SVMでのNASイベントの監査

ONTAP 9

NetApp
December 20, 2024

目次

SVMでのNASイベントの監査

SMBおよびNFSの監査とセキュリティトレース

ONTAPのSMBプロトコルおよびNFSプロトコルで使用できるファイルアクセス監査機能（標準の監査やFPolicyを使用したファイルポリシー管理など）を使用できます。

SMBおよびNFSのファイルアクセスイベントの監査は、次のような場合に設計し、実装する必要があります。

- SMBプロトコルと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を使用して監査の設定を作成および管理する。
  - ONTAPの標準機能
  - ガイブFPolicyサーバ

SVMでのNASイベントの監査

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。これにより、潜在的なセキュリティの問題を追跡し、セキュリティ違反の証拠を提供できます。また、Active Directoryの集約型アクセスポリシーをステージングおよび監査して、そ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ファイルオヨヒフォルタアクセスイヘント

  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の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ヘント

  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る監査では、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のステージングイベントを監査するように設定する必要があります。

  監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントはダイナミックアクセス制御が有効になっている場合にのみ生成されます。ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。

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の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 `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（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。このタスクでは、監査レコードを時間順にソートしてマージし、監査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（EVTXファイル形式または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監査プロセスの仕組みを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 ファイルの保存用に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と、エラーが表示されて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"`。

  ディレクトリは存在しているがシンボリックリンクが含まれている場合、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を確認するには、ファイルに保存されているコマンド履歴ログを確認し `audit.log`ます。
>
> 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"。

ノードが使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パートナー経由で使用可能な場合は、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パートナーを使用できない場合は、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の使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、統合ファイル名にサフィックスが追加され `.partial`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。

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確認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。

  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）がサポートされます。
- 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。

    監査の設定で指定された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（など）は指定しないで `/vs1/../` ください。

- 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よって異なります。

  監査対象のボリュームを含むアグリゲート内のステージングボリュームに十分なスペースを確保するための計画を把握しておく必要があります。

- 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するための計画を把握しておく必要があります。監査ディレクトリに保持するイベントログの数は、監査の設定の作成時にパラメータを使用して指定でき `-rotate-limit` ます。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、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。クラスタで監査を有効にする場合は、アグリゲートスペースに関する考慮事項について理解しておく必要があります。

アグリゲートにスペースがないと、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、既存のアグリゲートにステージングボリュームを格納できるだけ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。

監査レコードが大規模になる状況

管理監査中に、次のいずれかの状況で監査レコードが大量に発生する可能性があります。

- 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します。
- 多数のファイル共有ユーザがいるファイル共有に対するファイル共有のAccess Control List（ACL；アクセス制御リスト）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。

監査レコードが大きすぎる場合の影響

- 監査レコードのサイズが大きすぎる（32KBを超える）と、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。大きいキー値が指定されていない部分的な監査レコードが作成されます。
- 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とは

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、 `EVTX`および `XML`ファイル形式です。

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はバイナリログをファイル形式に変換し `EVTX`ます。

監査イベントログの表示

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、およびファイルやフォルダへの不適切なアクセス試行が行われたかどうかを確認できます。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`。

- `EVTX`ファイル形式

  変換された監査イベントログは、保存されたファイルとしてMicrosoftイベントビューアを使用して開くことができます `EVTX`。

  イベントビューアを使用してイベントログを表示する場合は、次の2つのオプションを使用できます。

  - 全般表示

    イベントレコードについては、すべてのイベントに共通の情報が表示されます。このバージョンのONTAPでは、イベントレコードのイベント固有のデータは表示されません。詳細ビューを使用すると、イベント固有のデータを表示できます。

  - 詳細ビュー

    フレンドリビューとXMLビューを使用できます。フレンドリビューとXMLビューには、すべてのイベントに共通する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

  監査イベントログは、ファイル形式をサポートする他社製アプリケーションで `XML`表示および処理できます `XML`。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スキーマと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は、統合プロセスによって、監査を有効にしたStorage Virtual Machine（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共有を介してMicrosoftイベントビューアでアクセスして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の表示に加えて、コンソールウィンドウの内容を更新できる更新オプションがあります。アクティブな監査ログへのアクセス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	イベントビューアは、その時点までに書き込まれたイベントを含むログを開きます。更新処理では、統合プロセスで追加された新しいイベントでログが更新されません。
無効にする	イベントビューアは、その時点までに書き込まれたイベントを含むログを開きます。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、イベントログにのみ適用され `EVTX`ます。 `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。

