



ロールベースアクセス制御 ONTAP tools for VMware vSphere 10

NetApp
April 17, 2025

目次

ロールベースアクセス制御	1
ONTAP tools for VMware vSphereでのロールベースアクセス制御の概要	1
vCenter Serverのロールの割り当てと変更に関するキーポイント	1
ONTAP Tools for VMware vSphereに付属の標準ロール	2
ONTAPストレージバックエンドとvSphereオブジェクトの権限	2
vCenter Serverアクセス許可のコンポーネント	2
権限	3
vSphereオブジェクト	4
ユーザとグループ	4
vCenter Serverの権限の割り当てと変更	4
権限の割り当て	4
アクセス許可と非vSphereオブジェクト	5
アクセス許可の変更	5
ONTAP Tools for VMware vSphereのタスクに必要な権限	5
ONTAP Tools for VMware vSphereで推奨されるONTAPロール	6

ロールベースアクセス制御

ONTAP tools for VMware vSphereでのロールベースアクセス制御の概要

vCenter Serverには、vSphereオブジェクトへのアクセスを制御するためのRole-Based Access Control (RBAC ; ロールベースアクセス制御) が用意されています。vCenter Serverは、ロールとPrivilegesでユーザ権限とグループ権限を使用して、インベントリ内のさまざまなレベルで一元的な認証および承認サービスを提供します。

コンポーネント	製品説明
権限	vSphereで操作を実行するためのアクセスを有効または拒否します。
役割	ロールには、1つ以上のシステム権限が含まれています。各権限は、システム内の特定のオブジェクトまたはタイプのオブジェクトに対する管理権限を定義します。ユーザにロールを割り当てると、そのロールで定義されている権限の機能が継承されます。
ユーザとグループ	ユーザとグループは、Active Directory (AD) からロールを割り当てる権限で使用されます。vCenter Serverには、使用可能な独自のローカルユーザとローカルグループがあります。
権限	権限を使用すると、Privilegesをユーザまたはグループに割り当てて、特定の操作を実行し、vCenter Server内のオブジェクトに変更を加えることができます。vCenter Serverの権限は、ESXiホストに直接ログインするユーザではなく、vCenter Serverにログインするユーザにのみ影響します。
オブジェクト	アクションが実行されるエンティティ。VMware vCenterオブジェクトは、データセンター、フォルダ、リソースプール、クラスタ、ホスト、およびVM

タスクを完了するには、適切なvCenter Server RBACロールが必要です。タスクの実行中、ONTAP tools for VMware vSphereは、ユーザのvCenter Serverロールを確認してから、ユーザのONTAP権限を確認します。



vCenter Serverのロールは、管理者ではなく、ONTAP Tools for VMware vSphere vCenterユーザに適用されます。デフォルトでは、管理者は製品へのフルアクセス権を持ち、ロールを割り当てる必要はありません。

ユーザとグループは、vCenter Serverロールに含まれることでロールにアクセスできます。

vCenter Serverのロールの割り当てと変更に関するキーポイント

vCenter Serverのロールは、vSphereのオブジェクトおよびタスクへのアクセスを制限する場合にのみ設定します。それ以外の場合は、管理者としてログインできます。このログインにより、すべてのvSphereオブジェクトに自動的にアクセスできるようになります。

ルールを割り当てる場所によって、ユーザが実行できるONTAP Tools for VMware vSphereタスクが決まります。一度に1つのルールを変更できます。ルール内の権限を変更した場合、そのルールに関連付けられているユーザは、更新されたルールを有効にするためにログアウトしてから再度ログインする必要があります。

ONTAP Tools for VMware vSphereに付属の標準ルール

vCenter Serverの権限とRBACを簡単に使用できるように、ONTAP Tools for VMware vSphereには、主要なONTAPツールfor VMware vSphereタスクを実行できる標準のONTAPツールfor VMware vSphereルールが用意されています。タスクを実行せずに情報を表示できる読み取り専用ルールもあります。

ONTAP Tools for VMware vSphereの標準ルールを表示するには、vSphere Clientのホームページで*[ルール]*をクリックします。ONTAP Tools for VMware vSphereのルールで、次のタスクを実行できます。

