概念
ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

目次

概念

ONTAP toolsについて学ぶ

ONTAP tools for VMware vSphereは、仮想マシンのライフサイクル管理用のツール セットです。 VMware エコシステムと統合することで、データストアのプロビジョニングを簡素化し、仮想マシンの基本的な保護を提供します。これは、Open Virtual Appliance (OVA) として展開される、水平にスケーラブルなイベント駆動型マイクロサービスのコレクションです。

ONTAP tools for VMware vSphereは以下をサポートします。

- 保護や災害復旧などのコア仮想マシン（VM）機能
- ストレージポリシーベースの管理のためのVASAプロバイダー
- ポリシーベースのストレージ管理
- Storage Replication Adapter （ SRA ）

VMware 向け**ONTAP**ツールの高可用性

ONTAP tools for VMware vSphereは、障害発生時にも中断のない運用を維持できるように高可用性 (HA) サポートを提供します。

HA ソリューションは、次の種類の停止から迅速に回復するのに役立ちます。

- ホスト障害 - 単一ノード障害のみがサポートされます。
- ネットワーク障害
- 仮想マシン（ゲストOS）の障害
- アプリケーション（ONTAPツール）の障害

ONTAP tools for VMware vSphereを有効にするために、追加の構成を実行する必要はありません。

ONTAP tools for VMware vSphereはvCenter HA をサポートしていません。

HA 機能を使用するには、展開時または後で VM 設定で CPU ホット アドとメモリ ホット プラグが有効になっていることを確認します。

ONTAP toolsの主要な概念と用語

次のセクションでは、このドキュメントで使用される主な概念と用語について説明します。

認証局（**CA**）

CAは、Secure Sockets Layer（SSL）証明書を発行する信頼されたエンティティです。

一貫性グループ

整合性グループは、単一のユニットとして管理されるボリュームの集合です。整合性グループは、ストレージユニットおよびボリューム間でデータの整合性を保つために同期されます。ONTAPでは、複数のボリュームにまたがるアプリケーション ワークロードの管理が容易になり、保護が保証されます。詳細はこちら "整合グループ"。

デュアルスタック

デュアルスタックネットワークは、IPv4アドレスとIPv6アドレスの同時使用をサポートするネットワーク環境です。

高可用性（ **HA** ）

クラスタノードは、ノンストップオペレーションを実現するためにHAペアで構成されます。

Logical Unit Number（**LUN**；論理ユニット番号）

LUNは、Storage Area Network（SAN；ストレージエリアネットワーク）内の論理ユニットを識別するために使用される番号です。これらのアドレス指定可能なデバイスは、通常、SCSI（Small Computer System Interface）プロトコルまたはそのカプセル化された派生物の1つを介してアクセスされる論理ディスクです。

NVMeネームスペースとサブシステム

NVMeネームスペースは、論理ブロックにフォーマット可能な不揮発性メモリの容量です。ネームスペースはFCプロトコルやiSCSIプロトコルのLUNに相当し、NVMeサブシステムはigroupに相当します。NVMeサブシステムをイニシエータに関連付けると、関連付けられたイニシエータがサブシステム内のネームスペースにアクセスできるようになります。

ONTAPツールマネージャ

ONTAP tools Managerを使用すると、VMware vSphere管理者は、管理対象のvCenter Serverインスタンスとオンボードストレージバックエンドを介して、ONTAPツールをより細かく制御できます。vCenter Serverインスタンス、ストレージバックエンド、証明書、パスワード、ログバンドルのダウンロードの管理に役立ちます。

Open Virtual Appliance（**OVA**；オープン仮想アプライアンス）

OVAは、仮想マシン上で実行する必要がある仮想アプライアンスまたはソフトウェアをパッケージ化して配布するためのオープンスタンダードです。

目標復旧時点（**RPO**）

RPOは、データのバックアップまたはレプリケーションの頻度を測定します。これは、障害発生後に業務を再開するためにデータを復元する必要がある正確な時点を指定します。たとえば、RPOが4時間の組織では、災害発生時に最大4時間のデータ損失を許容できます。

SnapMirrorアクティブ同期

SnapMirror Active Syncを使用すると、サイト全体に障害が発生してもビジネスサービスの運用を継続できるため、アプリケーションをセカンダリコピーを使用して透過的にフェイルオーバーできます。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作やカスタムスクリプトは必要ありません。詳

細については "SnapMirrorアクティブ同期"、をご覧ください。

ストレージバックエンド

ストレージバックエンドは、ESXiホストが仮想マシンファイル、データ、およびその他のリソースを格納するために使用する基盤となるストレージインフラです。ESXiホストが永続的データにアクセスして管理できるため、仮想環境に必要なストレージ機能とパフォーマンスが提供されます。

