



監査の仕組み ONTAP 9

NetApp
February 12, 2026

目次

監査の仕組み	1
ONTAP監査の基本的な概念を学ぶ	1
ONTAP監査プロセスの機能について学習します	1
あるSVMで監査が有効になっている場合の処理	2
イベント ログの統合	2
監査の保証	2
ノードが利用できない場合の統合処理	2
イベント ログのローテーション	3
SVMで監査が無効になっている場合の処理	3

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、その後には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を確認されます。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。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。