ONTAPを使用したRBAC

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/ontap-tools-vmware-vsphere-10/concepts/rbac-ontap-environment.html on September 29, 2025. Always check docs.netapp.com for the latest.

目次

ONTAPを使用したRBAC . . . 1
ONTAP RBAC環境とONTAP Tools for VMware vSphere 10 . . . 1
管理オプションの概要 . . . 1
ONTAP RESTロールの使用 . . . 2
ONTAP RBACとONTAP Tools for VMware vSphere 10の使用 . . . 2
セツテイフロセスノカイヨウ . . . 2
System Managerを使用してロールを設定する . . . 3

ONTAPを使用したRBAC

ONTAP RBAC環境とONTAP Tools for VMware vSphere 10

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で公開されるストレージおよびシステム処理へのアクセスを制御できます。ONTAP Tools for VMware vSphere 10環境で使用する前に、環境を理解しておくと役立ちます。

管理オプションの概要

ONTAP RBACを使用する際には、環境や目標に応じていくつかのオプションを使用できます。主な管理上の決定事項の概要を以下に示します。詳細については、も参照してください "ONTAPの自動化：RBACセキュリティの概要"。

> 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構成は必要ありません。

ロールと**Privileges**のタイプ

ONTAPユーザを定義するには、ONTAPロールが必要です。ONTAPロールには次の2種類があります。

- REST

  RESTロールはONTAP 9.6で導入されたもので、一般にREST APIを使用してONTAP にアクセスするユーザに適用されます。これらのロールに含まれるPrivilegesは、ONTAP REST APIエンドポイントへのアクセスと関連するアクションの観点から定義されます。

- 伝統的

  これらはONTAP 9.6より前のレガシーロールです。これらはRBACの基本的な側面であり続けています。Privilegesは、ONTAP CLIコマンドへのアクセスという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、従来のロールには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もできます。これにより、Privilegesは、追加のクエリパラメータが適用されるオブジェクトをより正確に定義できます。

適用範囲

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クラスタ全体（クラスタレベル）に適用できます。

ロールの定義

ONTAPには、クラスタレベルとSVMレベルの両方で事前定義された一連のロールが用意されています。カスタムロールを定義することもできます。

ONTAP RESTロールの使用

ONTAP tools for VMware vSphere 10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。

ロールマッピング

従来のロールを使用するかRESTロールを使用するかに関係なく、すべてのONTAPアクセスの決定は基になるCLIコマンドに基づいて行われます。ただし、RESTロールのPrivilegesはREST APIエンドポイントで定義されるため、ONTAPでは各RESTロールに対して_mapped_traditionalロールを作成する必要があります。そのため、各RESTロールは基盤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、ロールタイプ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。並行マッピングされたロールは変更できません。

CLI Privilegesを使用した**REST**ロールの定義

ONTAPでは常に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Privilegesを使用してRESTロールを表すことができます。このアプローチのメリットの1つは、従来の役割で利用できるきめ細かさです。

ONTAPロールを定義する際の管理インターフェイス

ONTAP CLIおよびREST APIを使用して、ユーザとロールを作成できます。ただし、System Managerのインターフェイスと ONTAP tools Managerから利用できるJSONファイルを使用する方が便利です。詳細については、を参照してください "ONTAP RBACとONTAP Tools for VMware vSphere 10の使用" 。

ONTAP RBACとONTAP Tools for VMware vSphere 10の使用

ONTAPでのONTAP Tools for VMware vSphere 10 RBACの実装については、本番環境で使用する前に考慮する必要があります。

セツテイフロセスノカイヨウ

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。

主な設定手順について、以下で大まかに説明します。"ONTAPユーザのロールと権限の設定"詳細については、を参照してください。

1.準備

ONTAP tools ManagerとONTAPクラスタの両方に対する管理クレデンシャルが必要です。

2.JSON定義ファイルをダウンロードする

ONTAP tools Managerのユーザインターフェイスにサインインしたら、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**ユーザを作成する

System Managerにサインインしたら、ユーザとロールを作成できます。

1. 左側の*を選択し、[設定]*を選択します。
2. [ユーザとロール]*まで下にスクロールし、をクリックします –→。

3. [Users]で[Add]*を選択し、[Virtualization products]*を選択します。
4. ローカルワークステーションでJSONファイルを選択してアップロードします。

4.ロールを設定する

ロールの定義の一環として、いくつかの管理上の決定を行う必要があります。詳細については、を参照してください System Managerを使用してロールを設定する。

System Managerを使用してロールを設定する

System Managerで新しいユーザ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、環境とニーズに基づいてロールをカスタマイズできます。

コアユーザとロールの設定

RBACの定義は、VSC、VASA Provider、SRAなど、複数の製品機能としてパッケージ化されています。RBACのサポートが必要な環境を選択してください。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。また、ユーザ名と関連するパスワードを選択する必要があります。

権限

Privilegesロールは、ONTAPストレージに必要なアクセスレベルに基づいて4セットに分類されます。ロールのベースとなるPrivilegesには次のものがあります。

- 検出

  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Privilegesも含まれます。

- ストレージの変更

  ストレージを変更できます。また、discoveryおよびcreate storageのロールに関連付けられているすべてのPrivilegesも含まれます。

- ストレージの削除

  ストレージを破棄できます。また、検出、ストレージの作成、ストレージの変更の各ロールに関連付けられているすべてのPrivilegesも含まれます。

ロールを持つユーザを生成する

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。生成されたロールの名前は、次の値を連結したものです。

- JSONファイルで定義された固定プレフィックス値（例：「OTV_10」）
- 選択した製品機能
- 権限セットのリスト。

例

```
OTV_10_VSC_Discovery_Create
```

新しいユーザーが「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。