グローバルクラスタ（ストレージバックエンド）

グローバルストレージバックエンドは、ONTAPクラスタのクレデンシャルでのみ使用でき、ONTAP tools Managerのインターフェイスからオンボードできます。最小限のPrivilegesで追加することで、VVOLの管理に必要な重要なクラスタリソースを検出できます。グローバルクラスタは、vVol管理用にSVMユーザをローカルに追加するマルチテナンシーシナリオに最適です。

ローカルストレージバックエンド

クラスタまたはSVMのクレデンシャルを使用したローカルストレージバックエンドは、ONTAP toolsのユーザインターフェイスで追加され、vCenterに限定されます。ローカルでクラスタのクレデンシャルを使用すると、関連付けられたSVMがvCenterに自動的にマッピングされてVVOLまたはVMFSが管理されます。SRAを含むVMFSの管理については、ONTAP toolsではグローバルクラスタを必要とせずにSVMクレデンシャルがサポートされます。

Storage Replication Adapter （ SRA ）

SRAは、VMware Live Site Recoveryアプライアンスにインストールされるストレージベンダー固有のソフトウェアです。このアダプタを使用すると、Site Recovery Managerとストレージコントローラの間で、Storage Virtual Machine（SVM）レベルおよびクラスタレベルの設定で通信できます。

Storage Virtual Machine（SVM）

SVMは、ONTAPのマルチテナンシーの単位です。SVMは、ハイパーバイザーで実行される仮想マシンと同様に、物理リソースを抽象化する論理エンティティです。SVMには、複数のデータボリュームと、クライアントへのデータの提供に使用するLIFが1つ以上含まれます。

均一な構成と非均一な構成

- *均一なホストアクセス*は、2つのサイトのホストが両方のサイトのストレージクラスタへのすべてのパスに接続されていることを意味します。サイト間パスが複数の距離にわたってストレッチされている。
- *非均一ホストアクセス*は、各サイトのホストが同じサイトのクラスタにのみ接続されることを意味します。サイト間パスとストレッチパスは接続されません。

> ⓘ 均一ホストアクセスは、すべてのSnapMirrorアクティブ同期配置でサポートされます。非均一ホストアクセスは、対称アクティブ/アクティブ配置でのみサポートされます。詳細については "ONTAPでのSnapMirrorアクティブ同期の概要"、をご覧ください。

Virtual Machine File System（VMFS）

VMFSは、VMware vSphere環境に仮想マシンファイルを格納するように設計された、クラスタ化されたファイルシステムです。

仮想ボリューム（ **VVOL** ）

vVols は、仮想マシンで使用されるストレージのボリューム レベルの抽象化を提供します。これにはいくつかの利点があり、従来のLUNの代わりに使用できます。 vVol データストアは通常、 vVolsのコンテナとして機能する単一の LUN に関連付けられます。

VMストレージポリシー

vCenter Serverの[Policies and Profiles]に仮想マシンストレージポリシーが作成されます。VVOLの場合は、NetApp VVOLストレージタイププロバイダのルールを使用してルールセットを作成します。

VMware Live Site Recovery

VMware Live Site Recoveryは、以前はSite Recovery Manager（SRM）と呼ばれていましたが、VMware仮想環境のビジネス継続性、ディザスタリカバリ、サイト移行、および無停止のテスト機能を提供します。

VMware vSphere APIs for Storage Awareness（VASA）

VASAは、管理用のストレージアレイとvCenter Serverを統合する一連のAPIです。このアーキテクチャは、VMware vSphereとストレージシステムの間の通信を処理するVASA Providerなど、複数のコンポーネントに基づいています。

VMware vSphere Storage APIs - Array Integration（VAAI）

VAAIは、VMware vSphere ESXiホストとストレージデバイスの間の通信を可能にする一連のAPIです。APIには、ストレージ処理をアレイにオフロードするためにホストが使用する一連のプリミティブ処理が含まれています。VAAIは、ストレージを大量に消費するタスクのパフォーマンスを大幅に向上させることができます。

vSphere Metroストレージクラスタ

vSphere Metro Storage Cluster（vMSC）は、拡張されたクラスタ環境でvSphereを有効にし、サポートするアーキテクチャです。vMSCソリューションは、NetApp MetroClusterおよびSnapMirror Active Sync（旧称SMBC）でサポートされます。これらのソリューションは、ドメインに障害が発生した場合のビジネス継続性を強化します。耐障害性モデルは、選択した構成に基づいています。詳細については "VMware vSphere Metroストレージクラスタ"、をご覧ください。

vVol データストア

vVolデータストアは、VASA Providerで作成および管理されるvVolコンテナを表す論理データストアです。

RPOはゼロです

RPOはRecovery Point Objective（目標復旧時点）の略で、所定の時間内に許容可能とみなされるデータ損失量です。RPOゼロとは、データ損失が一切許容されないことを意味します。

