役割ベースアクセス制御（RBAC）

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目次

役割ベースアクセス制御（RBAC）

ONTAP tools RBACについて学ぶ

ロールベースアクセス制御（RBAC）は、組織内のリソースへのアクセスを制御するためのセキュリティフレームワークです。RBACは、個々のユーザーに権限を割り当てるのではなく、アクションを実行するための特定の権限レベルを持つロールを定義することで、管理を簡素化します。定義されたロールはユーザーに割り当てられるため、エラーのリスクを軽減し、組織全体のアクセス制御の管理を簡素化するのに役立ちます。

RBAC標準モデルは、複雑さが増していく複数の実装技術またはフェーズで構成されています。その結果、実際のRBACの導入は、ソフトウェアベンダーとその顧客のニーズに基づいて異なり、比較的単純なものから非常に複雑なものまで多岐にわたる可能性があります。

RBACコンポーネント

大まかに言うと、RBACの実装には一般的にいくつかの構成要素が含まれています。これらの構成要素は、認可プロセスを定義する一環として、さまざまな方法で結び付けられています。

権限

_特権_とは、許可または拒否できるアクションまたは機能のことです。ファイルの読み取り機能のような単純なものである場合もあれば、特定のソフトウェア システムに固有のより抽象的な操作である場合もあります。Privilegesを定義して、REST APIエンドポイントおよびCLIコマンドへのアクセスを制限することもできます。すべてのRBAC実装には事前定義された特権が含まれており、管理者がカスタム特権を作成できる場合もあります。

ロール

ロールとは、1つ以上の権限を含むコンテナです。ロールは一般的に、特定の業務や職務内容に基づいて定義されます。ユーザーにロールが割り当てられると、そのユーザーにはそのロールに含まれるすべての権限が付与されます。権限と同様に、実装には事前定義されたロールが含まれており、一般的にはカスタムロールの作成も可能です。

オブジェクト

オブジェクトとは、RBAC環境内で識別される、現実のリソースまたは抽象的なリソースを表します。権限によって定義されたアクションは、関連付けられたオブジェクトに対して、または関連付けられたオブジェクトを使用して実行されます。実装方法によっては、オブジェクトタイプ全体または特定のオブジェクトインスタンスに対して権限を付与することができます。

ユーザとグループ

認証後、_ユーザー_には役割が割り当てられるか、役割に関連付けられます。RBAC の実装によっては、ユーザーに割り当てられる役割が 1 つだけの場合もあれば、ユーザーごとに複数の役割を割り当てられるものの、同時にアクティブにできる役割は 1 つだけという場合もあります。_グループ_に役割を割り当てることで、セキュリティ管理をさらに簡素化できます。

権限

権限とは、ユーザーまたはグループと役割をオブジェクトに関連付ける定義のことです。権限は、階層構造を持つオブジェクトモデルにおいて、階層内の子オブジェクトにオプションで継承させることができるため、非常に役立ちます。

2つのRBAC環境

ONTAP tools for VMware vSphere 10を使用する際には、考慮すべき2つの異なるRBAC環境があります。ONTAP tools for VMware vSphere 10では、操作を実行するためにvCenterとONTAPの両方で特定の権限が必要です。ONTAP toolsはストレージ管理タスクを自動化しますが、vCenterまたはONTAPのいずれにもユーザーアカウントを作成しません。サービスアカウントは、必要に応じてvSphere管理者が作成する必要があります。このドキュメントでは、管理者が効果的なONTAP tools管理のために必要なロールと権限を割り当てるためのガイダンスを提供します。

VMware vCenter Server

VMware vCenter Server におけるRBACの実装は、vSphere Client ユーザーインターフェースを通じて公開されているオブジェクトへのアクセスを制限するために使用されます。ONTAP tools for VMware vSphere 10 のインストールの一環として、RBAC環境はONTAP toolsの機能を表す追加のオブジェクトを含むように拡張されます。これらのオブジェクトへのアクセスはリモートプラグインを通じて提供されます。詳細については、"vCenter Server RBAC環境"を参照してください。

ONTAPクラスタ

ONTAP tools for VMware vSphere 10は、ONTAP REST APIを通じてONTAPクラスターに接続し、ストレージ関連の操作を実行します。ストレージリソースへのアクセスは、認証時に提供されたONTAPユーザーに関連付けられたONTAPロールによって制御されます。詳細については、"ONTAP RBAC環境"を参照してください。

