



トラバースチェックのバイパスの設定

ONTAP 9

NetApp
December 20, 2024

目次

トラバースチェックのバイパスの設定	1
トラバースチェックのバイパスの設定の概要	1
ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する	2
ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止する	3

トラバースチェックのバイパスの設定

トラバースチェックのバイパスの設定の概要

トラバースチェックのバイパスは、トラバースするディレクトリに対する権限がユーザにない場合でも、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできるかどうかを判断するユーザ権限です。トラバースチェックのバイパスを許可または拒否した場合の動作と、Storage Virtual Machine (SVM) でのユーザに対するトラバースチェックのバイパスの設定方法を理解しておく必要があります。

トラバースチェックのバイパスを許可または拒否した場合の動作

- 許可した場合、ユーザがファイルにアクセスしようとする時、中間ディレクトリのトラバース権限がONTAPでチェックされず、ファイルへのアクセスの可否が判別されます。
- 拒否した場合、ONTAPはファイルのパスにあるすべてのディレクトリでトラバース（実行）権限をチェックします。

中間ディレクトリのいずれかに「X」（トラバース権限）がない場合、ONTAPはファイルへのアクセスを拒否します。

トラバースチェックのバイパスの設定

トラバースチェックのバイパスを設定するには、ONTAP CLIを使用するか、Active Directoryグループポリシーにこのユーザ権限を設定します。

権限は `SeChangeNotifyPrivilege`、ユーザにトラバースチェックのバイパスを許可するかどうかを制御します。

- この権限をSVMのローカルSMBユーザまたはグループ、ドメインユーザまたはグループに追加すると、トラバースチェックのバイパスを許可できます。
- この権限をSVMのローカルSMBユーザまたはグループ、ドメインユーザまたはグループから削除すると、トラバースチェックのバイパスが拒否されます。

SVMの次のBUILTINグループには、デフォルトでトラバースチェックのバイパス権限があります。

- BUILTIN\Administrators
- BUILTIN\Power Users
- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

これらのいずれかのグループのメンバーにトラバースチェックのバイパスを許可しない場合は、グループからこの権限を削除する必要があります。

CLIを使用してSVMのローカルSMBユーザおよびグループのトラバースチェックのバイパスを設定する場合は、次の点に注意する必要があります。

- カスタムのローカルグループまたはドメイングループのメンバーにトラバースチェックのバイパスを許可する場合は、そのグループに権限を追加する必要があります `SeChangeNotifyPrivilege`。
- ローカルユーザまたはドメインユーザにトラバースチェックのバイパスを個別に許可し、そのユーザがその権限を持つグループのメンバーでない場合は、そのユーザアカウントに権限を追加できます `SeChangeNotifyPrivilege`。
- ローカルまたはドメインのユーザやグループに対するトラバースチェックのバイパスをいつでも無効にするには、権限を削除し `SeChangeNotifyPrivilege` ます。



特定のローカルまたはドメインのユーザまたはグループに対してトラバースチェックのバイパスを無効にするには、グループから権限 `Everyone` も削除する必要があります `SeChangeNotifyPrivilege`。

関連情報

[ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する](#)

[ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止する](#)

[ボリュームでのSMBファイル名の変換のための文字マッピングの設定](#)

[SMB共有のアクセス制御リストの作成](#)

[ストレージレベルのアクセス保護を使用したファイルアクセスの保護](#)

[サポートされるPrivilegesのリスト](#)

[ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加](#)

ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する

トラバースするディレクトリに対する権限がない場合でも、ファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできるようにするには、Storage Virtual Machine (SVM) のローカルSMBユーザまたはグループに権限を追加します `SeChangeNotifyPrivilege`。デフォルトでは、ユーザはディレクトリのトラバースチェックをバイパスできます。

開始する前に

- SVM上にSMBサーバが存在している必要があります。
- ローカルユーザとローカルグループのSMBサーバオプションが有効になっている必要があります。
- 権限を追加するローカルまたはドメインのユーザまたはグループ `SeChangeNotifyPrivilege` がすでに存在している必要があります。

タスクの内容

Privilegesをドメインユーザまたはグループに追加するときに、ONTAPがドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに権限を追加して、トラバースチェックのバイパスを有効にし `SeChangeNotifyPrivilege``ます。 ``vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege``

パラメータの値は `-user-or-group-name`、ローカルユーザまたはグループ、ドメインユーザまたはグループです。

2. 指定したユーザまたはグループでトラバースチェックのバイパスが有効になっていることを確認します。
`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name``

例

次のコマンドは、「example\eng」グループに権限を追加することで、「example\eng」グループに属するユーザがディレクトリのトラバースチェックをバイパスできるようにし ``SeChangeNotifyPrivilege``ます。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng             SeChangeNotifyPrivilege
```

関連情報

[ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスの禁止](#)

ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止する

トラバースするディレクトリに対する権限がないためにファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできないようにするには、Storage Virtual Machine (SVM) のローカルSMBユーザまたはグループから権限を削除します `SeChangeNotifyPrivilege``。

開始する前に

Privilegesを削除するローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

タスクの内容

ドメインユーザまたはグループからPrivilegesを削除する場合、ONTAPはドメインコントローラに接続してドメインユーザまたはグループを検証することがあります。ONTAPがドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. トラバースチェックのバイパスを禁止します。 `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

コマンドは、パラメータの値で指定したローカルまたはドメインのユーザまたはグループから権限を `-user-or-group-name name``削除します `SeChangeNotifyPrivilege。

2. 指定したユーザまたはグループに対してトラバースチェックのバイパスが無効になっていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次のコマンドを実行すると、「EXAMPLE\eng」グループに属するユーザに対して、ディレクトリのトラバースチェックのバイパスが禁止されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              -
```

関連情報

[ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスの許可](#)

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。