ロールベースのアクセス制御 (RBAC)

ONTAP tools RBAC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では、個 々 のユーザに許可を割り当てる

のではなく、特定のレベルの権限でロールを定義してアクションを実行することで、管理が簡易化されます。定義されたロールはユーザーに割り当てられます。これにより、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の標準モデルは、いくつかの実装テクノロジや複雑化するフェーズで構成されています。その結果、実際のRBACの導入は、ソフトウェアベンダーとその顧客のニーズに基づいて異なり、比較的単純なものから非常に複雑なものまでさまざまです。

RBACコンポーネント

大まかには、すべてのRBAC実装に一般的に含まれてい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部として、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。

ロール

a_role_は、1つ以上のPrivilegesを含むコンテナです。ロールは通常、特定のタスクまたはジョブ機能に基づいて定義されます。ロールをユーザに割り当てると、そのロールに含まれるすべてのPrivilegesがユーザに付与されます。また、Privileges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を作成できます。

オブジェクト

an_object_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。Privilegesで定義されたアクションは、関連オブジェクトに対して、または関連オブジェクトとともに実行されます。実装に応じて、Privilegesは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付与できます。

ユーザとグループ

_users_には、認証後に適用されるロールが割り当てられるか、またはロールに関連付けられます。RBACの実装によっては、1人のユーザに1つのロールのみを割り当てることができるものと、1人のユーザに複数のロールを割り当てることができるものがあります（一度に1つのロールのみがアクティブになる場合もあります）。ロールを_groups_に割り当てると、セキュリティ管理がさらに簡素化されます。

権限

a_permission_は'ロールとともにユーザーまたはグループを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することができます。

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。ONTAP tools for VMware vSphereでは、操作を実行するために vCenter とONTAP の両方で特定の権限が必要です。ONTAPツールはストレージ管理タスクを自動化しますが、vCenter またはONTAPのいずれにもユーザー アカウントを作成しません。サービス アカウントは、必要に応じて vSphere 管理者が作成する必要があります。このドキュメントでは、管理者が効果的なONTAPツール管理のために必要なロールと権限を割り当てるためのガイダンスを提供します。

VMware vCenter Server

VMware vCenter Serverに実装されたRBACは、vSphere Clientユーザ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 10のインストールの一環として、RBAC環境が拡張され、ONTAP toolsの機能を表すオブジェクトが追加されました。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。詳細については、を参照してください。"vCenter Server RBACカンキヨウ"

ONTAPクラスタ

ONTAP tools for VMware vSphere 10は、ONTAP REST APIを使用してONTAPクラスタに接続し、ストレージ関連の処理を実行します。ストレージリソースへのアクセスは、認証時に指定したONTAPユーザに関連付けられたONTAPロールで制御されます。詳細については、を参照してください "ONTAP RBACカンキヨウ" 。