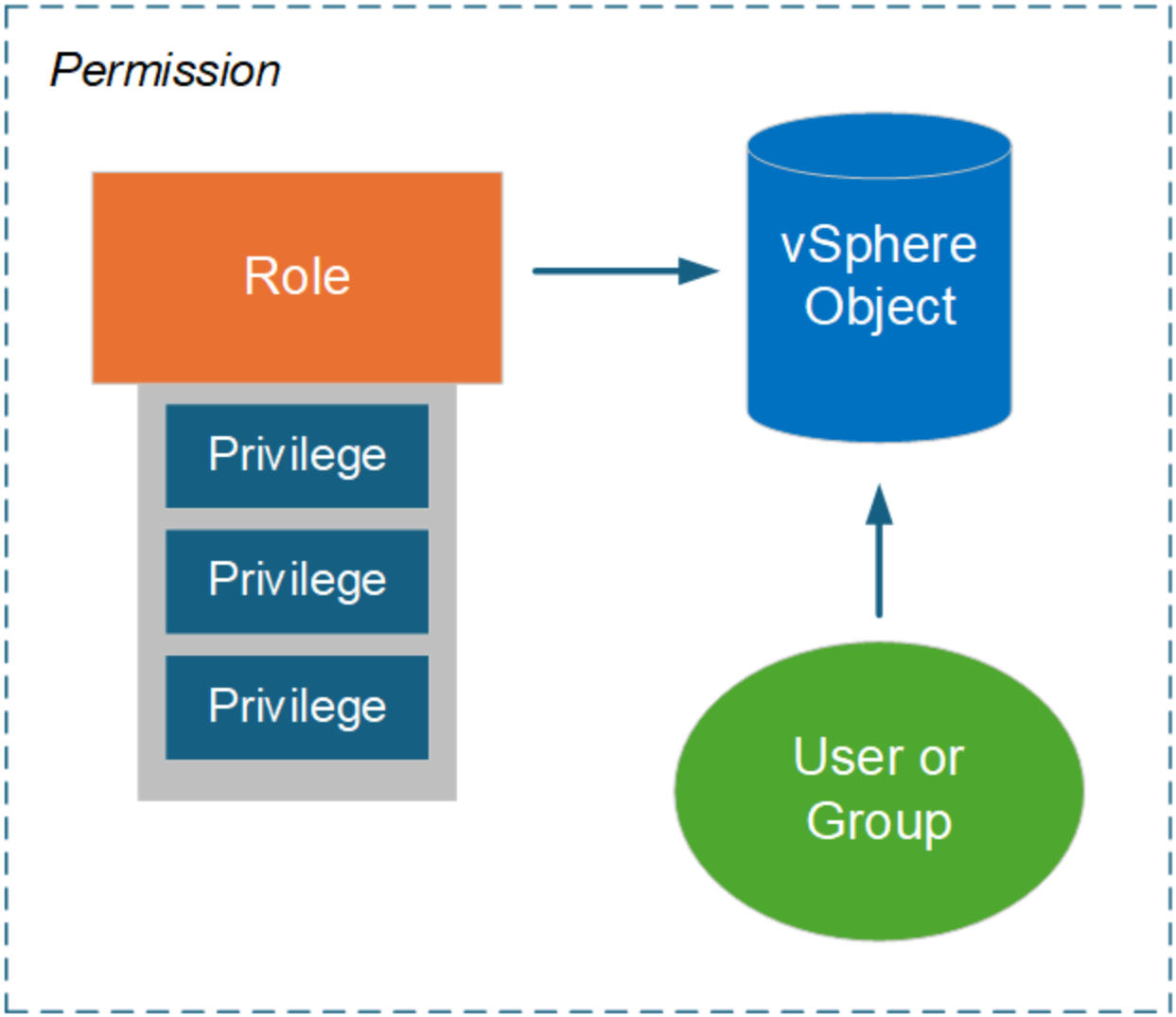
VMware vSphere を使用した RBAC

vCenter Server RBAC と ONTAP tools の連携

VMware vCenter Server は、vSphere オブジェクトへのアクセスを制御できる RBAC 機能を提供します。これは、vCenter の集中型認証および認可セキュリティサービスの重要な部分です。

vCenter Server 権限のイラスト

許可は、vCenter Server 環境でアクセス制御を適用するための基盤です。許可定義にユーザーまたはグループを含む vSphere オブジェクトに適用されます。vCenter 許可の概要を示す図を以下に示します。



vCenter Server 権限の構成要素

vCenter Server 権限は、権限が作成される際に結合される複数のコンポーネントのパッケージです。

vSphereオブジェクト

権限は、vSphere オブジェクト（vCenter Server、ESXi ホスト、仮想マシン、データストア、データセンター、フォルダなど）に関連付けられています。オブジェクトに割り当てられた権限に基づいて、vCenter Server は、各ユーザーまたはグループがオブジェクトに対して実行できるアクションまたはタスクを決定します。ONTAP tools for VMware vSphere に固有のタスクについては、すべての権限が vCenter Server のルートまたはルートフォルダレベルで割り当てられ、検証されます。詳細については、"RBACを使用するvCenterサーバ" を参照してください。

