出力形式 監査ログの出力形式を指定します。出力形式は、ONTAP固有の形式`XML`またはMicrosoft Windowsの`EVTX`ログ形式のいずれかです。デフォルトの出力形式は`EVTX`です。	`-format {xml`

evtx}	いいえ			ログ ファイルのローテーション制限 最も古いログファイルをローテーションする前に保持する監査ログファイルの数を決定します。たとえば、`5`の値を入力すると、最後の5つのログファイルが保持されます。 `0`の値は、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。

監査イベント ログをいつローテーションするかを決定するために使用されるパラメータ

ログのサイズに基づいてログをローテーションする

デフォルトでは、サイズに基づいて監査ログがローテーションされます。

- 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ログ サイズを使用する場合、ログ ローテーションに関して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をローテーションする場合は、次のコマンドを使用して `-rotate-schedule-minute`パラメータを設定解除します： `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、 `-rotate-size` パラメータを設定してカスタム ログ サイズを指定できます：

情報の種類	オプション	必須	含める	値
ログ ファイルのサイズ制限 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｜PB］}	いいえ		

スケジュールに基づいてログをローテーションする

スケジュールに基づいて監査ログをローテーションすることを選択した場合は、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使用して、ログのローテーションをスケジュールできます。

- 時間ベースのローテーションを使用する場合、 `-rotate-schedule-minute`パラメータは必須です。
- それ以外の時間に基づくローテーション 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、時間を指定するすべての値を使用して計算されます。

  たとえば、 `-rotate-schedule-minute`パラメータのみを指定すると、監査ログ ファイルは、年間のすべての月のすべての時間帯、すべての曜日に指定された分に基づいてローテーションされます。

- 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 つだけ指定すると（たとえば、 `-rotate-schedule-month`および `-rotate-schedule-minutes`）、指定した月のみ、すべての曜日、すべての時間帯で指定した分の値に基づいてログ ファイルがローテーションされます。

  たとえば、監査ログを1月、3月、8月のすべての月曜日、水曜日、土曜日の午前10：30にローテーションするように指定できます。

- `-rotate-schedule-dayofweek`と `-rotate-schedule-day`の両方に値を指定した場合、それらは独立して考慮されます。

  たとえば、 `-rotate-schedule-dayofweek`を金曜日、 `-rotate-schedule-day`を13と指定した場合、監査ログは13日の金曜日だけでなく、毎週金曜日と指定した月の13日にローテーションされます。

- スケジュールのみに基づいて監査ログをローテーションする場合は、次のコマンドを使用して `-rotate-size`パラメータを設定解除します： `vserver audit modify -vserver vs0 -destination`

```
/ -rotate-size -
```

使用可能な監査パラメータの次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を構成するために使用する値を決定できます：

情報の種類	オプション	必須	含める	値
ログローテーションスケジュール：月 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 `January`から `December`まで、および `all`です。たとえば、監査ログを1月、3月、8月の3か月間にローテーションす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 `Sunday`から `Saturday`まで、および `all`です。たとえば、監査ログを火曜日と金曜日にローテーションするように指定することも、週のすべての曜日にローテーションするように指定することもできます。	`-rotate-schedule -dayofweek chron_dayofweek`	いいえ		
ログローテーションスケジュール：日 監査ログのローテーションを実行する日（月の日）を指定します。 有効な値の範囲は `1`から `31`です。たとえば、監査ログを毎月 10 日と 20 日にローテーションするように指定することも、毎月すべての日にローテーションするように指定することもできます。	`-rotate-schedule-day chron_dayofmonth`	いいえ		
ログローテーションスケジュール：時間 監査ログをローテーションする時間単位のスケジュールを決定します。 有効な値の範囲は `0`（午前0時）から `23`（午後11：00）です。 `all`を指定すると、監査ログは1時間ごとにローテーションされます。例えば、監査ログを6（午前6時）と18（午後6時）にローテーションす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 監査ログをローテーションする分単位のスケジュールを決定します。 有効な値の範囲は 0～ `59`です。たとえば、監査ログを 30 分にローテーションす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構成する場合は「はい」、それ以外の場合は「いいえ」。		

ログのサイズとスケジュールに基づいてログをローテーションする

ログ サイズとスケジュールに基づいてログ ファイルをローテーションするには、 `-rotate-size`パラメータと時間ベースのローテーション パラメータを任意に組み合わせて設定します。例： `-rotate-size`を10 MBに設定し、 `-rotate-schedule-minute`を15に設定した場合、ログ ファイルのサイズが10 MBに達したとき、または毎時15分（どちらか早く発生したイベント）にログ ファイルがローテーションされます。

