



# ファイルおよびフォルダの監査ポリシーを設定する

## ONTAP 9

NetApp  
December 20, 2024

# 目次

ファイルおよびフォルダの監査ポリシーを設定する .....	1
ファイルおよびフォルダの監査ポリシーを設定する .....	1
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 .....	1
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 .....	4

# 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	<ol style="list-style-type: none"><li>a. [追加]*をクリックします。</li><li>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。</li><li>c. [OK]*をクリックします。</li></ol>
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"><li>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。</li><li>b. [削除 (Remove) ] をクリックします。</li><li>c. [OK]*をクリックします。</li><li>d. この手順の残りの部分はスキップしてください。</li></ol>
ユーザまたはグループの監査を変更する	<ol style="list-style-type: none"><li>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。</li><li>b. [編集 (Edit) ] をクリックします。</li><li>c. [OK]*をクリックします。</li></ol>

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

エ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`。

## 著作権に関する情報

Copyright © 2024 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。