



概念

## ONTAP tools for VMware vSphere 9.10

NetApp

January 18, 2024

# 目次

概念 .....	1
ONTAP ツールの概要 .....	1
VVOL 向けの VASA Provider の設定 .....	2
ディザスタリカバリを設定する .....	4
ロールベースアクセス制御 .....	4
ONTAP ツールのハイアベイラビリティを設定する .....	13
ONTAP ツールでサポートされる MetroCluster 構成 .....	14

# 概念

## ONTAP ツールの概要

VMware vSphere 用の ONTAP ツールは、ネットアップストレージシステムを使用する VMware 環境の仮想マシンに対して、エンドツーエンドのライフサイクル管理を提供します。管理者が vCenter Server 内でストレージを直接管理できるため、VMware 環境のストレージとデータの管理が簡単になります。

VMware は vSphere 6.5 で vSphere Client という名前の新しい HTML5 ベースのクライアントを導入しました。ONTAP ツール 9.6 以降のリリースでは、vSphere Client のみがサポートされます。ONTAP ツールは vSphere Client と統合されており、シングルサインオン（SSO）サービスを利用できます。複数の vCenter Server インスタンスがある環境では、管理する vCenter Server インスタンスごとに固有の VSC インスタンスを登録する必要があります。

ONTAP ツールの各コンポーネントは、ストレージをより効率的に管理するための機能を提供します。

### Virtual Storage Console （VSC）

VSC では次の作業を実行できます。

- SRA と VASA Provider の両方で利用できるストレージコントローラを追加し、クレデンシャルを割り当て、VSC のストレージコントローラのアクセス許可を設定する
- データストアをプロビジョニング
- vCenter Server 環境でデータストアと仮想マシンのパフォーマンスを監視します
- Role-Based Access Control （RBAC ; ロールベースアクセス制御）を使用して、次の 2 つのレベルで vCenter Server オブジェクトへの管理者アクセスを制御します。
  - 仮想マシンやデータストアなどの vSphere オブジェクト

これらのオブジェクトの管理には vCenter Server RBAC を使用します。

- ONTAP ストレージ

ストレージシステムの管理には ONTAP RBAC を使用します。

- ネットアップストレージに接続されている ESXi ホストのホスト設定を表示および更新します

NFS Plug-in for VMware vStorage APIs for Array Integration （VAAI）を使用することは、VSC のプロビジョニング処理にメリットがあります。NFS Plug-in for VAAI は、ESXi ホストにインストールされている VMware の仮想ディスクライブラリを統合するソフトウェアライブラリです。VMware VAAI パッケージを使用すると、特定のタスクを物理ホストからストレージアレイにオフロードできます。シンプロビジョニングやハードウェアアクセラレーションなどのタスクをアレイレベルで実行して、ESXi ホスト上のワークロードを削減できます。コピーオフロード機能やスペースリザーベーション機能によって、VSC の処理のパフォーマンスが向上します。

NetApp NFS Plug-in for VAAI は VSC に付属していません。ただし、ネットアップサポートサイトから、このプラグインのインストールパッケージをダウンロードして、インストール手順を確認できます。

## VASA Provider

VASA Provider for ONTAP は、VMware vSphere APIs for Storage Awareness（VASA）を使用して、VMware vSphere で使用されているストレージに関する情報を vCenter Server に送信します。ONTAP のツールには、VASA Provider と VSC が統合されています。VASA Provider では次の作業を実行できます。

- VMware 仮想ボリューム（vVol）データストアをプロビジョニングする
- 環境に応じた異なるストレージのサービスレベル目標（SLO）を定義するストレージ機能プロファイルを作成して使用します
- データストアがストレージ機能プロファイルに準拠しているかどうかを確認する
- ボリュームやアグリゲートがしきい値に近づいたときに警告するようにアラームを設定します
- VVol データストアに作成された仮想マシンディスク（VMDK）と仮想マシンのパフォーマンスを監視する

ONTAP 9.6 以前を使用している場合、VASA Provider は VASA API を使用して vCenter Server と通信し、ZAPI と呼ばれるネットアップの API を使用して ONTAP と通信します。ONTAP 9.6 以前の vVol ダッシュボードを表示するためには、OnCommand API サービスをインストールして vCenter Server に登録しておく必要があります。ONTAP 9.7 以降のバージョンを使用している場合、vVol ダッシュボードを表示するために OnCommand API サービスを VASA Provider に登録する必要はありません。



ONTAP 9.6 以前では、VASA Provider に専用の OnCommand API サービスインスタンスが必要です。OnCommand API サービスの 1 つのインスタンスを複数の VASA Provider インスタンスで共有することはできません。