* 役割 *	* 概要 *
VMware vSphere管理者向けNetApp ONTAPツール	ONTAP tools for VMware vSphereの一部のタスクを実行するために必要なvCenter Server標準の権限とONTAP tools固有の権限がすべて含まれています。
NetApp ONTAP Tools for VMware vSphere読み取り専用	ONTAP toolsへの読み取り専用アクセスを許可します。アクセスが制御されたONTAP tools for VMware vSphereアクションを実行することはできません。
NetApp ONTAP Tools for VMware vSphereのプロビジョニング	ストレージのプロビジョニングに必要なvCenter Server標準の権限とONTAP tools固有の権限が含まれています。次のタスクを実行できます。 <ul style="list-style-type: none">• 新しいデータストアを作成する• データストアの管理

ONTAP tools Managerの管理者ルールがvCenter Serverに登録されていません。このルールは、ONTAP tools Managerに固有です。

標準のONTAP tools for VMware vSphereルールよりも制限の厳しいルールを実装する必要がある場合は、ONTAP tools for VMware vSphereルールを使用して新しいルールを作成できます。

この場合は、必要なONTAP tools for VMware vSphereルールのクローンを作成し、そのクローンを編集してユーザに必要な権限だけを付与します。

ONTAPストレージバックエンドとvSphereオブジェクトの権限

vCenter Serverアクセス許可が十分であれば、ONTAP tools for VMware vSphereは、ストレージバックエンドのクレデンシャル（ユーザ名とパスワード）に関連付けられているONTAP RBAC権限（ONTAPルール）を確認します。そのストレージバックエンドでONTAP tools for VMware vSphereタスクに必要なストレージ処理を実行するための十分な権限があるかどうかを確認する。正しいONTAP Privilegesがあれば、ストレージバックエンドにアクセスしてONTAP Tools for VMware vSphereタスクを実行できます。ストレージバックエンドで実行できるONTAP Tools for VMware vSphereタスクは、ONTAPルールで決まります。

vCenter Serverアクセス許可のコンポーネント

vCenter Serverで認識されるのはアクセス許可で、Privilegesではありません。各vCenter

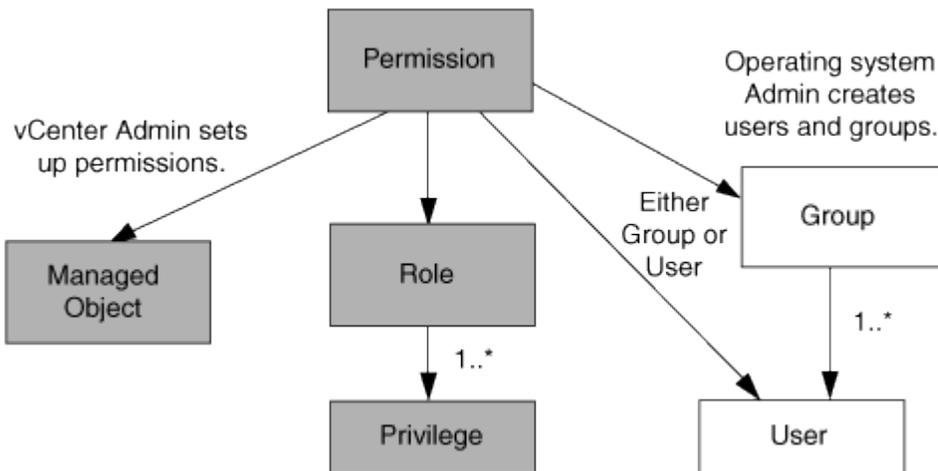
Serverアクセス許可は3つのコンポーネントで構成されます。

vCenter Serverには次のコンポーネントがあります。

- 1つ以上のPrivileges (ロール)
ユーザが実行できるタスクを定義します。
- vSphereオブジェクト
オブジェクトはタスクのターゲットです。
- ユーザまたはグループ
タスクを実行できるユーザまたはグループを定義します。



グレーのボックスはvCenter Serverにあるコンポーネント、白のボックスはvCenter Serverを実行しているオペレーティングシステムにあるコンポーネントを示しています。



