ONTAPを使用したRBAC

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

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はストレージ環境専用に設計されており、vCenter Serverで提供されるRBACよりも簡単に実装できます。ONTAPでは、ユーザに直接ロールを割り当てます。vCenter Serverで使用するアクセス許可などを明示的に設定する必要はありません。ONTAP RBACでは必要ありません。

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 10では、カスタムロールを持つONTAPユーザの作成がサポートされます。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。ユーザを作成し、環境やセキュリティのニーズに合わせてロールを調整できます。

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。

- 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

商標に関する情報