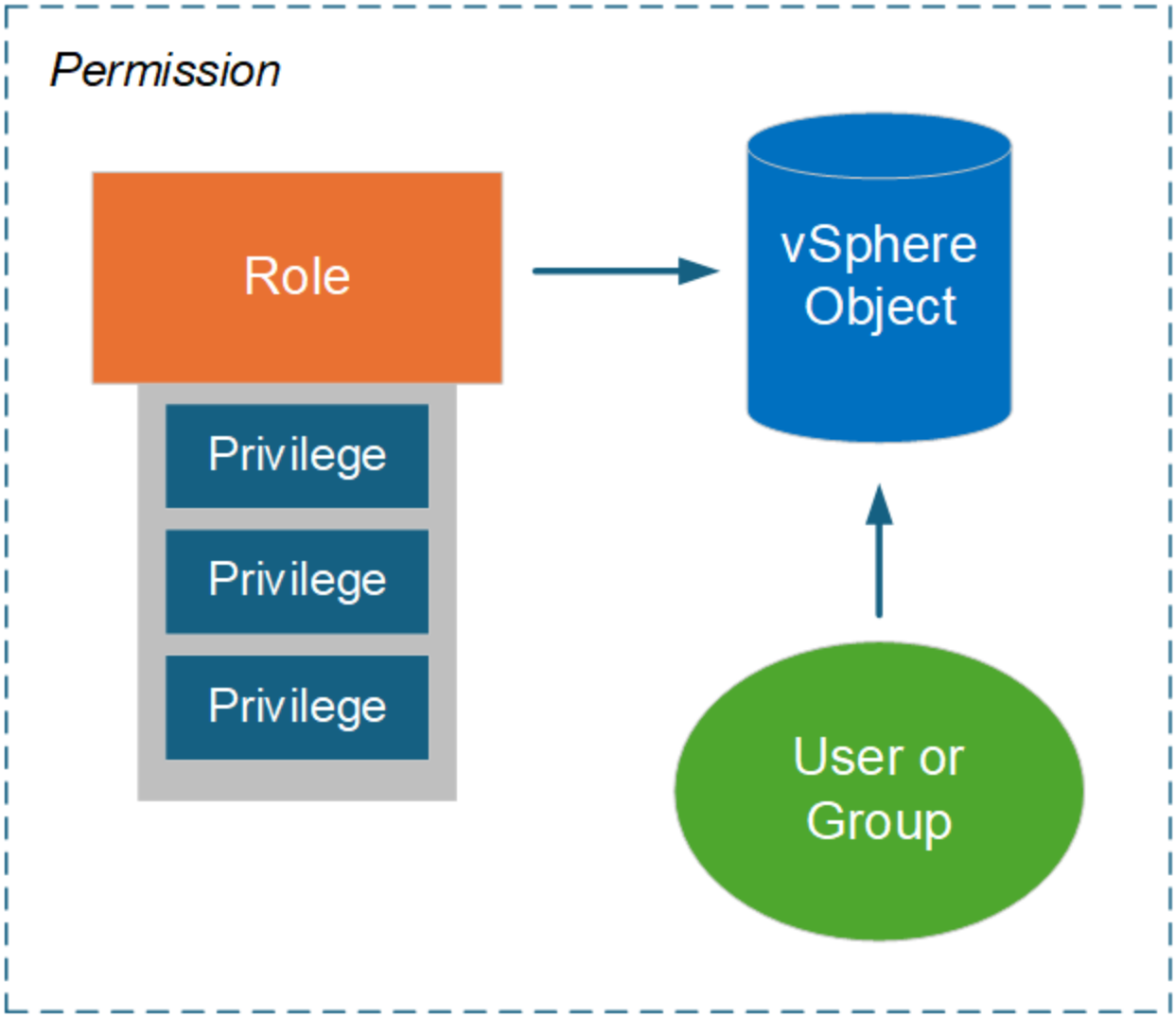
VMware vSphereを使用したRBAC

vCenter Server RBAC と ONTAP tools の連携

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 標準の権限

  これは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。

vCenter Serverの**RBAC**に関する**ONTAP tools**の考慮事項

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。vCenter の展開またはオンボーディングを担当する vCenter ユーザーに割り当てられるロールには、次の権限が含まれている必要があります。これらの権限が、展開またはオンボーディング プロセスの前提条件として構成されていることを確認します。

- アラーム
  - アラームを確認する
- コンテンツライブラリ
  - ライブラリアイテムを追加
  - テンプレートをチェックインする
  - テンプレートをチェックする
  - ファイルをダウンロードする
  - 輸入ストレージ
  - ストレージの読み取り
  - ライブラリアイテムを同期
  - 購読したライブラリを同期する
  - 構成設定を表示する
- 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エージェントマネージャ
  - 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
    - ネットワーク構成
    - System resources
    - 仮想マシンの自動起動構成
  - 現地での活動
    - Create virtual machine

        - Delete virtual machine
        - Reconfigure virtual machine
- ネットワーク
    - Assign network
    - 設定
- Ovfマネージャー
    - OvfConsumer アクセス
- ホストプロフィール
    - 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
- タスク
    - タスクを作成
    - 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
    - 動く
    - 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
        - 動く
        - 登録
        - 削除
        - 登録解除
    - 交流
        - 仮想マシン上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
        - カスタマイズ仕様を変更する
        - 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 3 つの定義済みロールがあります。

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
- データストアを管理します

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。

権限を割り当てます

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。

ONTAPを使用したRBAC

ONTAP RBAC が ONTAP tools と連携する仕組み

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で公開されるストレージおよびシステム処理へのアクセスを制御できます。ONTAP Tools for VMware vSphere 10環境で使用する前に、環境を理解しておくと役立ちます。

管理オプションの概要

ONTAP RBACを使用する際には、環境や目標に応じていくつかのオプションを使用できます。主な管理上の決定事項の概要を以下に示します。詳細については、も参照してください "ONTAPの自動化：RBACセキュリティの概要"。

