



VMware vSphere ドキュメント用の ONTAP ツール

ONTAP tools for VMware vSphere 10.0

NetApp
October 23, 2024

目次

VMware vSphere ドキュメント用の ONTAP ツール	1
リリースノート	2
概念	3
ONTAP ツールの概要	3
VVOL 向けの VASA Provider の設定	3
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	7
AutoSupport	8
ONTAP ツールを導入	9
VMware vSphere クイックスタート用の ONTAP ツール	9
ONTAP ツールを導入するための要件	10
ONTAP ツールのダウンロード方法	12
導入チェックリスト	12
ONTAP toolsの導入準備	14
非HAシングルノード構成の導入方法	15
HA 3ノード構成の導入方法	18
ONTAP ツールを設定する	22
ネットワークアクセスの管理	22
ユーザロールと権限を設定	22
ONTAP Tools Managerユーザインターフェイス	25
vCenterの追加	26
ストレージバックエンドの追加	27
ストレージバックエンドとvCenterの関連付け	27
vCenterを使用したオンボードストレージバックエンド (SVMまたはクラスタ)	28
VASA ProviderをvCenterに登録	28
vVolデータストアの作成	29
登録したSVMの確認	32
ONTAP ツールを管理します	33
データストアを管理します	33
ストレージバックエンドの管理	37
vCenterの管理	38
VVolライフサイクルの管理	40
管理対象のigroupとエクスポートポリシー	40
ONTAP ツールのメンテナンスコンソールにアクセスします	41
ログファイルを収集します	44
検出	44
ONTAPツールの移行	46
最新リリースのONTAP toolsに移行する	46
法的通知	49

著作権	49
商標	49
特許	49
プライバシーポリシー	49
オープンソース	49

VMware vSphere ドキュメント用の ONTAP ツール

リリースノート

解決済みの問題、既知の問題、注意事項、および制限事項など、VMware vSphere 用のこのリリースの ONTAP ツールに関する重要な情報を提供します。

詳細については、を参照してください ["ONTAP Tools for VMware vSphere 10.0リリースノート"](#)。

概念

ONTAP ツールの概要

ONTAP Tools for VMware vSphereは、NetAppストレージバックエンドを使用するVMware環境でのデータストアと仮想マシンのプロビジョニングを管理します。管理者は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易化されます。

ONTAP Tools for VMware vSphere 10.0リリースは、水平方向に拡張可能なイベントベースのOpen Virtual Appliance (OVA; オープン仮想アプライアンス) として導入されたマイクロサービス。オンプレミス向けのOpen Virtual Appliance (OVA; オープン仮想アプライアンス) やSoftware as a Service (SaaS) など、さまざまな導入フォームファクタでパッケージ化されています。

ONTAP Tools for VMware vSphereは次のコンポーネントで構成されています。

- 仮想マシンの機能
- VM単位のVASAプロバイダ
- ポリシーベースのストレージ管理

ONTAP Tools VASA Provider

ONTAP tools VASA Providerは、仮想ボリューム (VVOL) の拡張性に関する高度な要件をサポートしています。NFSプロトコル、iSCSIプロトコル、OVA環境をサポートしています。

VASA Provider for VMwareは、ONTAPを使用したVMware環境でライフサイクル管理を提供する製品です。

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データストアにストレージを追加したり、vVolデータストアからストレージを削除したりすることで、柔軟性を高めることができます。

vVolデータストアは、ストレージコンテナ (元のストレージとも呼ばれます) に含まれる1つ以上のFlexVol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またはiSCSI) および同じStorage Virtual Machine (SVM) を使用する必要があります。



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。多様なボリュームを追加すると、シンボリックボリュームとシックボリュームが混在している場合にデータストアの機能が向上し、両方の種類のVMをデータストアに作成できるようになります。

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。
vCenter 8では、シンプロビジョニングで256GBのLUNに容量を割り当てます。

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。

- * 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。

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。vCenter Serverは、ロールと権限を持つユーザ権限とグループ権限を使用して、インベントリ内のさまざまなレベルで一元的な認証および許可サービスを提供します。vCenter Serverには、RBACを管理するための5つの主要コンポーネントがあります。