カンサテキルSMBイヘント

カンサテキルSMBイヘントノカイヨウ

ONTAPでは、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、特定のSMBイベントを監査できます。どのアクセスイベントを監査できるかを把握しておくと、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、さらに次の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
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	アカウントが正常にログオンしました	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	削除するための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	オブジェクトの削除	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）を削除しようとしたときに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、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連続して多数の読み取りまたは書き込み処理を実行しても、ONTAPが過剰なログエントリを作成するのを防ぐことができます。	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ない	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	オブジェクトの名前変更	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`監査イベントのタグ `XML`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ています。 `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、監査XMLイベントのタグには HandleID`空（例： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>）が表示されます HandleID。

が HandleID`空になっているのは、（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、タグ内に適切なオブジェクトハンドルを持ちます `HandleID。

- open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タグに含まれ HandleID`ます（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特定する

監査レコードのタグに出力されたオブジェクトパス `<ObjectName>`には、ボリュームの名前（かっこ内）と、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. 監査イベントのタグを確認して、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>。

   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」で、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. タグ内の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 <ObjectName>。

   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、タグで識別される監査対象オブジェクトのパスなど、監査対象オブジェクトに関する情報が含まれます。 `ObjectName`シンボリックリンクおよびハードリンクのパスがタグ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`。

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 `target.txt`います。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、 `ObjectName`監査イベントのタグにファイルへのパスが含まれ `target.txt`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、監査イベントはハードリンクパスではなく、この正規の絶対パスをタグに記録します `ObjectName`。

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含む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、タグ（パス）とタグ（ハンドル）の `HandleID`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`。ログに記録されてい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の次のフィールドにONTAPが記録するものに注意する必要があります。

- 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タグに記録され `ObjectName`ます。
  - 代替データストリームのハンドルはタグに記録され `HandleID`ます。

- 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タグに記録され `ObjectName`ます。
  - 代替データストリームのハンドルはタグに記録され `HandleID`ます。

例

次の例は、タグを使用して代替データストリームのEVTX ID：4663イベントを特定する方法を示してい `HandleID`ます。 `ObjectName`読み取り監査イベントで記録されたタグ（パス）はベースファイルパスに対するものですが、 `HandleID`タグを使用すると、代替データストリームの監査レコードとしてイベントを識別できます。

ストリームファイル名はの形式になり `base_file_name:stream_name`ます。この例では、 `dir1`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ディレクトリに含まれています。