## Storage Replication Adapter（SRA）

SRA を有効にして VMware Site Recovery Manager（SRM）と一緒に使用している場合、障害時に vCenter Server のデータストアと仮想マシンをリカバリできます。SRA を使用すると、障害時のディザスタリカバリに、保護対象サイトとリカバリサイトにアレイベースのレプリケーション（ABR）を使用できます。

- 関連情報 \*

["ネットアップサポート"](#)

## VVOL 向けの VASA Provider の設定

VASA Provider for ONTAP を使用して、VMware 仮想ボリューム（vVol）を作成および管理することができます。VVOL データストアをプロビジョニング、編集、マウント、削除できます。また、VVOL データストアへのストレージの追加や VVOL データストアからのストレージの削除も行うことができます。柔軟性を高めることができます。すべての仮想マシンおよび関連する VMDK をプロビジョニングおよび管理できます。

VVOL データストアは、ストレージコンテナ（「バックアップストレージ」とも呼ばれます）に含まれる 1 つ以上の FlexVol ボリュームで構成されます。仮想マシンは 1 つの vVol データストアまたは複数の vVol データストアに分散している場合があります。

複数の FlexVol を含む VVOL データストアを作成する場合は、ストレージコンテナ内のすべての FlexVol で同じプロトコル（NFS、iSCSI、または FCP）および同じ Storage Virtual Machine（SVM）を使用する必

必要があります。

基盤となるストレージについての詳しい情報は必要ありません。たとえば、ストレージを格納する FlexVol を特定する必要はありません。FlexVol を VVOL データストアに追加すると、ストレージ要件がストレージコンテナで管理されるようになり、VM のプロビジョニング時に、VMware が容量のないバックアップボリュームにプロビジョニングされる状態を防ぐことができます。



パフォーマンスと柔軟性を高めるために、1 つの vVol データストアに複数の FlexVol を含めることを推奨します。FlexVol ボリュームの LUN 数には制限があり、それによって仮想マシンの数が制限されるため、複数の FlexVol を使用することで、より多くの仮想マシンを vVol データストアに格納することができます。

セットアッププロセスでは、作成する vVol データストアのストレージ機能プロファイルを指定する必要があります。1 つの vVol データストアに対して 1 つ以上の VASA Provider のストレージ機能プロファイルを選択できます。また、ストレージコンテナ内に自動で作成される vVol データストアに適用するデフォルトのストレージ機能プロファイルも指定できます。

VASA Provider では、仮想マシンのプロビジョニングまたは VMDK の作成時に、必要に応じてさまざまなタイプの VVOL を作成します。

#### • \* 設定 \*

この vVol データストアは、設定情報を格納するために VMware vSphere で使用されます。

SAN（ブロック）環境の場合、ストレージは 4GB の LUN です。

NFS 実装の場合は、vmx ファイルなどの VM 構成ファイル、および他の VVOL データストアへのポインタを含むディレクトリになります。

#### • \* データ \*

この vVol には、オペレーティングシステムの情報やユーザファイルが格納されます。

SAN 環境の場合は、仮想ディスクと同じサイズの LUN です。

NFS 環境の場合は、仮想ディスクと同じサイズのファイルです。

ONTAP クラスタ 9.8 以降でプロビジョニングされた NFS データ VVol ごとに、IOPS、スループット、レイテンシなどのパフォーマンス指標を監視するためにすべての VMDK ファイルが登録されます。

#### • \* スワップ \*

この vVol は、仮想マシンの電源をオンにすると作成され、オフにすると削除されます。

SAN 環境の場合は、仮想メモリと同じサイズの LUN です。

NFS 環境の場合は、仮想メモリと同じサイズのファイルです。

#### • \* メモリ \*

この vVol は、VM スナップショットの作成時にメモリのスナップショットオプションを選択した場合に作成されます。

SAN 環境の場合は、仮想メモリと同じサイズの LUN です。

NFS 環境の場合は、仮想メモリと同じサイズのファイルです。

## ディザスタリカバリを設定する

ディザスタリカバリの設定は、VMware の Site Recovery Manager (SRM) とともに vCenter Server で作成および管理できます。

VASA Provider に Storage Replication Adapter (SRA) の機能が組み込まれました。データセンターで VVOL データストアを設定している場合は、VVOL データストアのリカバリ用に、ディザスタリカバリ用に SRA を別途インストールする必要はありません。Site Recovery Manager (SRM) で、保護対象サイトとリカバリサイトをペアリングする必要があります。サイトをペアリングしたら、SRM の次の設定作業としてアレイペアを設定します。アレイペアにより、SRM がストレージシステムと通信してデバイスとデバイスのレプリケーションを検出できるようになります。アレイペアを設定する前に、まず SRM でサイトペアを作成する必要があります。