コンポーネント	説明
---------	----

権限	vSphereで操作を実行するためのアクセスを有効または拒否します。
ロール	ロールには、1つ以上のシステム権限が含まれています。各権限は、システム内の特定のオブジェクトまたはタイプのオブジェクトに対する管理権限を定義します。ユーザにロールを割り当てると、そのロールで定義されている権限の機能が継承されます。
ユーザとグループ	ユーザとグループは、Active Directory (AD) または潜在的にローカルのWindowsユーザ/グループからロールを割り当てる権限に使用される（推奨されません）
権限	権限を使用すると、ユーザまたはグループに権限を割り当てて、特定の操作を実行し、vCenter Server内のオブジェクトに変更を加えることができます。vCenter Serverアクセス許可は、ESXiホストに直接ログインするユーザではなく、vCenter Serverにログインするユーザにのみ影響します。
オブジェクト	アクションが実行されるエンティティ。VMware vCenterオブジェクトは、データセンター、フォルダ、リソースプール、クラスタ、ホスト、およびVM

タスクを完了するには、適切なvCenter Server RBACロールが必要です。タスクの実行中、ONTAP toolsはユーザのvCenter Serverロールを確認してから、ユーザのONTAP権限を確認します。



vCenter Serverのロールは、管理者ではなく、ONTAP toolsのvCenterユーザに適用されます。デフォルトでは、管理者は製品へのフルアクセス権を持ち、ロールを割り当てる必要はありません。

ユーザとグループは、vCenter Serverロールに含まれることでロールにアクセスできます。

vCenter Serverのロールの割り当てと変更に関するキーポイント

vCenter Serverのロールは、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。

ロールを割り当てる場所によって、ユーザが実行できるONTAP toolsタスクが決まります。一度に1つのロールを変更できます。

ロール内の権限を変更した場合、そのロールに関連付けられているユーザは、更新されたロールを有効にするために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 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、ONTAP toolsには、ONTAP toolsの主要なタスクを実行できる標準のONTAP toolsロールが用意されています。タスクを実行せずに情報を表示できる読み取り専用ロールもあります。

ONTAP toolsの標準ロールを表示するには、vSphere Clientの[ホーム]ページで*[ロール]*をクリックします。ONTAP toolsのロールで実行できるタスクは次のとおりです。

* 役割 *	* 概要 *
NetApp ONTAPツール管理者	ONTAP toolsの一部のタスクを実行するために必要なvCenter Server標準の権限とONTAP tools固有の権限がすべて含まれています。
NetApp ONTAP tools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。これらのユーザは、アクセス制御されたONTAP toolsアクションを実行できません。
NetApp ONTAPツールプロビジョニング	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。 <ul style="list-style-type: none"> • 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

Manager UI管理者ロールがvCenterに登録されていません。このロールはマネージャUIに固有です。

標準のONTAP toolsロールよりも制限の厳しいロールを実装する必要がある場合は、ONTAP toolsロールを使用して新しいロールを作成できます。

この場合は、必要なONTAP toolsロールのクローンを作成し、そのクローンロールを編集してユーザに必要な権限のみを付与します。

ONTAPストレージバックエンドとvSphereオブジェクトの権限

十分なvCenter Serverアクセス許可がある場合、ONTAP toolsは次に、ストレージバックエンドのクレデンシャル（ユーザ名とパスワード）に関連付けられているONTAP RBAC権限（ONTAPロール）を確認します。そのストレージバックエンドでONTAP toolsタスクに必要なストレージ処理を実行するための十分な権限があるかどうかを確認する。適切なONTAP権限があれば、ストレージバックエンドを使用し、ONTAP toolsタスクを実行します。ストレージバックエンドで実行できるONTAP toolsタスクは、ONTAPロールによって決まります。

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、ONTAP tools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。ONTAP System Manager 9.8P1以降を使用してONTAP ロールを作成できます。を参照してください

["管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト"](#) を参照してください。

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、ONTAP tools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、ONTAP toolsの最も基本的なストレージ処理に関連する権限だけが含まれます。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。

ONTAP toolsを使用する際に推奨されるONTAP RBACロールの一部を次に示します。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。

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



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。



vCenter HA は、ONTAP ツールではサポートされていません。

AutoSupport

AutoSupport は、システムヘルスをプロアクティブに監視し、ネットアップテクニカルサポート、社内のサポート部門、およびサポートパートナーにメッセージを自動的に送信します。

AutoSupport は、ストレージシステムの初回設定時にデフォルトで有効になります。AutoSupport は、AutoSupport が有効になってから 24 時間後にテクニカルサポートへのメッセージ送信を開始します。