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

次のイベント例の出力は、示されているように省略されています。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では、代替データストリーム名がタグに記録され `ObjectName`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、ベースファイル名がタグに記録され `ObjectName`ます。ただし、タグ内のハンドルは `HandleID`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>
```

カンサテキル**NFS**フアイルオヨヒテイレクトリノアクセスイヘント

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。

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は次のとおりです。

- 読み取り
- オープン
- 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
- 取り外します
- 属性の取得
- 確認します
- 非検証
- 名前の変更

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、ビジネスニーズを満たす監査の設定に役立ちます。

すべての監査設定に共通の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のパラメータもいくつかあります。監査の設定時に、次の3つの方法のいずれかを指定できます。

- ログサイズに基づく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	自分の価値観
SVM 名 _ 監査設定を作成するSVMの名前。SVMがすでに存在している必要があります。	`-vserver vserver_name`	○	○	

_ 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（通常は専用のボリュームまたはqtree）を指定します。SVMネームスペースにすでに存在しているパスを指定する必要があります。 パスは最大864文字で、読み取り/書き込み権限が必要です。 パスが無効な場合、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のソースである場合、ログデスティネーションパスをルートボリュームに配置することはできません。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デスティネーション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`	○	○	

_ 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。 • 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：*イベントカテゴリとしてを指定するには、 `cap-staging`SVM上にSMBサーバが存在している必要があります。監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントはダイナミックアクセス制御が有効になっている場合にのみ生成されます。ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。	-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固有またはMicrosoft Windows `EVTX`ログ形式のいずれかになり`XML`ます。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。この数を超えると、最も古いログファイルがローテーションから除外されます。たとえば、の値を入力する `5` と、最後の5つのログファイルが保持されます。 値がの `0` 場合は、すべてのログファイルが保持されます。デフォルト値は0です。

監査イベントログのローテーションのタイミングの決定に使用するパラメータ

- ログサイズに基づいてログを回転 *

デフォルトでは、監査ログのローテーションはサイズに基づいて行われます。

- 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式とデフォルトのログサイズを使用する場合は、ログローテーション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パラメータの設定を解除し `-rotate-schedule-minute`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、カスタムログサイズを指定するようにパラメータを設定でき `-rotate-size`ます。

情報の種類	オプション	必須	含める	自分の価値観
_ 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決定します。	`-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く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。

- 時間に基づく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。
- その他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、パラメータのみを指定する `-rotate-schedule-minute`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。

- 時間に基づくローテーションパラメータを1つか2つだけ指定した場合（、など `-rotate-schedule -month -rotate-schedule-minutes`）、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月の月曜日、水曜日、土曜日の午前10時30分に実行するように指定できます。

- との `-rotate-schedule-day`両方に値を指定すると `-rotate-schedule-dayofweek`、それらは独立して考慮されます。

  たとえば、にFridayを指定し、 `-rotate-schedule-day`に13を指定する `-rotate-schedule-dayofweek`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、および指定した月の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パラメータの設定を解除し `-rotate-size`ます。 `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の設定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	自分の価値観

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 `January`、～ `December`、および `all`です。たとえば、監査ログのローテーションを1月、3月、8月に実行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`、～ `Saturday`、および `all`です。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。 有効な値の範囲は `1`～ `31`です。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）～ `23`（午後11時）です。を指定する `all`と、監査ログのローテーションが1時間ごとに行われます。たとえば、監査ログのローテーションを6（午前6時）と18（午後6時）に行う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指定します。 有効な値の範囲は 0~ `59`です。たとえば、監査ログのローテーションを30分に行うように指定できます。	`-rotate-schedule-minute chron_minute`	はい（スケジュールベースのログローテーションを設定する場合）。それ以外の場合はいいえ。		

- ログサイズとスケジュールに基づいてログを回転 *

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ように選択するには、パラメータと時間ベースのローテーションパラメータの両方を任意に組み合わせて設定し `-rotate-size`ます。たとえば、が`10MB`に設定され、 `-rotate-schedule-minute`が`15`に設定されている場合 `-rotate-size`、ログファイルのサイズが10MBに達したとき、または1時間ごとの15分（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でファイルとディレクトリの監査設定を作成します。

監査の設定を作成する

Storage Virtual Machine（SVM）上でファイルとディレクトリの監査の設定を作成するには、使用可能な設定オプションについて理解し、設定を計画し、設定を行って有効にします。その後、監査の設定に関する情報を表示して、設定した設定が適切かどうかを確認できます。

ファイルおよびディレクトリイベントの監査を開始する前に、監査の設定をStorage Virtual Machine（SVM）で作成する必要があります。

開始する前に

集約型アクセスポリシーステージングの監査の設定を作成する場合は、SVM上にSMBサーバが存在している必要があります。

- 監査の設定では、SMBサーバでダイナミックアクセス制御を有効にしなくても集約型アクセスポリシーのステージングを有効にできますが、集約型アクセスポリシーのステージングイベントはダイナミックアクセス制御が有効になっている場合にのみ生成されます。

  ダイナミックアクセス制御はSMBサーバオプションを使用して有効にします。デフォルトでは有効になっていません。

- コマンドのフィールドの引数が無効な場合（フィールドのエントリが無効である、エントリが重複している、エントリがないなど）、コマンドは監査フェーズの前に失敗します。

  この場合、監査レコードは生成されません。

タスクの内容

SVMがSVMディザスタリカバリのソースである場合、デスティネーションパスをルートボリュームに配置することはできません。

ステップ

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。ログ形式は（デフォルト）です `EVTX`。ログはディレクトリに保存され `/audit_log`ます。ログファイルの最大サイズはです `200 MB`。ログは、サイズが200MBに達するとローテーションされます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

次の例は、サイズに基づくローテーションを使用してファイル操作とSMBログオンおよびログオフイベント（デフォルト）を監査する監査の設定を作成します。ログ形式は（デフォルト）です `EVTX`。ログはディレクトリに保存され `/cifs_event_logs`ます。ログファイルのサイズの上限は `100 MB`（デフォルト）、ログのローテーションの上限は次のとおり `5`です。

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

次の例は、時間に基づくローテーションを使用してファイル操作、CIFSのログオンおよびログオフイベン

ト、集約型アクセスポリシーのステージングイベントを監査する監査の設定を作成します。ログ形式は（デフォルト）です EVTX。監査ログのローテーションは、毎月、すべての曜日の午後12時30分に実行されます。ログのローテーションの上限は次のとおりです 5。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

関連情報

- "SVMで監査を有効にする"
- "監査の設定を確認する"

SVMで監査を有効にする

監査の設定が完了したら、 Storage Virtual Machine （ SVM ）で監査を有効にする必要があります。

開始する前に

SVM の監査設定がすでに存在している必要があります。

タスクの内容

SVM ディザスタリカバリ ID 破棄の設定が（ SnapMirror 初期化完了後に）初めて開始され、 SVM に監査の設定がある場合、 ONTAP は監査の設定を自動的に無効にします。読み取り専用 SVM では、ステージングボリュームがいっぱいにならないように監査が無効になっています。SnapMirror 関係が解除されて SVM が読み書き可能になったあとでないと、監査を有効にすることはできません。

手順

1. SVM で監査を有効にします。

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

関連情報

- "監査の設定を作成する"
- "監査の設定を確認する"

監査の設定を確認する

監査の設定が完了したら、監査が適切に設定されて有効になっていることを確認する必要があります。

手順

1. 監査の設定を確認します。

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

   次のコマンドは、Storage Virtual Machine（SVM）vs1のすべての監査の設定情報をリスト形式で表示します。

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                          Log Format: evtx
                  Log File Size Limit: 200MB
        Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
   ```