SVM上でのファイルとディレクトリの監査設定の作成

ONTAP SVMでファイルとディレクトリの監査設定を作成する

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、設定を計画してから、設定を作成して有効にします。その後、監査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予定がある場合は、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（DAC）を有効にしていなくても監査設定では集約型アクセス ポリシー ステージングを有効にすることができますが、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しか生成されません。

  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。

タスク概要

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 ボリューム上に設定することはできません。

手順

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	入力する内容
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

次の例では、サイズベースの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）を監査する監査設定を作成します。ログ形式は `EVTX`（デフォルト）です。ログは `/audit_log`ディレクトリに保存されます。ログファイルのサイズ制限は `200 MB`です。ログは200 MB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
```

次の例では、サイズベースのローテーションを使用して、ファイル操作とSMBログオン/ログオフイベント（デフォルト）を監査する監査設定を作成します。ログ形式は `EVTX`（デフォルト）です。ログは `/cifs_event_logs`ディレクトリに保存されます。ログファイルのサイズ制限は `100 MB`（デフォルト）、ログローテーション制限は `5`です。

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

次の例では、時間ベースの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、および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設定を作成します。ログ形式は EVTX（デフォルト）です。監査ログは毎月、毎日午後12：30にローテーションされます。ログローテーションの制限は 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での監査の有効化"
- "監査設定の確認"

監査設定を設定した後、ONTAP SVMで監査を有効にする

監査設定が完了したら、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。

タスク概要

SVMディザスタ リカバリのID破棄設定が（SnapMirrorの初期化完了後に）最初に開始されるときに、SVMに監査設定がある場合、ONTAPは監査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。監査を有効にできるのは、SnapMirror関係が解除されてSVMが読み取り / 書き込み可能になったあとのみです。

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

- "監査設定の作成"
- "監査設定の確認"

ONTAP監査設定を確認する

監査設定が完成したら、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
   ```

関連情報

- "監査設定の作成"
- "SVMでの監査の有効化"

ファイルおよびフォルダの監査ポリシーの設定

ONTAP SVM で監査設定を有効にし、ファイルとフォルダの監査ポリシーを設定します。

ファイルおよびフォルダへのアクセス イベントに対する監査の実装は、2つのステップで行います。まず、Storage Virtual Machine（SVM）上で監査設定を作成し、有効化する必要があります。次に、監視対象の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。監査ポリシーは、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設定できます。

SMB 監査ポリシーと NFS 監査ポリシーの両方を設定できます。SMB 監査ポリシーと NFS 監査ポリシーには、設定要件と監査機能が異なります。

適切な監査ポリシーが設定されている場合、ONTAP は、SMB サーバまたは NFS サーバが実行中の場合にのみ、監査ポリシーで指定されたとおりに 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とディレクトリにONTAP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 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にある*Windowsセキュリティ*タブを使用して、ファイルとディレクトリのNTFS監査ポリシーを設定できます。これは、Windowsクライアント上のデータの監査ポリシーを設定する場合と同じ方法で、使い慣れたGUIインターフェイスを使用できます。

開始する前に

監査は、システム アクセス制御リスト（SACL）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。

タスク概要

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. エクスプローラの ツール メニューから、ネットワーク ドライブの割り当て 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. フォルダー 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 SMB サーバー名と共有の名前を入力します。

      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アドレスを指定することもできます。

      SMB サーバー名が「`SMB_SERVER`」で、共有名が「`share1`」の場合は、 `\\SMB_SERVER\share1` と入力する必要があります。
   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となり、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. *Advanced*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。

次の操作を行う場合は....	以下の手順を実行してください
新しいユーザまたはグループの監査を設定する	a. *[追加]*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する	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、削除するユーザまたはグループを選択します。 b. *削除*をクリックします。 c. *OK*をクリックします。 d. 残りの手順は不要です。
ユーザまたはグループの監査を変更する	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、変更するユーザまたはグループを選択します。 b. *編集*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する場合、または既存のユーザーまたはグループの監査を変更する場合は、<object>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、この監査エントリを適用する方法を選択します。

   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 単一のファイルに監査を設定する場合、*適用先*ボックスはアクティブになりません。*適用先*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、監査対象を選択し、成功したイベント、失敗したイベント、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、[Success]ボックスを選択します。
- 失敗したイベントを監査するには、[Failure]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
- フォルダをトラバース / ファイルを実行
- フォルダの一覧表示/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
- 属性を書き込む
- 拡張属性を書き込む
- サブフォルダとファイルを削除する
- 削除
- 読み取り権限
- 権限の変更
- 責任を取る

