ロールベース アクセス制御

ONTAP tools for VMware vSphere 10

NetApp
November 04, 2025

目次

ロールベース アクセス制御 . . . 1
ONTAP tools for VMware vSphereについて学ぶ . . . 1
RBAC コンポーネント . . . 1
2つのRBAC環境 . . . 2
VMware vSphere を使用した RBAC . . . 2
ONTAP tools for VMware vSphereを使用した vCenter Server RBAC 環境 . . . 2
ONTAP tools for VMware vSphereで vCenter Server RBAC を使用する . . . 4
ONTAPを使用した RBAC . . . 6
ONTAP tools for VMware vSphereを使用したONTAP RBAC 環境 . . . 6
ONTAP tools for VMware vSphereでONTAP RBAC を使用する . . . 7

ロールベース アクセス制御

ONTAP tools for VMware vSphere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、個々のユーザーに承認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レベルの権限を持つロールを定義することで管理を簡素化します。定義されたロールがユーザーに割り当てられるため、エラーのリスクが軽減され、組織全体のアクセス制御の管理が簡素化されます。

RBAC 標準モデルは、複雑さが増す複数の実装テクノロジまたはフェーズで構成されています。その結果、実際の RBAC の展開は、ソフトウェア ベンダーとその顧客のニーズに基づいて、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、すべての RBAC 実装に一般的に含まれるコンポーネントがいくつかあります。これらのコンポーネントは、承認プロセスの定義の一環として、さまざまな方法で結合されます。

権限

_権限_とは、許可または拒否できるアクションまたは機能です。ファイルの読み取り権限のような単純なものから、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まで、多岐にわたります。また、REST API エンドポイントやCLIコマンドへのアクセスを制限するためにPrivilegesを定義することもできます。すべてのRBAC実装には、事前定義された権限が含まれており、管理者がカスタム権限を作成できる場合もあります。

役割

ロール は、1 つ以上の権限を含むコンテナーです。役割は通常、特定のタスクまたは職務機能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、そのロールに含まれるすべての権限がユーザーに付与されます。また、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、通常はカスタム ロールの作成も許可されます。

オブジェクト

オブジェクト は、RBAC 環境内で識別される実際のリソースまたは抽象リソースを表します。権限を通じ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。実装に応じて、オブジェクト タイプまたは特定のオブジェクト インスタンスに権限を付与できます。

ユーザとグループ

ユーザー は、認証後に適用されるロールに割り当てられるか、関連付けられます。一部の RBAC 実装では、ユーザーに割り当てられるロールは 1 つだけですが、他の実装では、ユーザーごとに複数のロールが許可され、一度にアクティブにできるロールは 1 つだけになる場合があります。グループにロールを割り当てると、セキュリティ管理がさらに簡素化されます。

権限

権限 は、ユーザーまたはグループをロールとともにオブジェクトにバインドする定義です。権限は、階層オブジェクト モデルで役立ち、階層内の子にオプションで継承できます。

2つのRBAC環境

ONTAP tools for VMware vSphereを使用する場合は、考慮する必要がある 2 つの異なる RBAC 環境があります。

VMware vCenter Server

VMware vCenter Server の RBAC 実装は、vSphere Client ユーザー インターフェイスを通じて公開され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のインストールの一環として、RBAC 環境が拡張され、 ONTAPツールの機能を表す追加オブジェクトが含まれるようになります。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。"vCenter Server RBAC 環境"詳細についてはこちらをご覧ください。

ONTAPクラスタ

ONTAP tools for VMware vSphereは、 ONTAP REST API を介して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ロールを通じて制御されます。見る"ONTAP RBAC環境"詳細についてはこちらをご覧ください。