関連情報

- "監査の設定を作成する"
- "SVMで監査を有効にする"

ファイルおよびフォルダの監査ポリシーを設定する

ファイルおよびフォルダの監査ポリシーを設定する

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）で監査の設定を作成し、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対する監査ポリシーの設定

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、監査設定のセットアップ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に対して監査ポリシーを設定する場合と同じ方法で、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。

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。

タスクの内容

NTFS監査ポリシーを設定するには、NTFSセキュリティ記述子に関連付けられているNTFS SACLにエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。これらのタスクはWindows GUIで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限を適用するための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、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

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（ 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てください。
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（ 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ため、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。単一ファイルのSACLを設定している場合は、[監査]ボックスに[すべての子孫の既存の継承可能な監査エントリをすべてこのオブジェクトからの継承可能な監査エントリで置き換える]ボックスは表示されません。

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、ファイルや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。

NTFS監査ポリシーを設定するには、コマンドファミリーを使用し `vserver security file-directory`ます。

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、ファイルやフォルダに追加する方法の詳細については、マニュアルページを参照してください。

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の設定

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。

タスクの内容

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. 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 `nfs4_getfacl`。

   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. または同等のコマンドを使用して、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`。

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する

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する

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、ファイルと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るため、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。

タスクの内容

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System Access Control List（SACL；システムアクセス制御リスト）が設定されているかどうかを確認できます。

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、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。

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を使用したFlexVolのNTFS監査ポリシーに関する情報の表示

セキュリティ形式と有効なセキュリティ形式、適用されている権限、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。

タスクの内容

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System Access Control List（SACL；システムアクセス制御リスト）が設定されているかどうかを確認できます。

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。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- 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やフォルダには、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には、UNIX対応またはNTFS対応のセキュリティを設定でき、NTFS SACLが格納されている場合と格納されていない場合があります。
- 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NTFS SACLの両方が表示されることがあります。
- 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表示専用のUNIXファイル権限情報が表示されます。