このリリースの ONTAP ツールには、ディザスタリカバリに同期 SnapMirror 設定を使用するオプションがあります。



VMware Site Recovery Manager (SRM) では、VVOL データストアのディザスタリカバリの管理に SRA は使用されません。代わりに、ONTAP 9.7 以降のクラスタの VVOL データストアのレプリケーションとフェイルオーバー制御に VASA Provider を使用します。

["Storage Replication Adapter を有効にする"](#)

## ロールベースアクセス制御

### ONTAP ツールでのロールベースアクセス制御の概要

vCenter Server の RBAC を使用すると、vSphere オブジェクトへのアクセスを制御できます。VMware vSphere 用の ONTAP® ツールでは、vCenter Server RBAC と ONTAP RBAC により、特定のストレージシステムのオブジェクトに対して特定のユーザが実行できる VSC タスクが決まります。

タスクを完了するには、適切な vCenter Server RBAC アクセス許可が必要です。VSC でのタスクの実行時、まずユーザの vCenter Server アクセス許可が確認され、次にユーザの ONTAP 権限が確認されます。

vCenter Server アクセス許可をルートオブジェクト（ルートフォルダ）に対して設定することができます。その後、アクセス許可が不要な子エンティティのアクセスを禁止することでセキュリティを強化できます。

### vCenter Server アクセス許可の要素

vCenter Server で認識されるのはアクセス許可で、権限ではありません。vCenter Server アクセス許可は 3 つの要素で構成されます。

vCenter Server には次のコンポーネントがあります。

- 1 つ以上の権限（ロール）

ユーザが実行できるタスクを定義します。

- vSphere オブジェクト

タスクの対象となるオブジェクトです。

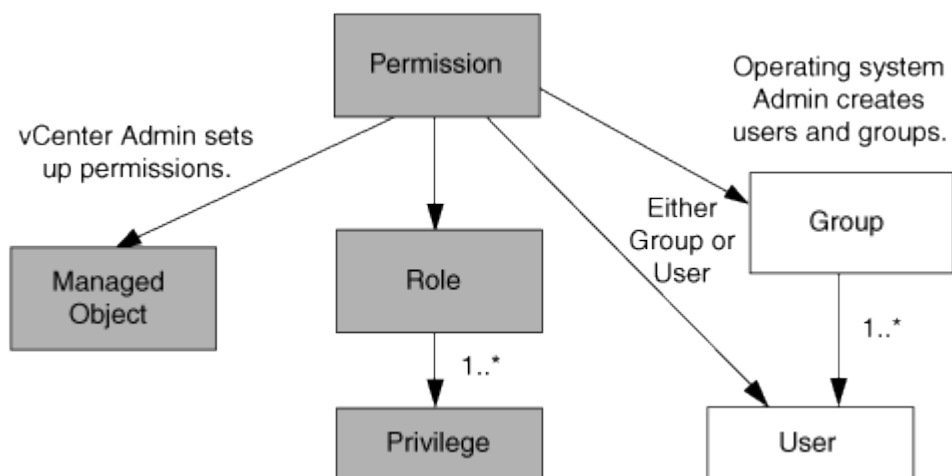
- ユーザまたはグループ

タスクを実行できるユーザまたはグループを定義します。

次の図に示すように、3 つの要素がすべて揃っていないとアクセスは許可されません。



グレーのボックスは vCenter Server 側の要素、白のボックスは vCenter Server を実行しているオペレーティングシステム側の要素を表しています。



## 権限

VMware vSphere 用の ONTAP ツールには、次の 2 種類の権限が関連付けられています。

- vCenter Server 標準の権限

vCenter Server に付属している権限です。

- VSC 固有の権限

特定の VSC タスク用に定義された、VSC 固有の権限です。

VSC のタスクを実行するには、VSC 固有の権限と vCenter Server 標準の権限の両方が必要です。これらの権限は ' ユーザーのロールを構成しますアクセス許可には複数の権限を含めることができます。これらの権限は、vCenter Server にログインしているユーザを対象としています。



vCenter Server RBAC の使用を簡単にするため、VSC には、VSC タスクの実行に必要な VSC 固有の権限と標準の権限をすべて含む標準ロールがいくつか用意されています。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

* 権限 *	* 役割 *	* タスク *
NetApp ONTAP Tools Console > View の順にクリックします	<ul style="list-style-type: none"> <li>• VSC 管理者</li> <li>• VSC によるプロビジョニング</li> <li>• VSC 読み取り専用</li> </ul>	VSC および VASA Provider 固有のタスクにはすべて View 権限が必要です。
NetApp Virtual Storage Console > Policy Based Management > Management または privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > Management の順にクリックします	VSC 管理者	ストレージ機能プロファイルおよびしきい値設定に関連する VSC および VASA Provider のタスク。

