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

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	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（ Remove ）] をクリックします。 c. [OK]*をクリックします。 d. この手順の残りの部分はスキップしてください。
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（ Edit ）] 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

ェ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

商標に関する情報