



# ロールベースアクセス制御

## ONTAP tools for VMware vSphere 10

NetApp  
September 30, 2025

# 目次

ロールベースアクセス制御 .....	1
ONTAP ツール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 ツール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
VMware vSphere 用の ONTAP ツールを使用する際に推奨される ONTAP ロール .....	2

# ロールベースアクセス制御

## ONTAP ツールでのロールベースアクセス制御の概要

vCenter Server の RBAC を使用すると、vSphere オブジェクトへのアクセスを制御できます。vCenter Serverは、ロールと権限を持つ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許可サービスを提供します。vCenter Serverには、RBACを管理するための5つの主要コンポーネントがあります。

コンポーネント	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。
ロール	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) または潜在的にローカルのWindowsユーザ/グループからロールを割り当てる権限に使用される（推奨されません）
権限	権限を使用すると、ユーザまたはグループに権限を割り当てて、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アクセス許可は、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の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。このログインでは、すべてのvSphereオブジェクトに自動的にアクセスできます。

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 ツール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には、ONTAP toolsの主要なタスクを実行できる標準のONTAP tools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のルールで実行できるタスクは次のとおりです。

* 役割 *	* 概要 *
NetApp ONTAPツール管理者	ONTAP tools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。これらのユーザは、アクセス制御されたONTAP toolsアクションを実行できません。
NetApp ONTAPツールプロビジョニング	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"><li>• 新しいデータストアを作成する</li><li>• データストアを管理します</li></ul>

Manager UI管理者ルールがvCenterに登録されていません。このルールはマネージャUIに固有です。

標準のONTAP tools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ルールのクローンを作成し、そのクローンルールを編集してユーザに必要な権限のみを付与します。

## ONTAPストレージバックエンドとvSphereオブジェクトの権限

十分なvCenter Serverアクセス許可がある場合、ONTAP toolsは次に、ストレージバックエンドのクレデンシヤル（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。適切なONTAP権限があれば、ストレージバックエンドを使用し、ONTAP toolsタスクを実行します。ストレージバックエンドで実行できるONTAP toolsタスクは、ONTAPルールによって決まります。

## VMware vSphere 用の ONTAP ツールを使用する際に推奨される ONTAP ロール

VMware vSphere および Role-Based Access Control （ RBAC ； ロールベースアクセス

制御) 用の ONTAP ツールを使用する際に推奨される ONTAP ロールをいくつか設定  
できます。これらのロールには、ONTAP tools タスクで実行するストレージ処理に必要な  
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 を実行しているストレージシステムに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。を参照し  
てください "[管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト](#)" を参照してく  
ださい。

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 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  
も制限のあるロールで、ONTAP tools の最も基本的なストレージ処理に関連する権限だけが含まれます。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。以降、  
上位のロールほど制限が少なく、より多くのストレージ処理をサポートします。

ONTAP tools 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そのロールを  
割り当てることができます。

#### 1. 検出

ストレージシステムを追加できます。

#### 2. ストレージを作成します

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。

#### 3. ストレージを変更します

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。

#### 4. ストレージを破棄します

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。

VASA Provider for ONTAP を使用する場合は、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。