## 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、とフォルダ。任意の vSphere オブジェクトに権限を割り当てることができます。vSphere オブジェクトに割り当てられたアクセス許可に基づいて、そのオブジェクトに対してどのユーザがどのタスクを実行できるかが決まります。VSC 固有のタスクについては、アクセス許可の割り当てと検証はルートフォルダレベル（vCenter Server）でのみ行われ、それ以外のエンティティでは行われません。ただし VAAI プラグインの処理は例外で、関連する ESXi に対して権限が検証されます。

## 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 マシン）を使用して設定できます。その後、設定したユーザまたはグループに vCenter Server アクセス許可を付与することで、特定の VSC タスクの実行を許可することができます。



これらの vCenter Server アクセス許可は、VSC 管理者以外の VSC vCenter ユーザに適用されます。VSC 管理者には、デフォルトでフルアクセスが許可されるため、アクセス許可を割り当てる必要はありません。

ユーザとグループにはロールは割り当てられません。vCenter Server アクセス許可を割り当てることで、間接的にロールが適用されます。

## vCenter Server のアクセス許可の割り当てと変更に関する要点

vCenter Server のアクセス許可を使用する際にはいくつかの点に注意する必要があります。VMware vSphere タスク用の ONTAP ツールを使用できるかどうかは、アクセス許可を割り当てた場所、およびアクセス許可の変更後にユーザが実行した操作によって決まります。

### 権限を割り当てます

vCenter Server のアクセス許可は、vSphere のオブジェクトおよびタスクへのアクセスを制限したい場合にのみ設定します。それ以外の場合は、管理者としてログインできます。このログインでは、すべての vSphere



オブジェクトに自動的にアクセスできます。

アクセス許可を割り当てる場所によって、ユーザが実行できる VSC タスクが決まります。

タスクによっては、完了を確認するために、ルートオブジェクトなどの上位レベルにアクセス許可を割り当てる必要があります。具体的には、特定の vSphere オブジェクトには適用されない権限（タスクの追跡など）がタスクに必要な場合や、必要な権限環境が vSphere 以外のオブジェクト（ストレージシステムなど）に必要な場合です。

このような場合は、子エンティティに継承されるようにアクセス許可を設定できます。子エンティティには、他の権限も割り当てることができます。子エンティティに割り当てたアクセス許可は、親エンティティから継承されたアクセス許可を上書きします。したがって、子エンティティにアクセス許可を割り当てることで、ルートオブジェクトに割り当てられ、子エンティティに継承されたアクセス許可の対象を制限することができます。



会社のセキュリティポリシーでアクセス許可を厳しく制限することが求められる場合を除き、ルートオブジェクト（ルートフォルダとも呼ばれる）にアクセス許可を割り当てることを推奨します。

## アクセス許可と非 vSphere オブジェクト

作成したアクセス許可は、vSphere 以外のオブジェクトに適用されます。たとえば、ストレージシステムは vSphere オブジェクトではありません。環境ストレージシステムにアクセス許可を割り当てることができる vSphere オブジェクトがないため、権限がある場合は、その権限を含むアクセス許可を VSC 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、「Add/Modify/Skip storage systems」といった VSC 権限を含む任意のアクセス許可は、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。

## アクセス許可の変更

一度に変更できるアクセス許可は 1 つです。

アクセス許可に含まれる権限が変更された場合、そのアクセス許可が関連付けられたユーザは、更新されたアクセス許可を有効にするためにログアウトしてログインし直す必要があります。

## ONTAP ツールに付属の標準ロール

vCenter Server の権限と RBAC を簡単に使用できるように、Virtual Storage Console（VSC）には主要な VSC タスクを実行できる標準の VSC ロールが用意されています。また、タスクの実行を制限し、VSC 情報の表示のみを許可する読み取り専用ロールもあります。

標準の VSC ロールには、ユーザが VSC タスクを実行するために必要な VSC 固有の権限と vCenter Server 標準の権限の両方が含まれています。また、サポートされるどのバージョンの vCenter Server でも必要な権限が付与されるように設定されています。

管理者は、必要に応じてこれらのロールをユーザに割り当てることができます。



VSC を最新バージョンにアップグレードした場合は、新しいバージョンの VSC で使用できるように自動的にアップグレードされます。

VSC の標準ロールは、vSphere Client のホームページで \* Roles \* をクリックすると表示できます。

VSC の組み込みのロールで実行できるタスクを次に示します。

* 役割 *	* 概要 *
VSC 管理者	すべての VSC タスクを実行するために必要な vCenter Server 標準の権限と VSC 固有の権限がすべて含まれています。
VSC 読み取り専用	VSC に対する読み取り専用アクセスが許可されます。アクセスが制御された VSC の処理は実行できません。
VSC によるプロビジョニング	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 VSC 固有の権限がすべて含まれています。次のタスクを実行できます。 <ul style="list-style-type: none"><li>• 新しいデータストアを作成する</li><li>• データストアを削除</li><li>• ストレージ機能プロファイルに関する情報を表示する</li></ul>