Privileges とロール

ONTAP tools for VMware vSphere 10 で使用される vSphere の権限には、2 種類あります。この環境での RBAC の操作を簡素化するために、ONTAP tools は、必要なネイティブ権限とカスタム権限を含むロールを提供します。権限には以下が含まれます：

- vCenter Server標準の権限

  これらは、vCenter Server が提供する Privileges です。

- ONTAP Tools固有の権限

  これらは、ONTAP tools for VMware vSphere に固有のカスタム Privileges です。

ユーザとグループ

Active Directory またはローカルの vCenter Server インスタンスを使用してユーザーとグループを定義できます。ロールと組み合わせることで、vSphere オブジェクト階層内のオブジェクトに対する権限を作成できます。この権限は、関連付けられたロールにおける権限に基づいてアクセスを許可します。ロールはユーザーに単独で直接割り当てられるものではないことに注意してください。代わりに、ユーザーとグループは、より大きな vCenter Server 権限の一部として、ロール権限を通じてオブジェクトへのアクセス権を取得します。

vCenter ServerのRBACに関するONTAP toolsの考慮事項

ONTAP tools for VMware vSphere 10 の RBAC 実装には、vCenter Server を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。

vCenter のロールと管理者アカウント

カスタム vCenter Server ロールを定義して使用する必要があるのは、vSphere オブジェクトおよび関連する管理タスクへのアクセスを制限する場合のみです。アクセスを制限する必要がない場合は、代わりに管理者アカウントを使用できます。各管理者アカウントは、オブジェクト階層の最上位レベルで管理者ロールが定義されています。これにより、ONTAP tools for VMware vSphere 10 によって追加されたオブジェクトを含む、vSphere オブジェクトへのフルアクセスが提供されます。

vSphereオブジェクト階層

vSphereオブジェクトインベントリは階層構造で整理されています。例えば、以下のように階層を下っていくことができます。

`vCenter Server` --> `Datacenter` --> `Cluster` --> `ESXi host` --> `Virtual Machine`

すべての権限は、VAAI プラグイン操作を除く vSphere オブジェクト階層で検証されます。VAAI プラグイン操作は、対象の ESXi ホストに対して検証されます。

ONTAP tools for VMware vSphere 10 に含まれるロール

vCenter Server RBAC での作業を簡素化するために、ONTAP tools for VMware vSphere では、さまざまな管理タスクに合わせた事前定義ロールが提供されます。

> 必要に応じて、新しいカスタムロールを作成できます。そのためには、既存のONTAP toolsロールの1つをクローニングし、必要に応じて編集します。構成変更後、影響を受けるvSphereクライアントユーザーは、変更を有効にするために一度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 tools for VMware vSphere のロールを表示するには、vSphere Client の上部にある **Menu** を選択し、**Administration** をクリックしてから、左側の **Roles** をクリックします。以下の権限は、vCenter Server

の導入またはオンボーディングを担当する vCenter ユーザに割り当てられたロールに含める必要があります。これらの権限が、導入またはオンボーディング プロセスの前提条件として設定されていることを確認してください。

- アラーム
  - 警報を確認する
- コンテンツライブラリ
  - ライブラリアイテムを追加
  - テンプレートでチェックイン
  - テンプレートを確認する
  - ファイルをダウンロード
  - ストレージのインポート
  - ストレージを読み取る
  - ライブラリアイテムを同期する
  - 購読ライブラリを同期する
  - 設定を表示する
- データストア
  - Allocate space
  - Browse datastore
  - Low level file operations
  - Remove file
  - Update virtual machine files
  - 仮想マシンのメタデータを更新する
- ESX Agent Manager
  - View
- フォルダ
  - フォルダを作成
- ホスト
  - 構成
    - 詳細設定
    - 設定の変更
    - ネットワーク設定
    - System resources
    - 仮想マシンの自動起動構成
  - ローカル操作
    - Create virtual machine

        - Delete virtual machine
        - Reconfigure virtual machine
- Network
    - Assign network
    - 設定
- OvfManager
    - OvfConsumer アクセス
- ホストプロファイル
    - View
- リソース
    - Assign virtual machine to resource pool
- スケジュールされたタスク
    - タスクを作成する
    - タスクの変更
    - タスクを実行する
- タスク
    - タスクを作成する
    - タスクの更新
- vApp
    - 仮想マシンを追加する
    - リソース プールの割り当て
    - vApp の割り当て
    - 作成
    - インポート
    - Move
    - Power off
    - Power on
    - URLから取得
    - OVF環境の表示
- 仮想マシン
    - 構成の変更
        - Add existing disk
        - Add new disk
        - Add or remove device
        - 高度な設定

