ファイルおよびフォルダの監査ポリシーの設定
ONTAP 9

NetApp
February 12, 2026

目次

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。

著作権に関する情報

商標に関する情報