## VSC の標準ロールの使用に関するガイドライン

VMware vSphere の標準的な ONTAP ツールを使用する場合は、一定のガイドラインに従う必要があります。

標準ロールは直接変更しないでください。ロールを直接変更すると、VSC をアップグレードするたびに変更が上書きされます。VSC をアップグレードするたびに、インストーラによって標準ロールの定義が更新されます。これにより、そのバージョンの VSC およびサポートされるすべてのバージョンの vCenter Server でロールを最新の状態に維持できます。

ただし、標準のロールを使用して環境に合わせたロールを作成することもできます。これを行うには、VSC の標準ロールをコピーし、コピーしたロールを編集します。新しいロールを作成しても、VSC Windows サービスを再起動またはアップグレードしてもこのロールを維持できます。

VSC の標準ロールの用途としては、次のようなものがあります。

- すべての VSC タスクに標準の VSC ロールを使用する。

このシナリオでは、標準ロールは VSC タスクの実行に必要なすべての権限をユーザに提供します。

- 複数のロールを組み合わせてユーザが実行できるタスクを拡張する。

単独では要件に合う標準の VSC ロールがない場合は、複数のロールを含む上位グループを作成してロールを拡張できます。

ユーザが vCenter Server 標準の別の権限を必要とする VSC 以外のタスクも実行する必要がある場合は、それらの権限を提供するロールを作成し、グループに追加します。

- より細分化されたロールを作成します。

標準の VSC ロールよりも少ない権限のロールが必要な場合は、VSC ロールを使用して新しいロールを作成することができます。

この場合は、必要な VSC ロールのクローンを作成し、そのクローンを編集してユーザーに必要な権限だけを残します。

## VSC タスクに必要な権限

VMware vSphere のタスクを実行するために必要な ONTAP ツールの権限の組み合わせは、Virtual Storage Console (VSC) に固有の権限と vCenter Server 標準の権限の組み合わせと異なります。

VSC タスクに必要な権限については、ネットアップの技術情報アーティクル 1032542 を参照してください。

### "Virtual Storage Console 用の RBAC の設定方法"

#### VMware vSphere 用の ONTAP ツールで必要な製品レベルの権限

VMware vSphere GUI の ONTAP ツールにアクセスするには、製品レベルの VSC 固有の View 権限が、適切な vSphere オブジェクトレベルで割り当てられている必要があります。この権限なしでログインすると、NetApp アイコンをクリックしたときにエラーメッセージが表示され、VSC にアクセスできません。

次の表に、VSC の製品レベルの View 権限について説明します。

* 権限 *	* 概要 *	* 割り当てレベル *
表示	VSC の GUI にアクセスできます。VSC でタスクを実行することはできません。VSC のタスクを実行するには、タスクで使用する適切な VSC 固有の権限と vCenter Server の標準権限が必要です。	<p>割り当てレベルによって、表示できる UI の部分が決まります。ルートオブジェクト（フォルダ）に View 権限が割り当てられている場合、NetApp アイコンをクリックして VSC にアクセスできます。</p> <p>他の vSphere オブジェクトレベルに View 権限を割り当ててもできますが、その場合は表示および使用できる VSC メニューが制限されます。</p> <p>View 権限を含むアクセス許可は、ルートオブジェクトに割り当てることを推奨します。</p>

## ONTAP ストレージシステムおよび vSphere オブジェクトの権限

ONTAP の RBAC を使用すると、特定のストレージシステムへのアクセスとそれらのストレージシステムで実行できる操作を制御できます。VMware vSphere 用の ONTAP<sup>®</sup> ツールでは、ONTAP RBAC と vCenter Server RBAC により、特定のストレージシステ

ムのオブジェクトに対して特定のユーザが実行できる Virtual Storage Console（VSC）タスクが決まります。

VSC では、各ストレージシステムの認証とそのストレージシステムで実行できるストレージ操作の判別に、VSC で設定したクレデンシャル（ユーザ名とパスワード）が使用されます。ストレージシステムごとに 1 組のクレデンシャルが使用され、そのクレデンシャルに基づいて、ストレージシステムで実行できる VSC タスクが決まります。つまり、このクレデンシャルは VSC のクレデンシャルであり、個々の VSC ユーザに対するものではありません。

ONTAP RBAC は、ストレージシステムへのアクセス、および仮想マシンのプロビジョニングなど、ストレージに関連する VSC タスクの実行にのみ適用されます。それぞれのストレージシステムに対する適切な ONTAP RBAC 権限がないと、そのストレージシステムでホストされる vSphere オブジェクトに対してタスクを実行することはできません。ONTAP RBAC と VSC 固有の権限を組み合わせることで、ユーザが実行できる VSC タスクを制御することができます。