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伝播させない場合は、これらの監査エントリをこのコンテナ内のオブジェクトおよび/またはコンテナにのみ適用する ボックスをオンにします。
12. *適用*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。

    <object>ボックスの監査エントリが閉じます。

14. *監査*ボックスで、このフォルダー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。
    - [すべての子孫の既存の継承可能な監査エントリを、このオブジェクトからの継承可能な監査エントリに置き換える] ボックスを選択します。
    - 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でください。単一のファイルに SACL を設定する場合、「すべての子孫の既存の継承可能な監査エントリを、このオブジェクトの継承可能な監査エントリに置き換える」ボックスは「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を使用したNTFS監査ポリシーの設定

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。

`vserver security file-directory`コマンド ファミリを使用して、NTFS監査ポリシーを構成できます。

NTFS SACLはCLIを使用してのみ設定できます。このONTAPコマンド ファミリーでは、NFSv4 SACLの設定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ファイルとフォルダにNTFS SACLを設定および追加する方法の詳細については、"ONTAPコマンド リファレンス"を参照してください。

UNIXセキュリティ形式のファイルとディレクトリのONTAP監査を構成する

UNIXセキュリティ形式のファイルと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、セキュリティ目的で特定のNFSファイルおよびディレクトリへのアクセス イベントを監視できます。

タスク概要

NFSv4.xでは、任意ACEとシステムACEの両方が同じACLに格納されます。これらは別々のDACLやSACLには格納されません。そのため、既存のACLに監査ACEを追加する際には、既存のACLが上書きされて失われないように注意する必要があります。監査ACEを既存のACLに追加する順序は重要ではありません。

手順

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

   ACL の操作の詳細については、"ONTAPコマンド リファレンス"を参照してください。

2. 必要な監査 ACE を追加します。
3. `nfs4_setfacl`または同等のコマンドを使用して、更新された ACL をファイルまたはディレクトリに適用します。

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の表示

Windows のセキュリティ タブにアクセスして ONTAP 監査ポリシー情報を表示

Windowsの[プロパティ]ウィンドウにある[セキュリティ]タブを使用して、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できます。これはWindowsサーバ上に存在するデータを利用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。

タスク概要

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ホストで以下の手順を実行します。

手順

1. エクスプローラの ツール メニューから、ネットワーク ドライブの割り当て 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 ボックスを完了します：

   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の名前の両方を保持する共有を含むStorage Virtual Machine（SVM）のIPアドレスまたはSMBサーバー名を入力します。

      SMB サーバー名が「`SMB_SERVER`」で、共有名が「`share1`」の場合は、 `\\SMB_SERVER\share1` と入力する必要があります。

      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アドレスを指定することもできます。

   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となり、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. *Advanced*をクリックします。
7. *監査*タブを選択します。
8. *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*をクリックします。

    <object>ボックスの監査エントリが開きます。

11. アクセス 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、**<object>** の監査エントリ 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。

ONTAP FlexVolボリューム上の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。

タスク概要

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）の名前と、監査情報を表示するファイルまたはディレクトリへのパスを指定する必要があります。出力には要約または詳細な一覧を表示できます。

- 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は、UNIXファイル権限（モード ビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- 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。
- mixedセキュリティ形式のボリュームまたはqtreeでは、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、ストレージレベルのアクセス保護セキュリティを設定できるため、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の出力には、標準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の表示時には、UNIX関連の出力フィールドに表示専用のUNIXファイル アクセス権情報が格納されます。

  ファイル アクセス権の決定時には、NTFSセキュリティ形式のファイルおよびフォルダで、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 ビットの権限のみ（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。

手順

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

情報を表示する場合…	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細な一覧	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1 内のパス `/corp`の監査ポリシー情報を表示します。パスには NTFS 有効セキュリティが設定されています。NTFS セキュリティ記述子には、SUCCESS と SUCCESS/FAIL の両方の SACL エントリが含まれています。

```
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、SVM vs1 内のパス `/datavol1`の監査ポリシー情報を表示します。パスには、通常の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ガード SACL の両方が含まれています。

```
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
```

ワイルドカード文字を使用して、**ONTAP**ファイルのセキュリティと監査ポリシーに関する情報を表示します。

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と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、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、その下のすべてのファイルとディレクトリの情報が表示されます。

「*」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、二重引用符（" "）で囲んで完全なパスを指定する必要があります。

例

ワイルドカード文字を使用した次のコマンドは、SVM vs1 のパス `/1/`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を表示します：

