VMware vSphere を使用した RBAC

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

目次

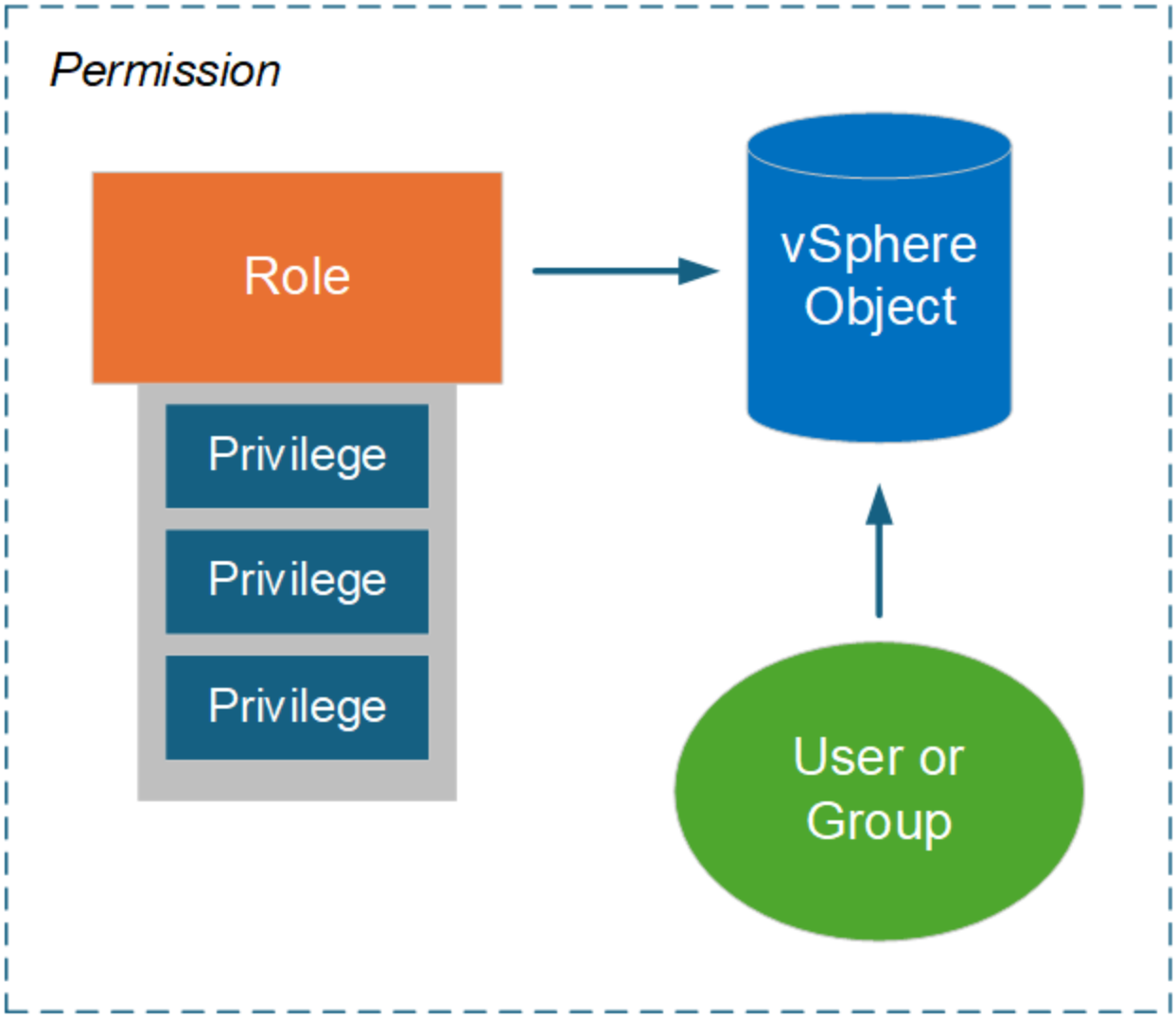
VMware vSphere を使用した RBAC

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

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 の集中認証および承認セキュリティ サービスの重要な部分です。

vCenter Server 権限の図

権限は、vCenter Server 環境でアクセス制御を実施するための基盤です。これは、権限定義に含まれるユーザーまたはグループを持つ vSphere オブジェクトに適用されます。次の図に、vCenter 権限の概要を示します。



vCenter Server 権限のコンポーネント

vCenter Server 権限は、権限の作成時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、vCenter Server、ESXi ホスト、仮想マシン、データストア、データセンター、フォルダなどの vSphere オブジェクトに関連付けられます。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に固有のタスクの場合、すべての権限は 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。見る"vCenter ServerでRBACを使用する"詳細についてはこちらをご覧ください。