- ストレージまたはストレージシステムに格納されている vCenter Server オブジェクトの監視と設定
- ストレージシステムに格納されている vSphere オブジェクトのプロビジョニング

ONTAP RBAC と VSC 固有の権限を使用すると、ストレージ主体のセキュリティレイヤをストレージ管理者が管理できるようになります。これにより、ONTAP RBAC または vCenter Server RBAC のどちらか一方のアクセス制御だけを使用した場合に比べ、よりきめ細かい制御が可能になります。たとえば、vCenter Server RBAC を使用して、ネットアップストレージでのデータストアのプロビジョニングを vCenterUserB には許可し、vCenterUserA には許可しないように設定したとします。この場合、特定のストレージシステムのクレデンシャルに対してストレージの作成を禁止すれば、vCenterUserB と vCenterUserA のどちらもそのストレージシステムでデータストアのプロビジョニングを実行することはできません。

VSC タスクを開始すると、最初にそのタスクに対する正しい vCenter Server アクセス許可がユーザにあるかどうかを検証されます。タスクを実行するための十分な vCenter Server アクセス許可がなければ、最初の vCenter Server のセキュリティチェックをパスできないため、そのストレージシステムの ONTAP 権限は確認されません。そのため、ストレージシステムにアクセスできません。

十分な vCenter Server アクセス許可がある場合は、次にストレージシステムのクレデンシャル（ユーザ名とパスワード）に関連付けられた ONTAP RBAC 権限（ONTAP ロール）が確認されます。その VSC タスクで必要なストレージ処理をストレージシステムで実行するための十分な権限があるかどうかを確認すること。適切な ONTAP 権限があれば、ストレージシステムにアクセスして VSC タスクを実行できます。ストレージシステムで実行できる VSC タスクは ONTAP ロールで決まります。

各ストレージシステムには、一連の ONTAP 権限が関連付けられます。

ONTAP RBAC と vCenter Server RBAC の両方を使用すると、次のような利点があります。

- セキュリティ

どのユーザがどのタスクを実行できるかを、vCenter Server オブジェクトレベルおよびストレージシステムレベルで制御できます。

- 監査情報

多くの場合、VSC はストレージシステムについての監査証跡を提供します。これにより、ストレージに対して変更を行った vCenter Server ユーザまでさかのぼってイベントを追跡できます。

- 使いやすさ

コントローラのクレデンシャルをすべて集約して一元管理できます。

## VMware vSphere 用の ONTAP ツールを使用する際に推奨される ONTAP ロール

VMware vSphere および Role-Based Access Control (RBAC ; ロールベースアクセス制御) 用の ONTAP® ツールを使用する際に推奨される ONTAP ロールをいくつか設定できます。これらのロールには、Virtual Storage Console (VSC) タスクで実行するストレージ処理に必要な ONTAP 権限が含まれています。

新しいユーザロールを作成するには、ONTAP を実行しているストレージシステムに管理者としてログインする必要があります。次のいずれかを使用して ONTAP ロールを作成できます。

- ONTAP システムマネージャ 9.8P1 以降

### "ユーザロールと権限を設定"

- RBAC User Creator for ONTAP ツール (ONTAP 9.6 以前を使用している場合)

各 ONTAP ロールには、ロールのクレデンシャルを構成するユーザ名とパスワードのペアが関連付けられています。このクレデンシャルを使用してログインしないと、ロールに関連付けられたストレージ処理にアクセスできません。

セキュリティ対策として、VSC 固有の ONTAP ロールは階層構造になっています。最初のロールは最も制限のあるロールで、VSC の最も基本的なストレージ処理に関連する権限だけを含みます。次のロールには、そのロール独自の権限と、前のロールに関連付けられているすべての権限が含まれます。以降、上位のロールほど制限が少なく、より多くのストレージ処理をサポートします。

VSC を使用する際に推奨される ONTAP RBAC ロールのいくつかを次に示します。ロールを作成したら、仮想マシンのプロビジョニングなど、ストレージに関するタスクを実行する必要があるユーザにそのロールを割り当てることができます。

#### 1. 検出

ストレージシステムを追加できます。

#### 2. ストレージを作成します

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権限が含まれます。

#### 3. ストレージを変更します

ストレージを変更できます。また、Discovery ロールと Create Storage ロールに関連付けられているすべての権限が含まれます。

#### 4. ストレージを破棄します

ストレージを破棄できます。また、Discovery ロール、Create Storage ロール、Modify Storage ロールに関連付けられているすべての権限が含まれます。

VASA Provider for ONTAP を使用する場合は、Policy-Based Management (PBM ; ポリシーベース管理) ロールも設定します。ストレージポリシーを使用してストレージを管理できます。このロールを使用するには、「検出」ロールも設定する必要があります。