```
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、SVM vs1のパス `/vol1/a`下にある「*」という名前のファイルの情報を表示します。パスは二重引用符（" "）で囲まれています。

```
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**ONTAP CLI**の変更イベントについて学習します

ONTAPでは、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と、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 ID	このコマンドを実行します…
Mhostの監査	policy-change	[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] ネットワーク共有が変更されました	`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	ユーザーアカウント	[4720] ローカルユーザーが作成されました	`vserver cifs users-and-groups local-user create` `vserver services name-service unix-user create`
[4722] ローカルユーザーが有効	`vserver cifs users-and-groups local-user create	modify`	[4724] ローカルユーザーのパスワードリセット
`vserver cifs users-and-groups local-user set-password`	[4725] ローカルユーザーが無効になっています	`vserver cifs users-and-groups local-user create	modify`
[4726] ローカルユーザーが削除されました	`vserver cifs users-and-groups local-user delete` `vserver services name-service unix-user delete`	[4738] ローカルユーザーの変更	`vserver cifs users-and-groups local-user modify` `vserver services name-service unix-user modify`
[4781] ローカルユーザーの名前変更	`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が変更されました

`vserver cifs users-and-groups local-group rename	modify` `vserver services name-service unix-group modify`	[4732] ユーザーがローカルグループに追加されました	`vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`
[4733] ユーザーがローカル グループから削除されました	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	承認ポリシーの変更	[4704] ユーザー権限が割り当てられました
`vserver cifs users-and-groups privilege add-privilege`	[4705] ユーザー権限が削除されました	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

関連情報

- "SVM"

ファイル共有**ONTAP**イベントを管理する

ストレージ仮想マシン（SVM）にファイル共有イベントが設定され、監査が有効になっている場合、監査イベントが生成されます。ファイル共有イベントは、 `vserver cifs share`関連コマンドを使用してSMBネットワーク共有が変更されたときに生成されます。

イベントID 5142、5143、5144 のファイル共有イベントは、SVM の 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。SMB ネットワーク共有の設定は、 `cifs share access control create|modify|delete`コマンドを使用して変更されます。

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file-share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)
```

監査ポリシー変更の**ONTAP**イベントを管理する

ストレージ仮想マシン（SVM）に監査ポリシー変更イベントが設定され、監査が有効になっている場合、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、`vserver audit`関連コマンド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。

イベントID 4719の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、または変更されるたびに生成され、ユーザーが痕跡を隠蔽するために監査を無効化しようとしたタイミングを特定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、無効化には診断権限が必要です。

次の例では、監査が無効にされたときにID 4719のaudit-policy-change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
```

ユーザーアカウントのONTAPイベントを管理する

Storage Virtual Machine（SVM）に対してuser-accountイベントが設定されていて、監査が有効になっている場合、監査イベントが生成されます。

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

次の例は、ローカル SMB ユーザーが作成されたときに生成された ID 4720 のユーザー アカウント イベントを示しています：

```
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 ~
```

次の例は、前の例で作成されたローカルSMBユーザーの名前が変更されたときに生成される、ID 4781のユーザー アカウント イベントを示しています：

```
 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の**ONTAP**イベントを管理する

Storage Virtual Machine（SVM）に対してsecurity-groupイベントが設定されていて、監査が有効になっている場合、監査イベントが生成されます。

イベント ID 4731、4732、4733、4734、4735 のセキュリティグループイベントは、ローカル SMB または NFS グループがシステムから作成または削除されたとき、およびローカルユーザーがグループに追加または削除されたときに生成されます。セキュリティグループイベントは、 `vserver cifs users-and-groups <*local-group*>`コマンドおよび `vserver services name-service <*unix-group*>`コマンドを使用してユーザーアカウントが変更されたときに生成されます。

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security-group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 ~
```

認可ポリシー変更の**ONTAP**イベントを管理する

Storage Virtual Machine（SVM）に対してauthorization-policy-changeイベントが設定されていて、監査が有効になっている場合、監査イベントが生成されます。

イベントID 4704 および 4705 の authorization-policy-change イベントは、SMB ユーザーおよび SMB グループに対して認可権限が付与または取り消されるたびに生成されます。authorization-policy-change イベントは、 `vserver cifs users-and-groups privilege`関連コマンドを使用して認可権限が割り当てまたは取り消された場合に生成されます。

次の例では、SMBユーザ グループに対する認証権限が割り当てられ、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
```

監査設定の管理

監査イベントログを手動でローテーションして、特定の**ONTAP SVM**イベントログを表示します

監査イベントログを表示するには、ログをユーザーが読み取り可能な形式に変換する必要があります。ONTAPがログを自動的にローテーションする前に特定のストレージ仮想マシン（SVM）のイベントログを表示したい場合は、SVM上の監査イベントログを手動でローテーションできます。

