VMware vSphereを使用したRBAC

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

目次

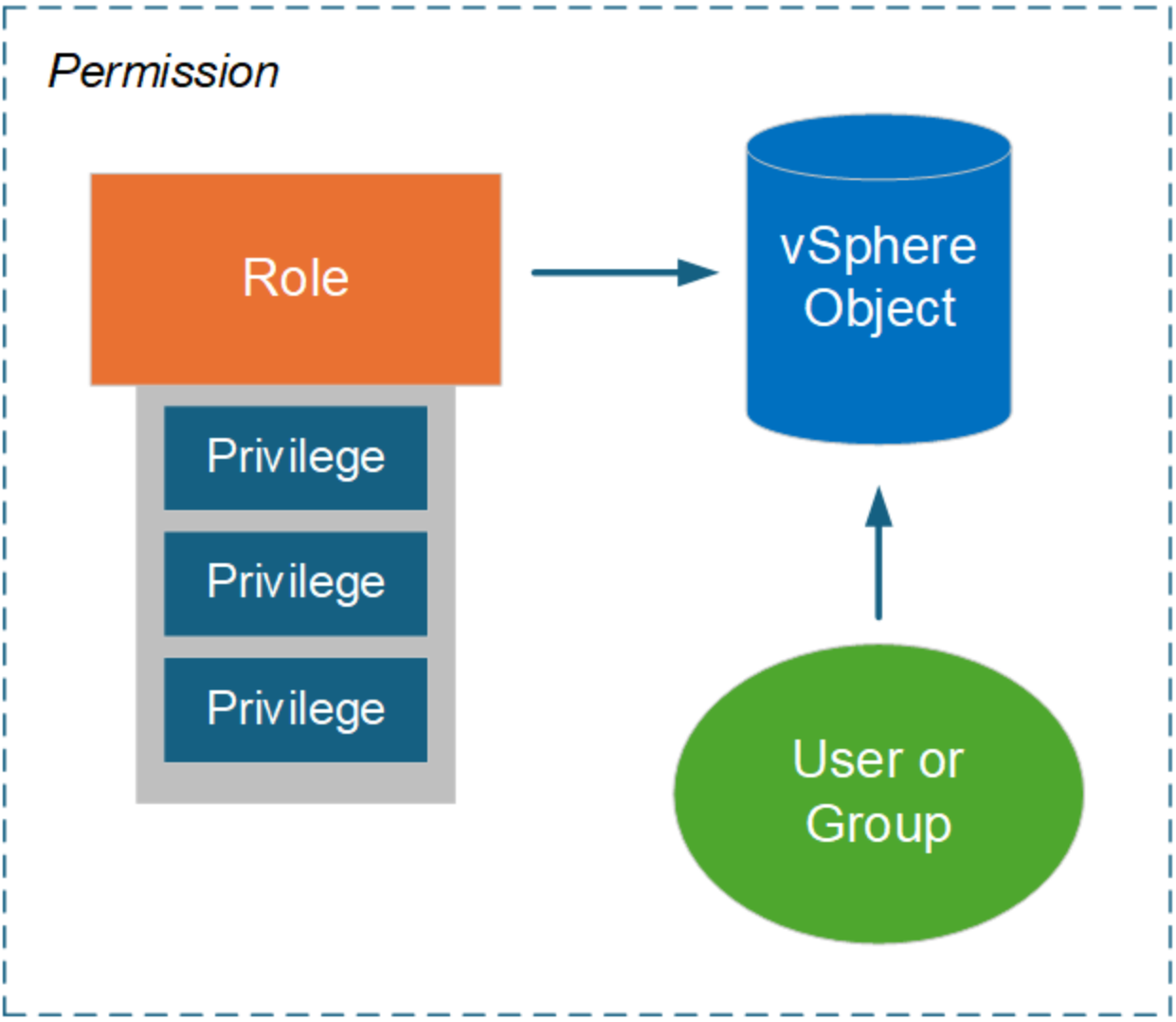
VMware vSphereを使用したRBAC

vCenter Server RBAC環境とONTAP Tools for VMware vSphere 10

VMware vCenter ServerにはRBAC機能が用意されており、vSphereオブジェクトへのアクセスを制御できます。これは、vCenterの一元化された認証および許可セキュリティサービスの重要な部分です。

vCenter Serverアクセス許可の図

アクセス許可は、vCenter Server環境でアクセス制御を適用するための基盤です。これは、アクセス許可の定義に含まれるユーザまたはグループを含むvSphereオブジェクトに適用されます。次の図に、vCenterアクセス許可の概要を示します。



vCenter Serverアクセス許可のコンポーネント

vCenter Serverアクセス許可は、アクセス許可の作成時にバインドされる複数のコンポーネントで構成されるパッケージです。

vSphereオブジェクト

アクセス許可はvSphereオブジェクトに関連付けられます。vCenter Server、ESXiホスト、仮想マシン、データストア、データセンター、フォルダなどがあります。vCenter Serverは、オブジェクトに割り当てられた権限に基づいて、各ユーザまたはグループがそのオブジェクトに対して実行できる操作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、すべてのアクセス許可がvCenter Serverのルートフォルダレベル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、を参照してください "vCenter ServerでRBACを使用する" 。