        - Change CPU count
        - メモリの変更
        - Change Settings
        - Change resource
        - Extend virtual disk
        - Modify device settings
        - Remove disk
        - ゲスト情報をリセットする
        - Upgrade virtual machine compatibility
    - 在庫を編集
        - Create from existing
        - Create new
        - Move
        - 登録
        - 削除
        - 登録解除
    - インタラクション
        - 仮想マシン上でのバックアップ操作
        - Configure CD media
        - Configure floppy media
        - デバイスを接続する
        - コンソール操作
        - VIX API によるゲストオペレーティングシステム管理
        - Power off
        - Power on
        - リセット
        - 中断
    - プロビジョニング
        - Allow disk access
        - Clone template
        - ゲストをカスタマイズ
        - Deploy template
        - カスタマイズ仕様の変更
        - Read customization specifications
    - Snapshotの管理
        - Snapshot の作成

- Remove snapshot
- スナップショットの名前を変更する
- Revert to snapshot

以下に説明するように、あらかじめ定義された3つのロールがあります。

NetApp ONTAP tools for VMware vSphere 管理者

すべてのネイティブ vCenter Server の Privileges と、VMware vSphere 管理者タスクのコア ONTAP tools for VMware を実行するために必要な ONTAP tools 固有の Privileges を提供します。

NetApp ONTAP tools for VMware vSphere 読み取り専用

ONTAP tools への読み取り専用アクセスを提供します。これらのユーザーは、アクセス制御された ONTAP tools for VMware vSphere の操作を実行できません。

NetApp ONTAP tools for VMware vSphere のプロビジョニング

ストレージのプロビジョニングに必要なネイティブの vCenter Server Privileges の一部と ONTAP tools 固有の Privileges を提供します。以下のタスクを実行できます：

- 新しいデータストアの作成
- データストアの管理

vSphereオブジェクトと**ONTAP**ストレージバックエンド

これら2つのRBAC環境は連携して動作します。vSphereクライアントインターフェースでタスクを実行する際、vCenter Serverに定義されたONTAPツールのロールが最初にチェックされます。操作がvSphereによって許可されている場合、ONTAPロールの権限が確認されます。この2番目のステップは、ストレージバックエンドの作成および構成時にユーザーに割り当てられたONTAPロールに基づいて実行されます。

vCenter Server RBAC の操作

vCenter Server の権限とアクセス許可を使用する際には、いくつか考慮すべき点があります。

必要な権限

ONTAP tools for VMware vSphere 10 のユーザーインターフェースにアクセスするには、ONTAPツール固有の「表示」権限が必要です。vSphere にこの権限なしでサインインして NetApp アイコンをクリックすると、ONTAP tools for VMware vSphere はエラーメッセージを表示し、ユーザーインターフェースへのアクセスを禁止します。

vSphereオブジェクト階層での割り当てレベルによって、アクセスできるユーザー インターフェイスの部分が決まります。ルート オブジェクトに表示（View）Privilegesを割り当てると、NetAppアイコンをクリックしてONTAP tools for VMware vSphereにアクセスできるようになります。

代わりに、別の下位の vSphere オブジェクトレベルに「表示」権限を割り当てることができます。ただし、これにより、アクセスして使用できる ONTAP tools for VMware vSphere のメニューが制限されます。

アクセス許可の割り当て

vSphere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は、vCenter Serverの権限を使用する必要があります。vSphereオブジェクト階層のどの位置に権限を割り当てるかによって、ユーザーが実行でき

るONTAP tools for VMware vSphere 10のタスクが決まります。

> より制限的なアクセス権限を定義する必要がない限り、一般的にはルートオブジェクトまたはルートフォルダのレベルで権限を割り当てることをお勧めします。

ONTAP tools for VMware vSphere 10 で使用可能な権限は、ストレージシステムなどのカスタム非 vSphere オブジェクトに適用されます。可能であれば、割り当て先となる vSphere オブジェクトが存在しないため、これらの権限は ONTAP tools for VMware vSphere のルートオブジェクトに割り当てることをお勧めします。たとえば、ONTAP tools for VMware vSphere の「ストレージシステムの追加/変更/削除」権限を含む権限は、ルートオブジェクトレベルで割り当てる必要があります。

オブジェクト階層の上位レベルで権限を定義する場合、その権限が下位レベルに渡され、子オブジェクトに継承されるように構成できます。必要に応じて、子オブジェクトに追加の権限を割り当てて、親オブジェクトから継承された権限を上書きすることができます。

権限はいつでも変更できます。権限内の Privileges を変更すると、その権限に関連付けられているユーザーは vSphere からログアウトし、変更を有効にするために再度ログインする必要があります。

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

```
OTV_10_VSC_Discovery_Create
```

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

商標に関する情報