監査の仕組み
ONTAP 9

NetApp
February 12, 2026

目次

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。