



ONTAP を使用した RBAC

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目次

ONTAP を使用した RBAC	1
ONTAP RBAC が ONTAP tools と連携する仕組み	1
管理オプションの概要	1
ONTAP REST ロールの操作	1
ONTAP tools に関する ONTAP RBAC の考慮事項	2
設定プロセスの概要	2
システムマネージャーを使用してロールを設定する	3

ONTAP を使用した RBAC

ONTAP RBAC が ONTAP tools と連携する仕組み

ONTAPは、堅牢で拡張性の高いRBAC環境を提供します。RBAC機能を使用して、REST APIおよびCLIを通じて公開されるストレージおよびシステム操作へのアクセスを制御できます。ONTAP tools for VMware vSphere 10の展開で使用する前に、この環境に慣れておくことをお勧めします。

管理オプションの概要

環境と目標に応じて、ONTAP RBAC を使用する際に利用できるオプションがいくつかあります。以下に、主要な管理上の決定事項の概要を示します。詳細については、["ONTAP Automation：RBACセキュリティの概要"](#)も参照してください。



ONTAP RBACはストレージ環境に合わせて調整されており、vCenter Serverに付属のRBAC実装よりもシンプルです。ONTAPでは、ユーザーに役割を直接割り当てます。vCenter Serverで使用されるような明示的な権限の設定は、ONTAP RBACでは不要です。

役割と権限の種類

ONTAPユーザーを定義する際には、ONTAPロールが必要です。ONTAPロールには2種類あります：

- REST

REST ロールは ONTAP 9.6 で導入され、REST API を通じて ONTAP にアクセスするユーザーに一般的に適用されます。これらのロールに含まれる権限は、ONTAP REST API エンドポイントおよび関連するアクションへのアクセスという観点から定義されます。

- 従来型

これらは、ONTAP 9.6 より前に存在していたレガシーロールです。これらは RBAC の根幹を成す要素であり続けています。権限は、ONTAP CLI コマンドへのアクセスに関して定義されます。

RESTロールは比較的最近導入されたものですが、従来のロールにもいくつかの利点があります。たとえば、追加のクエリパラメータを含めることで、権限が適用されるオブジェクトをより正確に定義できるようになります。

Scope

ONTAP ロールは、2つの異なるスコープのいずれかで定義できます。特定のデータSVM（SVMレベル）またはONTAPクラスター全体（クラスターレベル）に適用できます。

役割の定義

ONTAPは、クラスターレベルとSVMレベルの両方で、事前定義された一連のロールを提供します。カスタムロールを定義することもできます。

ONTAP REST ロールの操作

ONTAP tools for VMware vSphere 10 に含まれる ONTAP REST ロールを使用する際には、いくつかの考慮事

項があります。

役割マッピング

従来型ロールでもRESTロールでも、すべてのONTAPアクセス権限の決定は、基となるCLIコマンドに基づいて行われます。ただし、RESTロールの権限はREST APIエンドポイントの観点で定義されているため、ONTAPは各RESTロールに対してマッピングされた従来のロールを作成する必要があります。したがって、各RESTロールは基盤となる従来のロールに対応付けられます。これにより、ONTAPはロールの種類に関係なく、一貫した方法でアクセス制御の決定を行うことができます。並列マッピングされたロールは変更できません。

CLI権限を使用してRESTロールを定義する

ONTAPは常にCLIコマンドを使用して基本レベルでのアクセスを決定するため、RESTエンドポイントの代わりにCLIコマンドの権限を使用してRESTロールを表現することが可能です。このアプローチの利点の1つは、従来のロールで利用できる詳細な設定が可能になることです。

ONTAPロールを定義する際の管理インターフェース

ユーザーとロールは、ONTAP CLI と REST API を使用して作成できます。ただし、ONTAP tools Manager から入手できる JSON ファイルとともに System Manager インターフェースを使用する方が便利です。詳細については、["ONTAP tools for VMware vSphere 10 で ONTAP RBAC を使用する"](#)を参照してください。

ONTAP tools に関する ONTAP RBAC の考慮事項

ONTAP tools for VMware vSphere 10 の ONTAP との RBAC 実装には、本番環境で使用する前に考慮すべきいくつかの側面があります。

設定プロセスの概要

ONTAP tools for VMware vSphereには、カスタムロールを持つONTAPユーザーの作成のサポートが含まれています。定義はJSONファイルにパッケージ化されており、ONTAPクラスタにアップロードできます。ユーザーを作成し、環境やセキュリティ要件に合わせてロールをカスタマイズできます。

主な設定手順の概要を以下に説明します。詳細については、["ONTAP ユーザーロールと権限の設定"](#)を参照してください。

1. 準備

ONTAP tools Manager と ONTAP クラスタの両方に管理者資格情報が必要です。

2. JSON定義ファイルをダウンロードする

ONTAP tools Manager のユーザーインターフェースにサインインした後、RBAC 定義を含む JSON ファイルをダウンロードできます。

3. ロールを持つ ONTAP ユーザーを作成する

システムマネージャーにサインインした後、ユーザーとロールを作成できます。

1. 左側の「クラスター」を選択し、次に「設定」を選択します。
2. 「ユーザーとロール」までスクロールダウンして「→」をクリックします。
3. 「ユーザー」の下にある「追加」を選択し、「仮想化製品」を選択します。
4. ローカルワークステーション上のJSONファイルを選択してアップロードしてください。

4.役割を設定する

役割を定義する過程で、いくつかの管理上の決定を下す必要があります。詳細については、[\[システムマネージャーを使用してロールを設定する\]](#)を参照してください。

システムマネージャーを使用してロールを設定する

システムマネージャーを使用して新しいユーザーとロールの作成を開始し、JSONファイルをアップロードした後、環境とニーズに基づいてロールをカスタマイズできます。

コアユーザーとロールの設定

RBACの定義は、VSC、VASAプロバイダー、SRAの組み合わせなど、いくつかの製品機能としてパッケージ化されています。RBACサポートが必要な環境を選択してください。例えば、リモートプラグイン機能をサポートするロールが必要な場合は、VSCを選択します。ユーザー名とそれに関連付けられたパスワードも選択する必要があります。

権限

ロール権限は、ONTAP ストレージに必要なアクセス レベルに基づいて 4 つのセットに分けられています。ロールの基となる権限には次のものがあります：

- Discovery

ストレージ システムを追加できます。

- ストレージの作成

このロールにより、ストレージを作成できます。また、検出ロールに関連付けられたすべての権限も含まれます。

- ストレージを変更する

この役割により、ストレージを変更できます。また、ストレージロールの検出および作成に関連するすべての権限も含まれます。

- ストレージを削除する

このロールを使用すると、ストレージを削除できます。また、ストレージの検出、作成、および変更といったロールに関連するすべての権限も含まれます。

役割を持つユーザーを生成する

環境の構成オプションを選択したら、「追加」をクリックすると、ONTAPによってユーザーとロールが作成されます。生成されるロールの名前は、以下の値を連結したものです。

- JSONファイルで定義された定数プレフィックス値（例：「OTV_10」）
- 選択した製品機能
- 権限セットの一覧。

例

新しいユーザーは、「ユーザーと役割」ページの一覧に追加されます。HTTPとONTAPIの両方のユーザーログイン方法がサポートされていることに注意してください。

著作権に関する情報

Copyright © 2026 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。