ファイル権限を使用してファイルアクセスを保護
ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/smb-admin/configure-ntfs-windows-security-tab-task.html on September 12, 2024. Always check docs.netapp.com for the latest.

目次

ファイル権限を使用してファイルアクセスを保護 1
Windows のセキュリティタブを使用して、詳細な NTFS ファイル権限を設定します 1
ONTAP CLI を使用して NTFS ファイル権限を設定します 4
SMB 経由でファイルにアクセスする際の UNIX ファイルアクセス権によるアクセス制御方法 5

ファイル権限を使用してファイルアクセスを保護

Windows のセキュリティタブを使用して、詳細な NTFS ファイル権限を設定します

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。

作業を開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分な NTFS 権限を持っている必要があります。

このタスクについて

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。

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. [* フォルダー *] ボックスに、許可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て使用可能な状態になり、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. 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、ユーザーおよびグループに割り当てられている既存のファイルアクセス権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。

   [アクセス権] 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	実行する処理
新しいユーザまたはグループの詳細な NTFS 権限を設定します	a. [追加（ Add ）] 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 アクセス権を変更します	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。 次の詳細な権限に関する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を選択できない場合、その権限は親オブジェクトから継承されます。

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、 1 つのファイルに NTFS ファイルアクセス権を設定する場合は、 [アクセス権] ボックスには表示されません。

      > この設定を選択する場合は注意が必要です。この設定を選択すると、すべての子オブジェクトの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。削除する必要がなかった権限が誤って削除され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 でアクセス権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、このような子オブジェクトに NTFS 権限を適用すると、 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 権限が NTFS 権限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 を使用して、 NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します

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を表示する

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を表示する

ONTAP CLI を使用して NTFS ファイル権限を設定します

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を NTFS ファイルおよびディレクトリに適用します。

コマンドラインで設定できるのは NTFS ファイルアクセス権だけです。CLI で 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/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 ファイルアクセス権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

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権を有し、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権については、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。