権限

ONTAP Tools for VMware vSphereには、次の2種類のPrivilegesが関連付けられています。

- vCenter Server Privileges標準
これらのPrivilegesはvCenter Serverに付属しています。

- ONTAP tools固有のPrivileges

これらの権限は、特定のONTAP Tools for VMware vSphereタスク用に定義されています。ONTAP Tools for VMware vSphereに固有の機能です。

ONTAP tools for VMware vSphereのタスクには、ONTAP tools固有の権限とvCenter Server標準の権限の両方が必要です。これらの権限は'ユーザーのロールを構成しますアクセス許可には複数の権限を含めることができます。これらのPrivilegesは、vCenter Serverにログインしているユーザ用です。



vCenter Server RBACの使用を簡易化するために、ONTAP tools for VMware vSphereには、ONTAP tools for VMware vSphereタスクの実行に必要なONTAP tools固有の権限と標準の権限をすべて含む標準ロールがいくつか用意されています。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

vSphereオブジェクト

アクセス許可はvSphereオブジェクトに関連付けられます。vCenter Server、ESXiホスト、仮想マシン、データストア、データセンター、フォルダなどがあります。任意のvSphereオブジェクトに権限を割り当てることができます。vSphereオブジェクトに割り当てられたアクセス許可に基づいて、そのオブジェクトに対してどのユーザがどのタスクを実行できるかがvCenter Serverによって決まります。ONTAP tools for VMware vSphere固有のタスクの場合、アクセス許可の割り当てと検証はルートフォルダレベル（vCenter Server）でのみ行われ、他のエンティティでは行われません。ただしVAAIプラグインの処理は例外で、該当するESXiホストに対して権限が検証されます。

ユーザとグループ

ユーザとグループは、Active Directory（またはローカルのvCenter Serverマシン）を使用して設定できます。その後、vCenter Serverアクセス許可を使用してこれらのユーザまたはグループにアクセスを許可し、特定のONTAP Tools for VMware vSphereタスクを実行できるようにします。



これらのvCenter Serverアクセス許可は、ONTAP tools for VMware vSphere vCenterユーザに適用され、ONTAP tools for VMware vSphere管理者には適用されません。ONTAP tools for VMware vSphereの管理者には、デフォルトでフルアクセス権が付与され、権限を割り当てる必要はありません。

ユーザとグループにはロールは割り当てられません。vCenter Serverアクセス許可に含まれることでロールにアクセスできます。

vCenter Serverの権限の割り当てと変更

vCenter Serverのアクセス許可を使用する場合は、いくつかの重要な点に注意する必要があります。ONTAP tools for VMware vSphereのタスクを実行できるかどうかは、アクセス許可を割り当てた場所や、アクセス許可の変更後にユーザが実行した操作によって異なります。

権限の割り当て

vCenter Serverのアクセス許可は、vSphereのオブジェクトおよびタスクへのアクセスを制限する場合にのみ設定します。それ以外の場合は、管理者としてログインできます。このログインにより、すべてのvSphereオブジェクトに自動的にアクセスできるようになります。

権限の割り当て先によって、ユーザが実行できるONTAP tools for VMware vSphereタスクが決まります。

場合によっては、タスクを確実に完了させるために、ルートオブジェクトなどの上位レベルに権限を割り当てる必要があります。これは、特定のvSphereオブジェクトには適用されない権限（タスクの追跡など）がタスクに必要な場合や、必要な権限がvSphere以外のオブジェクト（ストレージシステムなど）に適用される場合

に該当します。

このような場合は、子エンティティに継承されるようにアクセス許可を設定できます。子エンティティに他の権限を割り当てることもできます。子エンティティに割り当てたアクセス許可は、親エンティティから継承されたアクセス許可を上書きします。つまり、子エンティティにアクセス許可を付与して、ルートオブジェクトに割り当てられ、子エンティティに継承されるアクセス許可の範囲を制限できます。



会社のセキュリティポリシーでアクセス許可の制限が厳しい場合を除き、ルートオブジェクト（ルートフォルダとも呼ばれます）にアクセス許可を割り当てることをお勧めします。