## VMware vSphere 用の ONTAP ツール用に ONTAP の RBAC を設定する方法

VMware vSphere 用の ONTAP ツールでロールベースアクセス制御を使用する場合は、ストレージシステムで ONTAP RBAC を設定する必要があります。ONTAP RBAC 機能を使用すると、アクセス権限を制限したカスタムユーザアカウントを 1 つ以上作成できます。

VSC と SRA は、クラスタレベルまたは Storage Virtual Machine (SVM) レベルでストレージシステムにアクセスできます。クラスタレベルでストレージシステムを追加する場合、必要なすべての機能を使用するには、管理者ユーザのクレデンシャルを指定する必要があります。SVM の詳細を直接追加してストレージシステムを追加する場合は、「vsadmin」ユーザには特定のタスクを実行するために必要なすべてのロールと機能が付与されるわけではないことに注意してください。

VASA Provider は、クラスタレベルでのみストレージシステムにアクセスできます。特定のストレージコントローラで VASA Provider が必要な場合は、VSC または SRA を使用している場合でも、クラスタレベルでストレージシステムを VSC に追加する必要があります。

新しいユーザを作成し、クラスタまたは SVM を ONTAP ツールに接続するには、次の作業を行う必要があります。

- クラスタ管理者または SVM 管理者ロールを作成する



これらのロールは、次のいずれかを使用して作成できます。

- ONTAP システムマネージャ 9.8P1 以降

["ユーザロールと権限を設定"](#)

- RBAC User Creator for ONTAP ツール (ONTAP 9.6 以前を使用している場合)

- ONTAP を使用して、ロールが割り当てられ、適切なアプリケーションが設定されたユーザを作成します

作成したストレージシステムクレデンシャルは、VSC 用にストレージシステムを構成する際に必要になります。VSC 用のストレージシステムを構成するには、VSC でクレデンシャルを入力する必要があります。これらのクレデンシャルを使用してストレージシステムにログインすると、クレデンシャルの作成時に ONTAP で設定した VSC 機能に対する権限が付与されます。

- VSC にストレージシステムを追加し、作成したユーザのクレデンシャルを指定します

### VSC ロール

VSC では、ONTAP の権限を以下に示す VSC ロールに分類します。

- 検出

接続されているすべてのストレージコントローラを検出できます

- ストレージを作成します

ボリュームおよび論理ユニット番号 (LUN) を作成できます

- ストレージを変更します

ストレージシステムのサイズ変更と重複排除を実行できます

- ストレージを破棄します

ボリュームおよび LUN を破棄できます

## VASA Provider ロール

クラスタレベルで作成できるのは Policy Based Management のみです。ストレージ機能プロファイルを使用してポリシーベースでストレージを管理できます。

## SRA ロール

SRA では、ONTAP 権限をクラスタレベルまたは SVM レベルで SAN または NAS ロールに分類します。これにより、ユーザは SRM 処理を実行できるようになります。

VSC にクラスタを追加する場合は、ONTAP RBAC ロールの権限の初期検証が実行されます。直接接続の SVM のストレージ IP を追加した場合、初期検証は実行されません。タスクワークフローの段階で権限が確認されて適用されます。

# ONTAP ツールのハイアベイラビリティを設定する

ONTAP ツールは、障害時に ONTAP ツールの機能を中断させないためのハイアベイラビリティ（HA）構成をサポートしています。

ONTAP ツールは、VMware vSphere のハイアベイラビリティ（HA）機能とフォールトトレランス（FT）機能を活用することで高可用性を実現します。ハイアベイラビリティ（HA）解決策は、以下のような理由で発生するシステム停止からの迅速なリカバリを可能にします。

- ホスト障害です
- ネットワーク障害
- 仮想マシンの障害（ゲスト OS の障害）
- アプリケーション（ONTAP ツール）がクラッシュする

高可用性を実現するために ONTAP ツールを使用する場合、追加の設定は必要ありません。要件に応じて、vCenter Server ホストと ESXi ホストで VMware vSphere HA または vSphere FT を設定する必要があります。HA と FT のどちらにも、クラスタホストと共有ストレージが必要です。FT には追加の要件と制限事項があります。

VMware vSphere HA 解決策および vSphere FT 解決策に加え、ONTAP ツールを使用することで、ONTAP Tools のサービスを常時実行できます。ONTAP ツールの watchdog プロセスが 3 つのサービスをすべて定期的に監視し、何らかの障害を検出するとサービスを自動的に再起動します。これにより、アプリケーションの障害を防止できます。



vCenter HA は、ONTAP ツールではサポートされていません。



## VMware vSphere HA の場合

VMware vSphere 用の ONTAP ツールを導入した vSphere 環境をハイアベイラビリティ（HA）構成にすることができます。VMware HA は、仮想環境でハードウェアやオペレーティングシステムの障害が発生した場合にフェイルオーバー保護を提供します。

