



ONTAPによるファイルアクセスの制御方法

ONTAP 9

NetApp
December 20, 2024

目次

ONTAPによるファイルアクセスの制御方法	1
ONTAPによるファイルアクセスの制御方法の概要	1
認証ベースの制限	1
ファイルベースの制限	1

ONTAPによるファイルアクセスの制御方法

ONTAPによるファイルアクセスの制御方法の概要

ONTAP は、指定された認証ベースおよびファイルベースの制限に従って、ファイルアクセスを制御します。

クライアントがファイルにアクセスするためにストレージシステムに接続するとき、ONTAP は 2 つのタスクを実行する必要があります。

- 認証

ONTAP は、信頼できるソースで ID を検証して、クライアントを認証する必要があります。また、クライアントの認証タイプは、エクスポートポリシーの設定時にクライアントがデータにアクセスできるかどうかの判断に使用できる方法の 1 つです（CIFS の場合は省略可能）。

- 許可

ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに設定されている権限を比較し、提供するアクセスのタイプ（ある場合）を判別することで、ユーザを許可する必要があります。

ファイルアクセス制御を適切に管理するため、ONTAP は、NIS、LDAP、および Active Directory サーバなどの外部サービスと通信します。CIFS または NFS を使用するストレージシステムのファイルアクセスを設定するには、ONTAP の環境に応じて、サービスを適切に設定する必要があります。

認証ベースの制限

認証ベースの制限を使用すると、Storage Virtual Machine (SVM) に接続できるクライアントマシンおよびユーザを指定できます。

ONTAP は、UNIX サーバおよび Windows サーバの両方からの Kerberos 認証をサポートします。

ファイルベースの制限

ONTAP では、3 つのレベルのセキュリティを評価して、SVM 上にあるファイルおよびディレクトリに対して要求された操作を実行する権限がエンティティにあるかどうかを判断します。アクセスは、3 つのセキュリティレベルの評価後に有効な権限によって判断されます。

どのストレージオブジェクトにも、最大 3 種類のセキュリティレイヤを含めることができます。

- エクスポート (NFS) および共有 (SMB) セキュリティ

エクスポートおよび共有セキュリティは、特定の NFS エクスポートまたは SMB 共有へのクライアントアクセスに適用されます。管理 Privileges を持つユーザは、SMB クライアントおよび NFS クライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルとディレクトリのセキュリティ

ストレージレベルのアクセス保護セキュリティは、SVMボリュームへのSMBおよびNFSクライアントアクセスに適用されます。NTFSのアクセス権限のみがサポートされます。ONTAPがストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスするUNIXユーザのセキュリティチェックを実行するには、UNIXユーザがボリュームを所有するSVM上のWindowsユーザにマッピングされている必要があります。



NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護セキュリティは表示されません。システム (Windows または UNIX) 管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。

- NTFS、UNIX、およびNFSv4の標準のファイルレベルセキュリティ

ストレージオブジェクトを表すファイルまたはディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスにSMBとNFSのどちらを使用するかに関係なく有効です。

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。