



VMware vSphere を使用した RBAC

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目次

VMware vSphere を使用した RBAC	1
vCenter Server RBAC と ONTAP tools の連携	1
vCenter Server 権限のイラスト	1
vCenter Server 権限の構成要素	2
vCenter ServerのRBACに関するONTAP toolsの考慮事項	2
vCenter のロールと管理者アカウント	2
vSphereオブジェクト階層	3
ONTAP tools for VMware vSphere 10 に含まれるロール	3
vSphereオブジェクトとONTAPストレージバックエンド	6
vCenter Server RBAC の操作	7

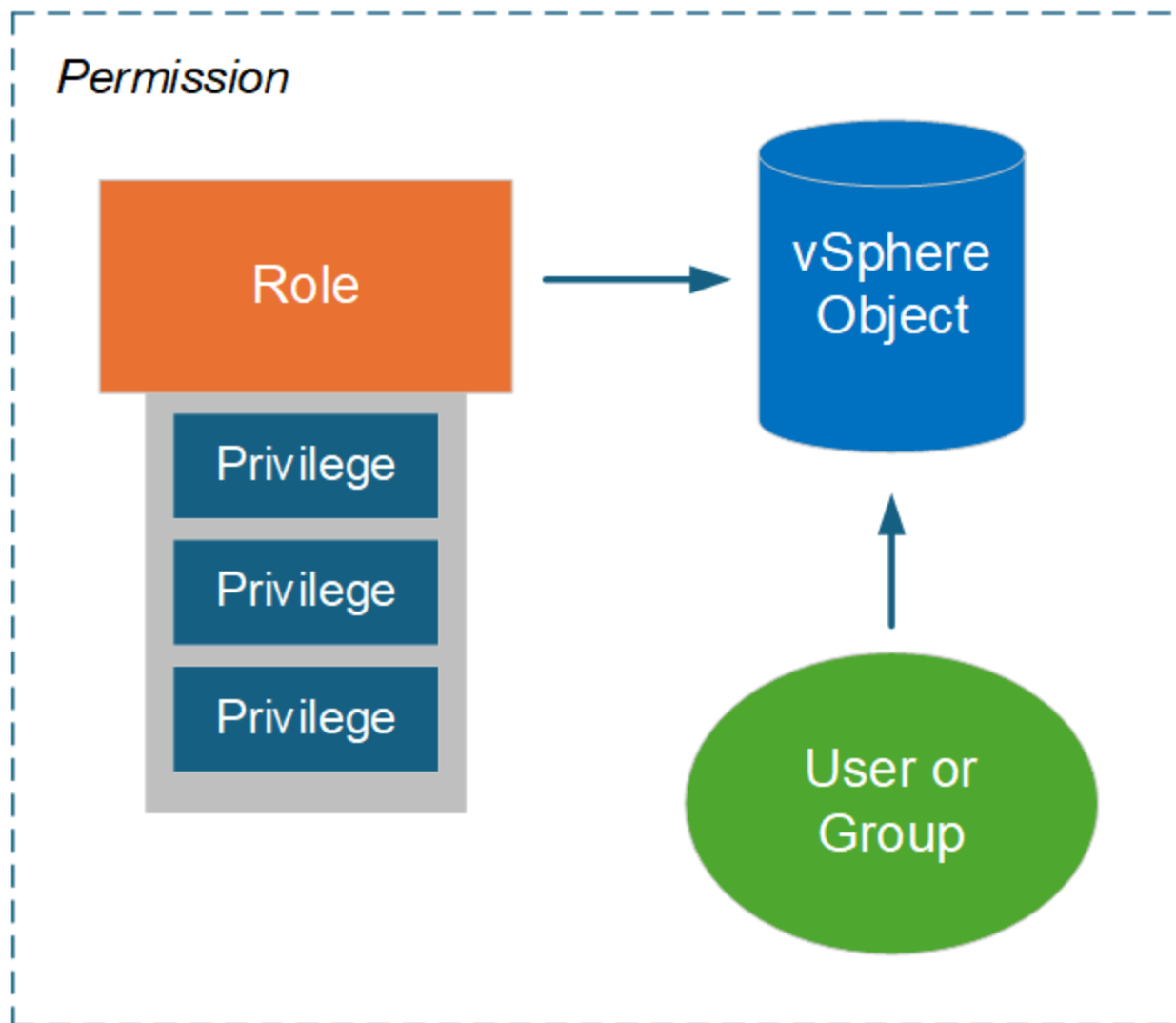
VMware vSphere を使用した RBAC

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ておく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ておく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てする必要があります。

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。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。