Privilegesと役割

ONTAP tools for VMware vSphereで使用される vSphere 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ツール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 によって提供される権限です。

- ONTAP Tools固有の権限

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

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の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直接個別に割り当てられるのではなく、ユーザーとグループは、vCenter Server のより広範な権限の一部として、ロール権限を通じてオブジェクトへのアクセスを取得します。

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

vCenter Server 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。

vCenter のロールと管理者アカウント

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にのみ、カスタム vCenter Server ロールを定義して使用する必要があります。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を使用して定義されます。これにより、 ONTAP tools for VMware vSphere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的に編成されます。たとえば、次のように階層を下に移動できます。

`vCenter Server⟶ Datacenter ⟶ Cluster ⟶ ESXi host ⟶ Virtual Machine`

VAAI プラグイン操作を除くすべての権限は、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、ターゲット ESXi ホストに対して検証されます。

ONTAP tools for VMware vSphere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て事前定義された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。この場合、既存のONTAPツール ロールの 1 つを複製し、必要に応じて編集する必要があります。構成を変更した後、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ログアウトして再度ログインする必要があります。

ONTAP tools for VMware vSphereを表示するには、vSphere Client の上部にある メニュー を選択し、左側の 管理 をクリックしてから ロール をクリックします。以下に説明する 3 つの定義済みロールがあります。

VMware vSphere 管理者向け**NetApp ONTAP tools for VMware vSphere**

ONTAP tools for VMware vSphereを実行するために必要な、すべてのネイティブ vCenter Server 権限とONTAPツール固有の権限を提供します。

ONTAP tools for VMware vSphereNetApp ONTAP ツール（読み取り専用）

ONTAP Toolsに対する読み取り専用アクセスが許可されます。これらのユーザーは、アクセス制御されているONTAP tools for VMware vSphereを実行できません。

VMware vSphere プロビジョニング用の**NetApp ONTAP tools for VMware vSphere**

ストレージのプロビジョニングに必要なネイティブ vCenter Server 権限とONTAPツール固有の権限の一部を提供します。次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

2 つの RBAC 環境が連携して動作します。 vSphere クライアント インターフェイスでタスクを実行する場合、最初に vCenter Server に定義されているONTAPツール ロールがチェックされます。操作が vSphere によって許可されている場合は、 ONTAPロールの権限が検査されます。この 2 番目の手順は、ストレージ バックエンドが作成および構成されたとき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操作する際に考慮すべき点がいくつかあります。

必要な権限

ONTAP tools for VMware vSphereにアクセスするには、 ONTAPツール固有の *View* 権限が必要です。この権限なしで vSphere にサインインしてNetAppアイコンをクリックすると、 ONTAP tools for VMware vSphereエラー メッセージが表示され、ユーザー インターフェイスにアクセスできなくなります。

vSphere オブジェクト階層内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権限を割り当てると、 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もできます。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 権限を使用する必要があります。 vSphere オブジェクト階層内で権限を割り当てる場所によって、ユーザーが実行できるONTAP tools for VMware vSphereが決まります。

より制限的なアクセスを定義する必要がない限り、通常はルート オブジェクトまたはルート フォルダー 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で使用できる権限は、ストレージ システムなどの vSphere 以外のカスタム オブジェクトに適用されます。割り当てることができる vSphere オブジェクトがないため、可能であれば、これらの権限をONTAP tools for VMware vSphereに割り当てる必要があります。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」権限を含むすべての権限は、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、その権限が子オブジェクトに渡され継承されるように構成できます。必要に応じて、親から継承した権限を上書きする追加の権限を子オブジェクトに割り当てることができます。

権限はいつでも変更できます。権限内のいずれかの権限を変更する場合、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、再度ログインして変更を有効に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