Privilegesとロール

ONTAP Tools for VMware vSphere 10で使用されるvSphere Privilegesには、2つのタイプがあります。この環境でのRBACの使用を簡易化するために、ONTAP toolsには、必要なネイティブおよびカスタムのPrivilegesを含むロールが用意されています。Privilegesには以下が含まれます。

- vCenter Server Privileges標準

  これはvCenter Serverが提供するPrivilegesです。

- ONTAP tools固有のPrivileges

  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

ユーザとグループは、Active DirectoryまたはローカルのvCenter Serverインスタンスを使用して定義できます。ロールと組み合わせて、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Privilegesに基づいてアクセスを許可します。役割は、個別にユーザーに直接割り当てられるわけではないことに注意してください。代わりに、ユーザとグループは、より大きなvCenter Serverアクセス許可の一部としてPrivilegesロールを使用してオブジェクトにアクセスできます。

vCenter Server RBACとONTAP Tools for VMware vSphere 10の使用

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

vCenterのロールと管理者アカウント

カスタムの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にある管理者ロールで定義されます。これにより、ONTAP tools for VMware vSphere 10によって追加されたvSphere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になっています。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
```

vSphereオブジェクト階層ではすべての権限が検証されますが、VAAIプラグインの処理はターゲットESXiホストに対して検証されます。

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

vCenter Server RBACの使用を簡易化するために、ONTAP Tools for VMware vSphereには、さまざまな管理タスクに合わせてカスタマイズされた事前定義されたロールが用意されています。

> 必要に応じて、新しいカスタムロールを作成できます。この場合は、既存のONTAP toolsロールのいずれかをクローニングし、必要に応じて編集する必要があります。設定を変更したら、影響を受けるvSphere Clientユーザがログアウトしてから再度ログインし、変更をアクティブ化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*を選択し、[管理]をクリックしてから、左側の[ロール]*をクリックします。以下に説明する3つの事前定義されたロールがあります。

VMware vSphere管理者向けNetApp ONTAPツール

VMware vSphere管理者タスク用のコアONTAPツールを実行するために必要なvCenter Server PrivilegesおよびONTAPツール固有のPrivilegesをすべて提供します。

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許可します。アクセスが制御されたONTAP tools for VMware vSphereアクションを実行することはできません。

NetApp ONTAP Tools for VMware vSphere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
- データストアの管理

vSphereオブジェクトとONTAPストレージのバックエンド

2つのRBAC環境が連携して動作します。vSphere Clientインターフェイスでタスクを実行する場合は、まずvCenter Serverに定義されているONTAP toolsのロールがチェックされます。処理がvSphereで許可されている場合は、ONTAPロールPrivilegesが検証されます。2番目の手順は、ストレージバックエンドの作成および設定時にユーザに割り当てられたONTAPロールに基づいて実行します。

vCenter Server RBACノシヨウ

vCenter ServerのPrivilegesとアクセス許可を使用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 10のユーザインターフェイスにアクセスするには、ONTAP tools固有の_view_privilegeが必要です。この権限がない状態でvSphereにサインインし、NetAppアイコンをクリックすると、ONTAP tools for VMware vSphereにエラーメッセージが表示され、ユーザインターフェイスにアクセスできません。

vSphereオブジェクト階層の割り当てレベルによって、ユーザインターフェイスのどの部分にアクセスできるかが決まります。ルートオブジェクトにView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View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メニューが制限されます。

権限の割り当て

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は、vCenter Serverアクセス許可を使用する必要があります。vSphereオブジェクト階層で権限を割り当てる場所によって、ユーザが実行できるONTAP tools for VMware vSphere 10タスクが決まります。

アクセスをより制限的に定義する必要がないかぎり、ルートオブジェクトレベルまたはルートフォルダ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。割り当て可能なvSphereオブジェクトがないため、可能であればこれらのアクセス許可をONTAP tools for VMware vSphereルートオブジェクトに割り当てる必要があります。たとえば、ONTAP tools for VMware vSphereの「Add/Modify/Remove storage systems」権限を含むすべてのアクセス許可は、ルートオブジェクトレベルに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アクセス許可を定義する場合は、アクセス許可が子オブジェクトに継承されるように設定できます。必要に応じて、親から継承したアクセス許可を上書きする追加のアクセス許可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。アクセス許可に含まれるPrivilegesを変更した場合、アクセス許可に関連付けられているユーザが変更を有効にするには、vSphereからログアウトしてログインし直す必要があります。

著作権に関する情報

商標に関する情報