



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	1
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。	1
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	1
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	1
ONTAP CLIを使用したNTFS監査ポリシーの設定	4
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	4

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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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DAACL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

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。