仮想マシンを監視してオペレーティングシステムの障害やハードウェアの障害を検出し、リソースプール内の他の物理サーバ上の仮想マシンを再起動します。サーバの障害が検出された場合、手動での対応は不要です。

VMware HA を設定する手順は、vCenter Server のバージョンによって異なります。VMware HA の設定手順を確認するには、次の参照先で必要な vCenter Server のバージョンを選択してください。

["VMware vSphere のドキュメント：「vSphere HA クラスタの作成と使用」](#)

## VMware vSphere フォールトトレランス

VMware vSphere フォールトトレランス（FT）機能を使用すると、高度なハイアベイラビリティ（HA）を実現し、データや接続が失われないよう仮想マシンを保護することができます。vSphere FT for ONTAP ツールは vCenter Server から有効または無効にする必要があります。

環境内の ONTAP ツールに必要な数の vCPU（少なくとも 2 個、大規模環境の場合は 4 個）と FT が vSphere ライセンスでサポートされていることを確認してください。

vSphere FT を使用すると、サーバの障害時にも仮想マシンを継続的に稼働できます。仮想マシンで vSphere FT が有効になっている場合は、Distributed Resource Scheduler（DRS）で選択された別のホスト（セカンダリ仮想マシン）にプライマリ仮想マシンのコピーが自動的に作成されます。DRS が有効になっていない場合は、使用可能なホストの中からターゲットホストが選択されます。vSphere FT では、プライマリ仮想マシンとセカンダリ仮想マシンをロックステップモードで運用し、それぞれの仮想マシンの実行状態をセカンダリ仮想マシンにミラーリングします。

ハードウェアに障害が発生してプライマリ仮想マシンに障害が発生すると、セカンダリ仮想マシンはプライマリ仮想マシンが停止した場所をすぐに検出します。ネットワーク接続、トランザクション、データが失われることなく、セカンダリ仮想マシンの実行が継続されます。

vCenter Server インスタンスで vSphere FT を設定するには、システムが CPU 要件、仮想マシンの制限要件、およびライセンス要件を満たしている必要があります。

HA を設定する手順は、vCenter Server のバージョンによって異なります。HA の設定手順を確認するには、次の参照先で必要な vCenter Server のバージョンを選択してください。

["VMware vSphere のドキュメント：「Fault Tolerance の要件、制限、およびライセンス」](#)

## ONTAP ツールでサポートされる MetroCluster 構成

VMware vSphere 用の ONTAP ツールでは、ONTAP の MetroCluster IP 構成と FC 構成を使用する環境がサポートされます。このサポートはほぼ自動的に行われます。ただし、MetroCluster 環境で VSC および VASA Provider を使用している場合はいくつかの違いがあります。



SRA では、MetroCluster 構成がサポートされません。



## MetroCluster 構成と VSC

プライマリサイトとセカンダリサイトで VSC がストレージシステムコントローラを検出することを確認する必要があります。通常、VSC は自動的にストレージコントローラを検出します。クラスタ管理 LIF を使用している場合は、VSC が両方のサイトでクラスタを検出していることを確認することを推奨します。検出されていない場合は、手動でストレージコントローラを VSC に追加できます。VSC がストレージコントローラへの接続に使用するユーザ名とパスワードのペアを変更することもできます。

スイッチオーバーが発生した場合、セカンダリサイトの SVM がテイクオーバーします。これらの SVM には、名前に「-mc」というサフィックスがつけられています。データストアのプロビジョニングなどの処理の実行中にスイッチオーバー処理が発生すると、データストアが存在する SVM の名前が「-mc」サフィックスのついたものになります。スイッチバックが発生してプライマリサイトの SVM に制御が戻ると、このサフィックスは削除されます。



MetroCluster 構成の直接接続 SVM を VSC に追加した場合は、スイッチオーバー後に SVM 名の変更（「-mc」サフィックスの追加）が反映されません。他のスイッチオーバー操作は、いずれも引き続き通常どおりに実行されます。

スイッチオーバーまたはスイッチバック後、VSC で自動的にクラスタが検出されて認識されるまでに数分かかる場合があります。データストアのプロビジョニングなどの VSC 処理を実行中にスイッチオーバーまたはスイッチバックが発生した場合、処理に遅れが生じることがあります。

## MetroCluster 構成と VASA Provider

VASA Provider では、MetroCluster 構成を使用する環境が自動的にサポートされます。VASA Provider 環境では、スイッチオーバーは透過的に行われます。直接接続 SVM を VASA Provider に追加することはできません。



VASA Provider では、スイッチオーバーの実行後にセカンダリサイトの SVM の名前に「-mc」というサフィックスが付加されません。

## 著作権に関する情報

Copyright © 2024 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。