アクセス許可と非vSphereオブジェクト

作成したアクセス許可はvSphere以外のオブジェクトに適用されます。たとえば、ストレージシステムはvSphereオブジェクトではありません。ストレージシステムの環境権限がある場合は、tools for VMware vSphereルートオブジェクトに割り当てることができるvSphereオブジェクトがないため、その権限を含むアクセス許可をONTAP tools for VMware vSphereルートオブジェクトに割り当てする必要があります。

たとえば、ONTAP tools for VMware vSphereの「Add/Modify/Skip storage systems」などの権限を含むすべてのアクセス許可は、ルートオブジェクトレベルに割り当てする必要があります。

アクセス許可の変更

変更できる権限は一度に1つです。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

ONTAP Tools for VMware vSphereのタスクに必要な権限

ONTAP Tools for VMware vSphereのタスクごとに、ONTAP Tools for VMware vSphere固有の権限とvCenter Server標準の権限の組み合わせが異なります。

ONTAP tools for VMware vSphere GUIにアクセスするには、製品レベルのONTAP tools固有のView権限が、適切なvSphereオブジェクトレベルで割り当てられている必要があります。この権限なしでログインすると、NetAppアイコンをクリックしたときにONTAP tools for VMware vSphereにエラーメッセージが表示され、ONTAP toolsにアクセスできません。

View *権限では、VMware vSphere用のONTAPツールにアクセスできます。この権限では、ONTAP tools for VMware vSphere内でタスクを実行することはできません。ONTAP tools for VMware vSphereのタスクを実行するには、タスクに対する適切なONTAP tools固有の権限とvCenter Server標準の権限が必要です。

割り当てレベルによって、UIのどの部分を表示できるかが決まります。ルートオブジェクト（フォルダ）にView権限を割り当てると、NetAppアイコンをクリックしてONTAP tools for VMware vSphereにアクセスできるようになります。

別のvSphereオブジェクトレベルにView権限を割り当てることもできますが、その場合、表示および使用できるONTAP Tools for VMware vSphereメニューが制限されます。

View権限を含むアクセス許可は、ルートオブジェクトに割り当ててを推奨します。

ONTAP Tools for VMware vSphereで推奨されるONTAPロール

ONTAP tools for VMware vSphereおよびRole-Based Access Control (RBAC ; ロールベースアクセス制御) を使用する際に推奨されるONTAPロールを設定できます。これらのロールには、ONTAP tools for VMware vSphereタスクで実行するストレージ処理の実行に必要なONTAP権限が含まれています。

新しいユーザロールを作成するには、ONTAPを実行するストレージシステムの管理者としてログインする必要があります。ONTAP System Manager 9.8P1以降を使用してONTAPロールを作成できます。

各ONTAPロールには、ロールのクレデンシャルを構成するユーザ名とパスワードのペアが関連付けられています。このクレデンシャルを使用してログインしないと、ロールに関連付けられたストレージ処理にアクセスできません。

セキュリティ対策として、ONTAP Tools for VMware vSphere固有のONTAPロールは階層構造になっています。最初のロールは最も制限が高く、ONTAP tools for VMware vSphereのストレージ処理の最も基本的なセットに関連する権限のみが含まれています。次のロールには、そのロール独自の権限と、前のロールに関連付けられているすべての権限が含まれます。ロールを追加するたびに、サポートされるストレージ処理に対する制限が少なくなります。

ONTAP Tools for VMware vSphereを使用する際に推奨されるONTAP RBACロールの一部を次に示します。ロールを作成したら、仮想マシンのプロビジョニングなど、ストレージに関するタスクを実行する必要があるユーザに割り当てることができます。

* 役割 *	権限
調査	ストレージシステムを追加できます。
ストレージの作成	ストレージを作成できます。また、Discoveryロールに関連付けられているすべての権限が含まれます。
ストレージの変更	ストレージを変更できます。また、DiscoveryロールとCreate Storageロールに関連付けられているすべての権限が含まれます。
ストレージの削除	ストレージを破棄できます。また、Discoveryロール、Create Storageロール、Modify Storageロールに関連付けられているすべての権限が含まれます。

ONTAP tools for VMware vSphereを使用している場合は、Policy-Based Management (PBM ; ポリシーベース管理) ロールも設定します。ストレージポリシーを使用してストレージを管理できます。このロールを使用するには、「検出」ロールも設定する必要があります。

著作権に関する情報

Copyright © 2025 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。