ONTAPを使用した RBAC

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/ontap-tools-vmware-vsphere-104/concepts/rbac-ontap-environment.html on November 04, 2025. Always check docs.netapp.com for the latest.

目次

ONTAPを使用した RBAC

ONTAP tools for VMware vSphereを使用したONTAP RBAC環境

ONTAP は、堅牢で拡張可能な RBAC 環境を提供します。 RBAC 機能を使用すると、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を使用する前に、環境をよく理解しておくと役立ちます。

管理オプションの概要

ONTAP RBAC を使用する場合、環境と目的に応じていくつかのオプションが利用できます。主要な行政上の決定の概要は以下のとおりです。こちらもご覧ください "ONTAP Automation: RBAC セキュリティの概要"詳細についてはこちらをご覧ください。

> ONTAP RBAC はストレージ環境に合わせて調整されており、vCenter Server で提供される RBAC 実装よりもシンプルです。ONTAPでは、ロールをユーザーに直接割り当てます。ONTAP RBAC では、vCenter Server で使用されるような明示的な権限の設定は必要ありません。

役割と権限の種類

ONTAPユーザーを定義するときは、 ONTAPロールが必要です。 ONTAPロールには 2 つの種類があります。

- REST

  REST ロールはONTAP 9.6 で導入され、通常は REST API を介してONTAPにアクセスするユーザーに適用されます。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の観点から定義されます。

- 伝統的

  これらは、 ONTAP 9.6 より前に含まれていたレガシー ロールです。これらは引き続き RBAC の基本的な側面です。権限は、 ONTAP CLI コマンドへのアクセスの観点から定義されます。

REST ロールは最近導入されましたが、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 パラメータをオプションで含めることができるため、権限が適用されるオブジェクトがより正確に定義されます。

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。これらは、特定のデータ SVM (SVM レベル) またはONTAPクラスタ全体 (クラスタ レベル) に適用できます。

役割の定義

ONTAP は、クラスタ レベルと SVM レベルの両方で事前定義されたロールのセットを提供します。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に含まれているONTAP REST ロールを使用する場合は、いくつかの考慮事項があります。

役割マッピング

従来のロールを使用する場合でも、REST ロールを使用する場合でも、すべてのONTAPアクセスの決定は、基盤となる 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 エンドポイントに基づいて定義されるため、 ONTAP は各 REST ロールに対してマップ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、基礎となる従来のロールにマッピングされます。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。並列にマップされたロールを変更することはできません。

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 エンドポイントではなく CLI コマンド権限を使用して REST ロールを表現することができます。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追加の粒度です。

ONTAPロールを定義する際の管理インターフェース

ONTAP CLI および REST API を使用してユーザーとロールを作成できます。ただし、 ONTAPツール マネージャーから利用できる JSON ファイルとともに System Manager インターフェイスを使用する方が便利です。見る"ONTAP tools for VMware vSphereでONTAP RBAC を使用する"詳細についてはこちらをご覧ください。

ONTAP tools for VMware vSphereでONTAP RBAC を使用する

ONTAPを使用したONTAP tools for VMware vSphereには、実稼働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。

構成プロセスの概要

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、 ONTAPクラスターにアップロードできる JSON ファイルにパッケージ化されています。ユーザーを作成し、環境とセキュリティのニーズに合わせてロールをカスタマイズできます。

主要な構成手順の概要を以下に説明します。参照"ONTAPユーザーの役割と権限を構成する"詳細についてはこちらをご覧ください。

1.準備

ONTAPツール マネージャーとONTAPクラスターの両方の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 ユーザー インターフェイ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

System Manager にサインインしたら、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*までスクロールしてクリックします -→。
3. *ユーザー*の下の*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、アップロードします。

4.役割を構成する

役割を定義する一環として、いくつかの管理上の決定を行う必要があります。見る[システムマネージャを使用してロールを構成する]詳細についてはこちらをご覧ください。

システムマネージャを使用してロールを構成する

System Manager 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ら、環境とニーズに応じ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構成

RBAC 定義は、VSC、VASA プロバイダー、SRA の組み合わせを含む複数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する必要があります。たとえば、ロールでリモート プラグイン機能をサポートする場合は、VSC を選択します。ユーザー名と関連する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 つのセットに分類されます。ロールのベースとなる権限は次のとおりです。

- 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

  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ているすべての権限も含まれます。

- ストレージを変更する

  ストレージを変更できます。また、ストレージの検出および作成のロールに関連付けられているすべての権限も含まれます。

- ストレージを破壊する

  ストレージを破棄できます。また、検出、ストレージの作成、ストレージ ロールの変更に関連するすべての権限も含まれます。

ロールを持つユーザーを生成する

環境の設定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。生成されたロールの名前は、次の値の連結になります。

- JSON ファイルで定義された定数プレフィックス値 (例: "OTV_10")

- 選択した製品の機能
- 権限セットのリスト。

例

```
OTV_10_VSC_Discovery_Create
```

新しいユーザーは、「ユーザーとロール」ページのリストに追加されます。 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 © 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。