AutoSupport を有効または無効にできるのは導入時のみです。有効のままにしておくことをお勧めします。AutoSupport を有効にしておくことで、ストレージ・システムに問題が発生したときに、迅速に原因を判断し解決できます。デフォルトでは、AutoSupport を無効にした場合でも、AutoSupport の情報が収集されてローカルに格納されます。

送信を成功させるには、ネットワークで 216.240.21.18 // support.netapp.com URL をホワイトリストに登録する必要があります。

ONTAP ツールを導入

VMware vSphere クイックスタート用の ONTAP ツール

ONTAP Tools for VMware vSphereはvCenter Serverプラグインで、ONTAPツールとVASA Provider拡張機能が含まれています。ベストプラクティスに基づいてESXiホストの設定とONTAPストレージのプロビジョニングが行われるため、すべてのONTAP vSphere環境でONTAPツールを使用することを推奨します。VASA Providerは、仮想ボリューム (VVOL) をサポートするために必要です。

設置を準備しています

このプラグインを仮想アプライアンスとして導入することで、各製品を別々にインストールして vCenter Server に登録する手間を減らすことができます。

導入の要件

ONTAP tools for VMware vSphereを導入する前に、導入パッケージのスペース要件とホストシステムのいくつかの基本的な要件を理解しておく必要があります。

ONTAPツールは、Windows vCenter ServerまたはVMware vCenter Server VirtualAppliance (vCSA) で使用できます。ESXiシステムを含むサポートされているvSphereにONTAP toolsを導入する必要があります。

- ノードあたりのインストールパッケージのスペース要件
 - シンプロビジョニング環境の場合は10GB
 - シックプロビジョニングの場合は200GB
- ノードあたりのホストシステムのサイジング要件
次の表に、導入サイズおよびノードごとの推奨メモリを示します。

導入のタイプ	CPU	メモリ (GB)
小 (S)	8	16
中 (M)	12	24
大 (L)	16	32だ

ストレージとアプリケーションの最小要件：

ストレージ、ホスト、およびアプリケーション	バージョン要件
ONTAP	ONTAP 9.10.1、9.11、9.12、9.13
VMware vSphere の場合	サポートされるVMwareの最小バージョンは7.0.3です。
ESXiホスト	ESXi 7.0.3以降のバージョン
vCenterサーバ	vCenter 7.0.3

ストレージ、ホスト、およびアプリケーション	バージョン要件
VASA Provider	3.0
OVAアプリケーション	10.0

詳細については、を参照してください "[ONTAP ツールを導入するための要件](#)"

ONTAP ツールの要件

- vCenter Server 環境を設定およびセットアップします。
- .ova ファイルをダウンロードします。
- vCenter Server インスタンスのログインクレデンシアルを用意します。
- ブラウザキャッシュを削除して、ONTAP ツールの導入時にブラウザキャッシュの問題が発生しないようにします。
- 仮想アプライアンスが ICMP ping に応答するために使用するデフォルトゲートウェイを設定します。
- 仮想アプライアンスの有効な DNS ホスト名。

ONTAP ツールの導入

手順

1. ダウンロード .zip のバイナリと署名済み証明書を含むファイル "[NetApp Support Site](#)" から vSphere Client システムにアップロードして、ONTAP ツールを導入できます。
2. を展開します .zip ファイルを作成してを導入します .ova ファイル。
3. vSphereサーバにログインします。
4. OVAを導入するリソースプールまたはホストに移動します。
5. 目的のデータセンターを右クリックし、*[Deploy OVF template...]*を選択します。
6. .ovaファイルのURLを入力するか、.ovaファイルが保存されているフォルダを参照して、*[次へ]*を選択します。
7. 必要な詳細を入力して導入を完了します。

導入の進捗状況は[Tasks]タブで確認でき、導入が完了するまで待ちます。

ONTAP ツールを導入するための要件

VMware vSphere 用の ONTAP ツールを導入する前に、導入パッケージのスペース要件とホストシステムのいくつかの基本的な要件について理解しておく必要があります。

ONTAPツールは、Windows vCenter ServerまたはVMware vCenter Server Virtual Appliance (vCSA) で使用できます。ESXiシステムを含むサポートされているvSphereにONTAP toolsを導入する必要があります。