手順

1. `vserver audit rotate-log`コマンドを使用して監査イベントログをローテーションします。

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

   監査イベント ログは、監査設定（(`XML`または `EVTX`）で指定された形式で SVM 監査イベント ログ ディレクトリに保存され、適切なアプリケーションを使用して表示できます。

ONTAP SVMの監査を有効または無効にする

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、いつでも有効にすることができます（監査設定が存在する場合）。

開始する前に

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

"監査設定の作成"

タスク概要

監査を無効にしても、監査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。

監査を実行したい場合...	コマンドを入力してください...
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
```

ONTAP監査設定に関する情報を表示する

監査設定に関する情報を表示できます。この情報は、各SVMの設定が適切かどうかを判断するのに役立ちます。また、表示される情報から、監査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。

タスク概要

すべてのSVMの監査設定に関する詳細情報を表示できます。また、オプション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。オプションパラメータをいずれも指定しない場合は、以下の情報が表示されます：

- 監査設定が適用される SVM 名
- 監査状態。 `true`または `false`のいずれかになります

  監査状態が `true`の場合、監査は有効です。監査状態が `false`の場合、監査は無効です。

- 監査するイベントのカテゴリ
- 監査ログの形式
- 監査サブシステムが統合および変換された監査ログを保存するターゲット ディレクトリ

手順

1. `vserver audit show`コマンドを使用して監査構成に関する情報を表示します。

   `vserver audit show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-audit-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

例

次の例では、すべての SVM の監査設定の概要が表示されます：

```
cluster1::> vserver audit show

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

次の例では、すべての SVM のすべての監査設定情報をリスト形式で表示します：

```
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
```

監査設定を変更するための**ONTAP**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など、現在の設定をいつでも変更したり、保存するログ ファイルの最大数を指定したりできます。

状況	使用するコマンド
ログのディスティネーション パスを変更する	`vserver audit modify`と `-destination`パラメータ

監査するイベント カテゴリを変更する	`vserver audit modify`と `-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、ダイナミック アクセス制御（DAC）の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。
ログ形式を変更する	`vserver audit modify`と `-format`パラメータ
一時ログ ファイルのサイズに基づく自動保存を有効にする	`vserver audit modify`と `-rotate-size`パラメータ
定期的な自動保存を有効にする	`vserver audit modify`と `-rotate-schedule-month`、`-rotate-schedule-dayofweek`、`-rotate-schedule-day`、`-rotate-schedule-hour`、および `-rotate-schedule-minute`パラメータ
保存可能な最大ログ ファイル数を指定する	`vserver audit modify`と `-rotate-limit`パラメータ

ONTAP SVMの監査設定を削除する

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で監査設定を維持する必要がなくなった場合は、監査設定を削除できます。

手順

1. 監査構成を無効にします：

   ```
   vserver audit disable -vserver vserver_name

   vserver audit disable -vserver vs1
   ```

2. 監査構成を削除します：

   ```
   vserver audit delete -vserver vserver_name

   vserver audit delete -vserver vs1
   ```

監査済みのONTAPクラスタを元に戻すことの影響を理解する

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）がクラスタ内にあるときにONTAPが実行するリバート プロセスを把握しておく必要があります。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 イベントや集約型アクセス 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 イベントや集約型アクセス 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から開始されています。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。

ONTAPの監査およびステージング 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

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問題を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 ボリュームに関するスペースの問題のトラブルシューティング

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。

> ⓘ 次の場合はデータへのアクセスが拒否されます。
>
> - デスティネーション ディレクトリが削除されている
> - 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

詳細については以下を参照してください。

- "ボリュームに関する情報の表示方法とボリューム サイズの増加方法"。
- "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

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が失敗する場合は、ステージングボリュームのスペースが不足している可能性があります。SVM管理者は、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のスペースが不足していないかどうかを確認するために、管理者に連絡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のために監査イベントを生成できない場合、監査サブシステムはEMSイベントを生成します。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は管理者のみが表示できます。SVM管理者は表示できません。

すべてのステージング ボリューム名は `MDV_aud_`で始まり、その後にそのステージング ボリュームを含むアグリゲートのUUIDが続きます。次の例は、クラスタ内のデータSVMにファイル サービス監査設定が作成されたときに自動的に作成された、管理SVM上の4つのシステム ボリュームを示しています：

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
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大きくすることができるのは、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（ONTAP 9.14.1以前）または5GB未満（ONTAP 9.15.1以降）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。

著作権に関する情報

商標に関する情報