ロールベースアクセス制御
ONTAP tools for VMware vSphere 10

NetApp
September 30, 2025

目次

ロールベースアクセス制御 . . . 1
ONTAP ツールでのロールベースアクセス制御の概要 . . . 1
vCenter Serverのロールの割り当てと変更に関するキーポイント . . . 1
ONTAP ツールに付属の標準ロール . . . 2
ONTAPストレージバックエンドとvSphereオブジェクトの権限 . . . 2
VMware vSphere 用の ONTAP ツールを使用する際に推奨される ONTAP ロール . . . 2

ロールベースアクセス制御

ONTAP ツールでのロールベースアクセス制御の概要

vCenter Server の RBAC を使用すると、 vSphere オブジェクトへのアクセスを制御できます。vCenter Serverは、ロールと権限を持つユーザ権限とグループ権限を使用して、インベントリ内のさまざまなレベルで一元的な認証および許可サービスを提供します。vCenter Serverには、RBACを管理するための5つの主要コンポーネントがあります。

コンポーネント	説明
権限	vSphereで操作を実行するためのアクセスを有効または拒否します。
ロール	ロールには、1つ以上のシステム権限が含まれています。各権限は、システム内の特定のオブジェクトまたはタイプのオブジェクトに対する管理権限を定義します。ユーザにロールを割り当てると、そのロールで定義されている権限の機能が継承されます。
ユーザとグループ	ユーザとグループは、Active Directory（AD）または潜在的にローカルのWindowsユーザ/グループからロールを割り当てる権限に使用される（推奨されません）
権限	権限を使用すると、ユーザまたはグループに権限を割り当てて、特定の操作を実行し、vCenter Server内のオブジェクトに変更を加えることができます。vCenter Serverアクセス許可は、ESXiホストに直接ログインするユーザではなく、vCenter Serverにログインするユーザにのみ影響します。
オブジェクト	アクションが実行されるエンティティ。VMware vCenterオブジェクトは、データセンター、フォルダ、リソースプール、クラスタ、ホスト、 およびVM

タスクを完了するには、適切なvCenter Server RBACロールが必要です。タスクの実行中、ONTAP toolsはユーザのvCenter Serverロールを確認してから、ユーザのONTAP権限を確認します。

> vCenter Serverのロールは、管理者ではなく、ONTAP toolsのvCenterユーザに適用されます。デフォルトでは、管理者は製品へのフルアクセス権を持ち、ロールを割り当てる必要はありません。

ユーザとグループは、vCenter Serverロールに含まれることでロールにアクセスできます。

vCenter Serverのロールの割り当てと変更に関するキーポイント

vCenter Serverのロールは、vSphereの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にのみ設定します。それ以外の場合は、管理者としてログインできます。このログインでは、すべての vSphere オブジェクトに自動的にアクセスできます。

ロールを割り当てる場所によって、ユーザが実行できるONTAP toolsタスクが決まります。一度に1つのロールを変更できます。 ロール内の権限を変更した場合、そのロールに関連付けられているユーザは、更新されたロールを有効にするために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 ツールに付属の標準ロール

vCenter Serverの権限とRBACを簡単に使用できるように、ONTAP toolsには、ONTAP toolsの主要なタスクを実行できる標準のONTAP toolsロールが用意されています。タスクを実行せずに情報を表示できる読み取り専用ロールもあります。

ONTAP toolsの標準ロールを表示するには、vSphere Clientの[ホーム]ページで*[ロール]*をクリックします。ONTAP toolsのロールで実行できるタスクは次のとおりです。

* 役割 *	* 概要 *
NetApp ONTAPツール管理者	ONTAP toolsの一部のタスクを実行するために必要なvCenter Server標準の権限とONTAP tools固有の権限がすべて含まれています。
NetApp ONTAP tools読み取り専用	ONTAP toolsへの読み取り専用アクセスを許可します。これらのユーザは、アクセス制御されたONTAP toolsアクションを実行できません。
NetApp ONTAPツールプロビジョニング	ストレージのプロビジョニングに必要なvCenter Server標準の権限とONTAP tools固有の権限が含まれています。次のタスクを実行できます。 • 新しいデータストアを作成する • データストアを管理します

Manager UI管理者ロールがvCenterに登録されていません。このロールはマネージャUIに固有です。

標準のONTAP toolsロールよりも制限の厳しいロールを実装する必要がある場合は、ONTAP toolsロールを使用して新しいロールを作成できます。

この場合は、必要なONTAP toolsロールのクローンを作成し、そのクローンロールを編集してユーザに必要な権限のみを付与します。

ONTAPストレージバックエンドとvSphereオブジェクトの権限

十分なvCenter Serverアクセス許可がある場合、ONTAP toolsは次に、ストレージバックエンドのクレデンシャル（ユーザ名とパスワード）に関連付けられているONTAP RBAC権限（ONTAPロール）を確認します。 そのストレージバックエンドでONTAP toolsタスクに必要なストレージ処理を実行するための十分な権限があるかどうかを確認する。適切なONTAP権限があれば、 ストレージバックエンドを使用し、ONTAP toolsタスクを実行します。ストレージバックエンドで実行できるONTAP toolsタスクは、ONTAPロールによって決まります。

VMware vSphere 用の ONTAP ツールを使用する際に推奨される ONTAP ロール

VMware vSphere および Role-Based Access Control （ RBAC ；ロールベースアクセス

制御）用の ONTAP ツールを使用する際に推奨される ONTAP ロールをいくつか設定できます。これらのロールには、ONTAP toolsタスクで実行するストレージ処理に必要なONTAP権限が含まれています。

新しいユーザロールを作成するには、 ONTAP を実行しているストレージシステムに管理者としてログインする必要があります。ONTAP System Manager 9.8P1以降を使用してONTAP ロールを作成できます。を参照してください "管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト" を参照してください。

各 ONTAP ロールには、ロールのクレデンシャルを構成するユーザ名とパスワードのペアが関連付けられています。このクレデンシャルを使用してログインしないと、ロールに関連付けられたストレージ処理にアクセスできません。

セキュリティ対策として、ONTAP tools固有のONTAPロールは階層構造になっています。最初のロールは最も制限のあるロールで、ONTAP toolsの最も基本的なストレージ処理に関連する権限だけが含まれます。次のロールには、そのロール独自の権限と、前のロールに関連付けられているすべての権限が含まれます。以降、上位のロールほど制限が少なく、より多くのストレージ処理をサポートします。

ONTAP toolsを使用する際に推奨されるONTAP RBACロールの一部を次に示します。ロールを作成したら、仮想マシンのプロビジョニングなど、ストレージに関するタスクを実行する必要があるユーザにそのロールを割り当てることができます。

1. 検出

   ストレージシステムを追加できます。

2. ストレージを作成します

   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権限が含まれます。

3. ストレージを変更します

   ストレージを変更できます。また、 Discovery ロールと Create Storage ロールに関連付けられているすべての権限が含まれます。

4. ストレージを破棄します

   ストレージを破棄できます。また、 Discovery ロール、 Create Storage ロール、 Modify Storage ロールに関連付けられているすべての権限が含まれます。

VASA Provider for ONTAP を使用する場合は、 Policy-Based Management （ PBM ；ポリシーベース管理）ロールも設定します。ストレージポリシーを使用してストレージを管理できます。このロールを使用するには、「検出」ロールも設定する必要があります。

著作権に関する情報

商標に関する情報