  ファイルアクセス権の決定時に、NTFSセキュリティ形式のファイルおよびフォルダでは、NTFSファイル権限と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や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の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	`vserver security file-directory show -vserver vserver_name -path path`
詳細なリスト	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/corp`。パスにはNTFS対応の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、SVM vs1のパスの監査ポリシーの情報を表示します `/datavol1`。このパスには、通常のファイルとフォルダの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
```

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

次のコマンドでワイルドカード文字を使用すると、SVM vs1の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 `/1/` 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のパスの下にある「*」という名前のファイルの情報を表示します `/vol1/a`。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

監査できる**CLI**変更イベントの概要

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、特定のCLI変更イベントを監査できます。どの変更イベントを監査できるかを理解しておくと、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）によるCLI変更イベントの監査の管理作業として、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、監査変更イベントに関する情報の表示、監査変更イベントの変更、監査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各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 IDs	実行するコマンド
Mhostの監査	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`

フアイルキヨウユウイヘントノカンリ

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が生成されるのは、の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場合 `vserver cifs share`です。

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、コマンドを使用して変更し `cifs share access control create|modify|delete`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が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)
```

カンサホリシイヘンコウイヘントノカンリ

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、の関連コマンドを使用して監査ポリシーが変更された場合に生成され `vserver audit`ます。

監査ポリシー変更イベント（イベントID 4719）は、監査ポリシーが無効、有効、または変更されたときに生成され、ユーザが監査を無効にしようとしたタイミングを特定して追跡できます。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、監査が無効になっているときに、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の管理

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、コマンドおよび `vserver services name-service *<unix user>*`コマンド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 `vserver cifs users-and-groups *<local user>*`ます。

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、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アカウントが変更されたときに生成され `vserver cifs users-and-groups <*local-group*>`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の管理

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グループに対して認証権限が付与または取り消されるたびに生成されます。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が生成されるのは、の関連コマンド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 `vserver cifs users-and-groups privilege`です。

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

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実行できます。

ステップ

1. コマンドを使用して、監査イベントログのローテーションを行い `vserver audit rotate-log`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(XML EVTX、該当するアプリケーションを使用して表示できます。

SVMでの監査の有効化と無効化

Storage Virtual Machine（SVM）で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。

"監査の設定を作成する"

タスクの内容

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`
無効にする	`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

次の例では、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
```

次の例では、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する

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。

タスクの内容

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（ `true`または） `false`

  監査の状態がの場合、 `true`監査は有効になっています。監査の状態がの場合、 `false`監査は無効になります。

- 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. コマンドを使用して、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
```

カンサノセツテイノヘンコウヨウコマント

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と形式の変更、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できます。また、保存するログファイルの最大数の指定も可能です。

状況	使用するコマンド
ログのデスティネーションパスを変更します。	`vserver audit modify`パラメータを指定した場合 `-destination`
監査するイベントのカテゴリを変更する	`vserver audit modify`パラメータを指定した場合 `-events` 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。

ログ形式の変更	`vserver audit modify`パラメータを指定した場合 `-format`
内部的な一時ログファイルサイズに基づく自動保存の有効化	`vserver audit modify`パラメータを指定した場合 `-rotate-size`
時間間隔に基づいた自動保存の有効化	`vserver audit modify`を使用して、 `-rotate-schedule-dayofweek、 -rotate-schedule-day、、、 -rotate-schedule-hour`および `-rotate-schedule-minute`パラメータを指定します。 `-rotate-schedule-month`
保存されるログファイルの最大数の指定	`vserver audit modify`パラメータを指定した場合 `-rotate-limit`

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）がクラスタ内にあるときにONTAPが従うリバート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で開始されました。3.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または監査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と、問題が発生する可能性があります。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連するスペースの問題をトラブルシューティングする

イベントログファイルを含むボリュームの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ません。その結果、クライアントアクセスが失敗します。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拡張方法"です。
- "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"です。

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が失敗します。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、ユーザに問い合わせて、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どう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、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 `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。次の例は、管理SVM上にある4つのシステムボリュームを示しています。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が作成されたとき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          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の場合は、ボリュームのサイズを拡張する前に、アグリゲートのサイズを拡張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実行できません。

2GB未満（ONTAP 9.14.1以前）または5GB（ONTAP 9.151以降）の使用可能なスペースがあるアグリゲートが1つ以上あると、SVMの監査の作成が失敗します。SVMの監査の作成に失敗すると、作成されていたステージングボリュームが削除されます。

著作権に関する情報

商標に関する情報