> 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構成は必要ありません。

ロールとPrivilegesのタイプ

ONTAPユーザを定義するには、ONTAPロールが必要です。ONTAPロールには次の2種類があります。

- REST

  RESTロールはONTAP 9.6で導入されたもので、一般にREST APIを使用してONTAP にアクセスするユーザに適用されます。これらのロールに含まれるPrivilegesは、ONTAP REST APIエンドポイントへのアクセスと関連するアクションの観点から定義されます。

- 伝統的

  これらはONTAP 9.6より前のレガシーロールです。これらはRBACの基本的な側面であり続けています。Privilegesは、ONTAP CLIコマンドへのアクセスという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、従来のロールには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含めることもできます。これにより、Privilegesは、追加のクエリパラメータが適用されるオブジェクトをより正確に定義できます。

適用範囲

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。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。

ロールの定義

ONTAPには、クラスタレベルとSVMレベルの両方で事前定義された一連のロールが用意されています。カスタムロールを定義することもできます。

ONTAP RESTロールの使用

ONTAP tools for VMware vSphere 10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。

ロールマッピング

従来のロールを使用するかRESTロールを使用するかに関係なく、すべてのONTAPアクセスの決定は基になるCLIコマンドに基づいて行われます。ただし、RESTロールのPrivilegesはREST APIエンドポイントで定義されるため、ONTAPでは各RESTロールに対して_mapped_traditionalロールを作成する必要があります。そのため、各RESTロールは基盤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、ロールタイプ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。並行マッピングされたロールは変更できません。

CLI Privilegesを使用した**REST**ロールの定義

ONTAPでは常に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エンドポイントの代わりにCLIコマンドPrivilegesを使用してRESTロールを表すことができます。このアプローチのメリットの1つは、従来の役割で利用できるきめ細かさです。

ONTAPロールを定義する際の管理インターフェイス

ONTAP CLIおよびREST APIを使用して、ユーザとロールを作成できます。ただし、System Managerのインターフェイスと ONTAP tools Managerから利用できるJSONファイルを使用する方が便利です。詳細については、を参照してください "ONTAP RBACとONTAP Tools for VMware vSphere 10の使用" 。

ONTAP tools に関する **ONTAP RBAC** の考慮事項

ONTAPでのONTAP Tools for VMware vSphere 10 RBAC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。

セツテイフロセスノカイヨウ

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。

主な設定手順について、以下で大まかに説明します。"ONTAPユーザのロールと権限の設定"詳細については、を参照してください。

1.準備

ONTAP tools ManagerとONTAPクラスタの両方に対する管理クレデンシャルが必要です。

2.JSON定義ファイルをダウンロードする

ONTAP tools Managerのユーザインターフェイスにサインインしたら、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**ユーザを作成する

System Managerにサインインしたら、ユーザとロールを作成できます。

1. 左側の*を選択し、[設定]*を選択します。
2. [ユーザとロール]*まで下にスクロールし、をクリックします -→。
3. [Users]で[Add]*を選択し、[Virtualization products]*を選択します。
4. ローカルワークステーションでJSONファイルを選択してアップロードします。

4.ロールを設定する

ロールの定義の一環として、いくつかの管理上の決定を行う必要があります。詳細については、を参照してくださいSystem Managerを使用してロールを設定する。

System Managerを使用してロールを設定する

System Managerで新しいユーザ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、環境とニーズに基づいてロールをカスタマイズできます。

コアユーザとロールの設定

RBACの定義は、VSC、VASA Provider、SRAなど、複数の製品機能としてパッケージ化されています。RBACのサポートが必要な環境を選択してください。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。また、ユーザ名と関連するパスワードを選択する必要があります。

権限

Privilegesロールは、ONTAPストレージに必要なアクセスレベルに基づいて4セットに分類されます。ロールのベースとなるPrivilegesには次のものがあります。

- 検出

  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、Discoveryロールに関連付けられているすべてのPrivilegesも含まれます。

- ストレージの変更

  ストレージを変更できます。また、discoveryおよびcreate storageのロールに関連付けられているすべてのPrivilegesも含まれます。

- ストレージの削除

  ストレージを破棄できます。また、検出、ストレージの作成、ストレージの変更の各ロールに関連付けられているすべてのPrivilegesも含まれます。

ロールを持つユーザを生成する

環境の構成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、次の値を連結したものです。

- JSONファイルで定義された固定プレフィックス値（例：「OTV_10」）
- 選択した製品機能
- 権限セットのリスト。

例

```
OTV_10_VSC_Discovery_Create
```

新しいユーザーが「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。