ファイル権限を使用したファイルアクセスの保護
ONTAP 9

NetApp
December 20, 2024

目次

ファイル権限を使用したファイルアクセスの保護

Windowsの[セキュリティ]タブを使用した詳細なNTFSファイル権限の設定

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、ファイルおよびフォルダの標準 NTFS ファイルアクセス権を構成できます。

開始する前に

このタスクを実行する管理者には、選択したオブジェクトの権限を変更するための十分なNTFS権限が必要です。

タスクの内容

NTFSファイル権限を設定するには、Windowsホストで、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）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。

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 *] ダイアログ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、権限を適用するデータと共有名を含む共有を含む CIFS サーバー名を入力します。

      CIFSサーバ名が「CIFS_SERVER」で、共有の名前が「'share1'」の場合は、と入力します。
      `\\CIFS_SERVER\share1`

      CIFSサーバ名の代わりに、CIFS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。

   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. NTFSファイル権限を設定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。

   Security タブには、 NTFS アクセス権が設定されているユーザーおよびグループのリストが表示されます。[* アクセス許可の対象 *] ボックスには、選択した各ユーザーまたはグループに対して有効な [許可] と [拒否] のアクセス許可のリストが表示されます。
6. 「 * 詳細設定 * 」をクリックします。

Windowsの[プロパティ]ウィンドウには、ユーザおよびグループに割り当てられている既存のファイル権限に関する情報が表示されます。

7. [権限の変更 *] をクリックします。

   [権限]ウィンドウが開きます。

8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループの詳細なNTFS権限を設定する	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、追加するユーザー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の詳細なNTFS権限を変更する	a. [* アクセス権エントリ： *] ボックスで、詳細なアクセス権を変更するユーザー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。
ユーザまたはグループの詳細なNTFS権限を削除する	a. [* アクセス許可エントリ： *] ボックスで、削除するユーザー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. 手順13に進みます。

   新しいユーザまたはグループに詳細な NTFS 権限を追加する場合、または既存のユーザまたはグループの NTFS 詳細権限を変更する場合は、 <Object> の権限エントリボックスが開きます。

9. [* 適用先 *] ボックスで、この NTFS ファイル許可エントリを適用する方法を選択します。

   1 つのファイルに NTFS ファイル権限を設定する場合、 * Apply to * ボックスはアクティブになりません。[* 適用先 * （ Apply to * ）] 設定のデフォルトは、 * このオブジェクトのみ * です。

10. [* アクセス許可 *] ボックスで、このオブジェクトに設定する詳細なアクセス許可の [* 許可 *] または [* 拒否 *] ボックスを選択します。

    - 指定したアクセスを許可するには、 * 許可 * ボックスを選択します。
    - 指定されたアクセスを許可しない場合は、 * Deny * ボックスを選択します。次の詳細な権限に対して権限を設定できます。
    - * フルコントロール *

      この詳細な権限を選択すると、他のすべての詳細な権限が自動的に選択されます（それらの権限が許可または拒否されます）。

    - * 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 *

> いずれかの詳細な権限ボックスが選択できない場合は、権限が親オブジェクトから継承されるためです。

11. このオブジェクトのサブフォルダとファイルにこれらのアクセス権を継承させる場合は、 [このコンテナ内のオブジェクトまたはコンテナにこれらのアクセス権を適用する *] ボックスをオンにします。
12. [OK]*をクリックします。
13. NTFS権限の追加、削除、または編集が完了したら、このオブジェクトの継承設定を指定します。
    - [このオブジェクトの親から継承可能な権限を含める *] ボックスをオンにします。

      これがデフォルトです。
    - [このオブジェクトから継承可能な権限ですべての子オブジェクトを置換する *] ボックスをオンにします。

      この設定は、単一ファイルに対してNTFSファイル権限を設定する場合は[権限]ボックスに表示されません。

      > この設定を選択する場合は注意が必要です。この設定では、すべての子オブジェクトに対する既存の権限がすべて削除され、このオブジェクトの権限設定に置き換えられます。削除したくない権限を誤って削除する可能性があります。これは、mixedセキュリティ形式のボリュームまたはqtreeで権限を設定する場合に特に重要です。子オブジェクトがUNIX対応のセキュリティ形式を使用している場合に、これらの子オブジェクトにNTFSアクセス権を適用すると、ONTAPによってこれらのオブジェクトがUNIXセキュリティ形式からNTFSセキュリティ形式に変更され、これらの子オブジェクトのすべてのUNIXアクセス権がNTFSアクセス権に置き換えられます。
    - 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。
14. **OK** をクリックして、 *Permissions * ボックスを閉じます。

15. OK * をクリックして、 * <Object>* の高度なセキュリティ設定ボックスを閉じます。

    詳細なNTFS権限の設定方法の詳細については、Windowsのマニュアルを参照してください。

関連情報

CLIを使用したNTFSファイルおよびフォルダに対するファイルセキュリティの設定と適用

NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

mixedセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

UNIXセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示

ONTAP CLIを使用したNTFSファイル権限の設定

ONTAP CLIを使用して、ファイルおよびディレクトリに対してNTFSファイル権限を設定できます。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ファイル権限を設定できます。

NTFSファイル権限を設定するには、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）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。

コマンドラインを使用して設定できるのはNTFSファイル権限のみです。CLIを使用してNFSv4 ACLを設定することはできません。

手順

1. NTFSセキュリティ記述子を作成します。

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. NTFSセキュリティ記述子にDACLを追加します。

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. ファイルやディレクトリのセキュリティポリシーを作成します。

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

SMB経由でファイルにアクセスする際のUNIXファイル権限によるアクセス制御方法

FlexVol ボリュームのセキュリティ形式は、 NTFS 、 UNIX 、 mixed の 3 種類のいずれかにすることができます。セキュリティ形式に関係なく SMB 経由でデータにアクセスできますが、 UNIX 対応のセキュリティを使用するデータにアクセスするには、適切な UNIX ファイル権限が必要になります。

SMB 経由でのデータへのアクセス時には、いくつかのアクセス制御を使用して、要求した操作を実行する権限がユーザにあるかどうかが判断されます。

- エクスポート権限

  SMB アクセスに関するエクスポート権限の設定はオプションです。

- 共有権限
- ファイル権限

  ユーザが操作を実行するデータには、次のタイプのファイル権限を適用できます。

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX モードビット

NFSv4 ACL または UNIX モードビットが設定されたデータの場合は、 UNIX 形式のアクセス権を使用してデータへのファイルアクセス権が決定されます。SVM 管理者は、適切なファイル権限を設定して、ユーザに目的のアクションを実行する権限が付与されるようにする必要があります。

mixed セキュリティ形式のボリューム内のデータでは、 NTFS または UNIX 対応のセキュリティ形式を使用できます。UNIX 対応のセキュリティ形式を使用するデータの場合は、データに対するファイル権限を判断するときに NFSv4 権限または UNIX モードビットが使用されます。

著作権に関する情報

商標に関する情報