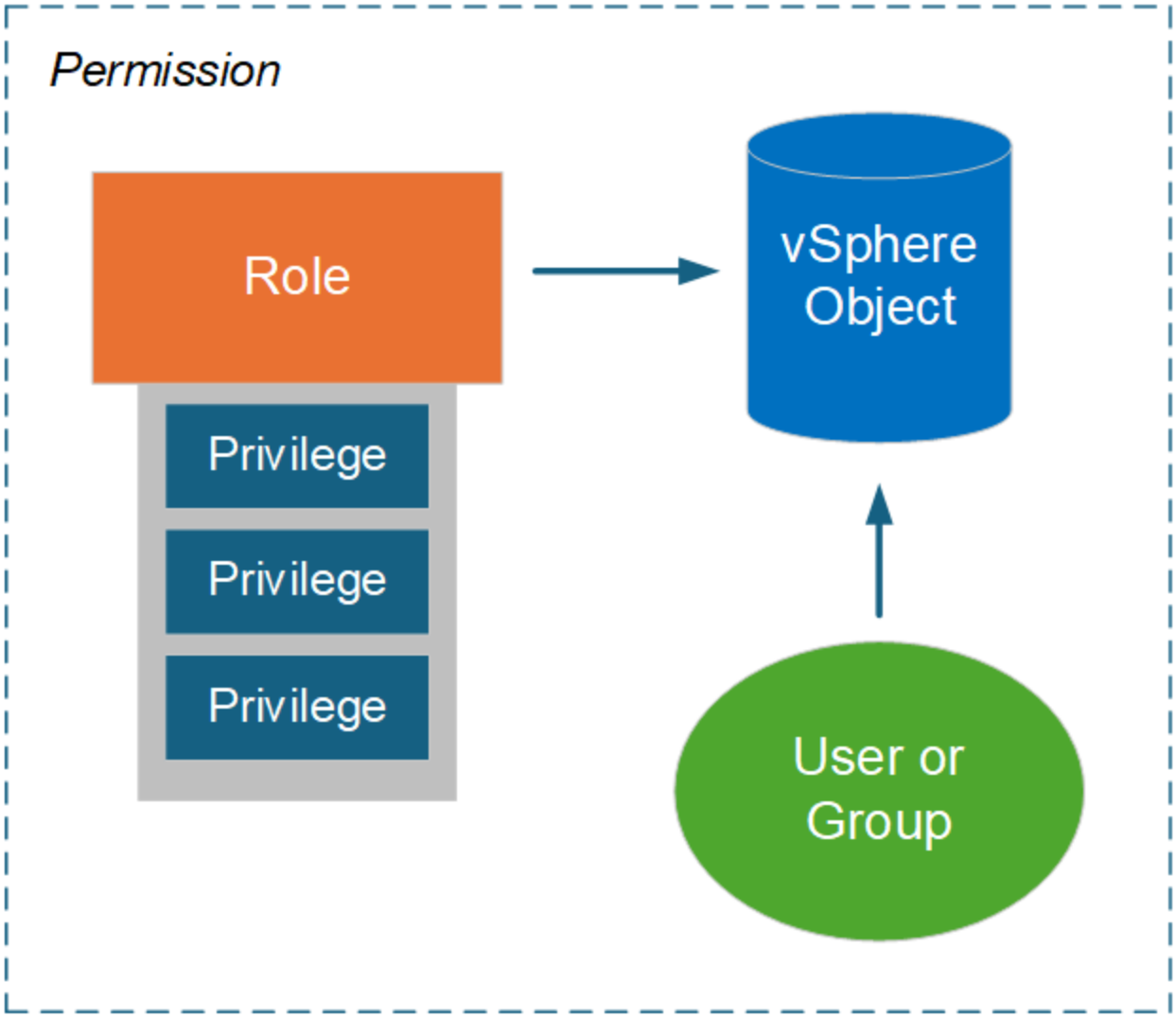
VMware vSphere を使用した RBAC

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。

ONTAPを使用した RBAC

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

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 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を使用する前に、環境をよく理解しておくと役立ちます。

管理オプションの概要

ONTAP RBAC を使用する場合、環境と目的に応じていくつかのオプションが利用できます。主要な行政上の決定の概要は以下のとおりです。こちらもご覧ください "ONTAP Automation: RBAC セキュリティの概要"詳細についてはこちらをご覧ください。

> ONTAP RBAC はストレージ環境に合わせて調整されており、vCenter Server で提供される RBAC 実装よりもシンプルです。ONTAPでは、ロールをユーザーに直接割り当てます。ONTAP RBAC では、vCenter Server で使用されるような明示的な権限の設定は必要ありません。

役割と権限の種類

ONTAPユーザーを定義するときは、 ONTAPロールが必要です。 ONTAPロールには 2 つの種類があります。

- REST

  REST ロールはONTAP 9.6 で導入され、通常は REST API を介してONTAPにアクセスするユーザーに適用されます。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の観点から定義されます。

- 伝統的

  これらは、 ONTAP 9.6 より前に含まれていたレガシー ロールです。これらは引き続き RBAC の基本的な側面です。権限は、 ONTAP CLI コマンドへのアクセスの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 パラメータをオプションで含めることができるため、権限が適用されるオブジェクトがより正確に定義されます。

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。これらは、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。

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ロールのセットを提供します。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。

役割マッピング

従来のロールを使用する場合でも、REST ロールを使用する場合でも、すべてのONTAPアクセスの決定は、基盤となる 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 エンドポイントに基づいて定義されるため、 ONTAP は各 REST ロールに対してマップ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、基礎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。並列にマップされたロールを変更することはできません。

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 エンドポイントではなく CLI コマンド権限を使用して REST ロールを表現することができます。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追加の粒度です。

ONTAPロールを定義する際の管理インターフェース

ONTAP CLI および REST API を使用してユーザーとロールを作成できます。ただし、 ONTAPツール マネージャーから利用できる JSON ファイルとともに System Manager インターフェイスを使用する方が便利です。見る"ONTAP tools for VMware vSphereでONTAP RBAC を使用する"詳細についてはこちらをご覧ください。

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

ONTAP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。

構成プロセスの概要

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、 ONTAPクラスターにアップロードできる JSON ファイルにパッケージ化されています。ユーザーを作成し、環境とセキュリティのニーズに合わせてロールをカスタマイズできます。

主要な構成手順の概要を以下に説明します。参照"ONTAPユーザーの役割と権限を構成する"詳細についてはこちらをご覧ください。

1.準備

ONTAPツール マネージャーとONTAPクラスターの両方の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 ユーザー インターフェイ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

System Manager にサインインしたら、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*までスクロールしてクリックします →。
3. *ユーザー*の下の*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、アップロードします。

4.役割を構成する

役割を定義する一環として、いくつかの管理上の決定を行う必要があります。見る[システムマネージャを使用してロールを構成する]詳細についてはこちらをご覧ください。

システムマネージャを使用してロールを構成する

System Manager 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ら、環境とニーズに応じ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構成

RBAC 定義は、VSC、VASA プロバイダー、SRA の組み合わせを含む複数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する必要があります。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。ユーザー名と関連する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 つのセットに分類されます。ロールのベースとなる権限は次のとおりです。

- 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

  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ているすべての権限も含まれます。

- ストレージを変更する

  ストレージを変更できます。また、ストレージの検出および作成のロールに関連付けられているすべての権限も含まれます。

- ストレージを破壊する

  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 ロールの変更に関連するすべての権限も含まれます。

ロールを持つユーザーを生成する

環境の設定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、次の値の連結になります。

- JSON ファイルで定義された定数プレフィックス値 (例: "OTV_10")
- 選択した製品の機能
- 権限セットのリスト。

例

```
OTV_10_VSC_Discovery_Create
```

新しいユーザーは、「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