- ノードあたりのインストールパッケージのスペース要件
 - シンプロビジョニング環境の場合は10GB
 - シックプロビジョニングの場合は200GB

- ノードあたりのホストシステムのサイジング要件
次の表に、導入サイズおよびノードごとの推奨メモリを示します。

導入のタイプ	CPU	メモリ (GB)
小 (S)	8	16
中 (M)	12	24
大 (L)	16	32だ

ストレージとアプリケーションの最小要件：

ストレージ、ホスト、およびアプリケーション	バージョン要件
ONTAP	ONTAP 9.10.1、9.11、9.12、9.13
VMware vSphere の場合	サポートされるVMwareの最小バージョンは7.0.3です。
ESXiホスト	ESXi 7.0.3以降のバージョン
vCenterサーバ	vCenter 7.0.3
VASA Provider	3.0
OVAアプリケーション	10.0

サポートされるONTAP、vCenter Server、ESXiホスト、およびプラグインアプリケーションのバージョンの最新情報については、Interoperability Matrix Tool (IMT) を参照してください。

["Interoperability Matrix Tool で確認してください"](#)

導入に関するその他の考慮事項

導入 ONTAP ツールをカスタマイズするときは、いくつかの要件について考慮する必要があります。

アプリケーションユーザのパスワード

管理者アカウントに割り当てられたパスワードです。セキュリティ上の理由から、パスワードの長さは8~30文字にすることを推奨します。パスワードには、最低1文字の上部、下部、1文字の数字、および特殊文字を使用します。パスワードは90日後に期限切れになります。

アプライアンスのメンテナンスコンソールのクレデンシャル

メンテナンスコンソールにアクセスするには、「maint」ユーザ名を使用する必要があります。導入時に「maint」ユーザのパスワードを設定できます。パスワードを変更するには、ONTAP ツールのメンテナンスコンソールの [アプリケーションの設定] メニューを使用します。

vCenter Server の IP アドレス

- ONTAP toolsの登録先のvCenter ServerインスタンスのIPアドレス (IPv4) を指定する必要があります。

生成されるONTAP toolsとVASA証明書のタイプは、導入時に指定したIPアドレス (IPv4) によって異なります。

- vCenter Serverへの登録に使用するONTAP toolsのIPアドレスは、導入ウィザードで入力したvCenter ServerのIPアドレスのタイプ (IPv4) によって異なります。

ONTAPツールとVASA証明書は、vCenter Serverの登録時に使用したものと同一タイプのIPアドレスを使用して生成されます。

- インストール中にVMが移行されていないことを確認します。



ONTAP tools for VMware vSphere 10.0リリースでは、IPv6はサポートされません。

アプライアンスのネットワーク・プロパティ

ONTAP toolsの有効なDNSホスト名 (非修飾) と静的IPアドレス、およびその他のネットワークパラメータを指定します。ONTAP tools for VMware vSphere 10.0リリースでは、DHCPはサポートされません。これらのパラメータはすべて、適切なインストールと運用のために必要です。

ONTAP ツールのダウンロード方法

はダウンロードできます .zip のONTAP tools for VMware vSphereのバイナリ (.ova) と署名済み証明書を含むファイル "[NetApp Support Site](#)"。

コンテンツライブラリ

ova ファイルには **ONTAP** ツールが含まれています。導入が完了すると、**ONTAP**ツールと**VASA**製品が環境にインストールされます。デフォルトでは、後続の導入モデルを決定し、要件に基づいて**VASA Provider**を有効にするかどうかを選択すると、すぐに**ONTAP tools**が機能し始めます。

VMwareのコンテンツライブラリは、VMテンプレート、vAppテンプレート、およびその他の種類のファイルを格納するコンテナオブジェクトです。コンテンツライブラリを使用した展開では、ネットワーク接続に依存しないシームレスなエクスペリエンスが提供されます。

OVAをHA構成に導入する前に、コンテンツライブラリを作成してOVAを格納する必要があります。コンテンツライブラリのセキュリティポリシーを選択したり、パスワードを設定したりしないでください。

次の手順に従ってコンテンツライブラリを作成します。

- 手順 *
 1. vSphere Clientにログインします。
 2. vSphere Clientの横の省略記号を選択し、*[Content library]*を選択します。
 3. ページの右側にある*[作成]*ボタンを選択します。
 4. ライブラリの名前を指定し、コンテンツライブラリを作成します。

導入チェックリスト

このチェックリストは、導入を開始する前にすべての情報を確認するのに役立ちます。を導入する前に、これらの設定値をメモしておいてください。

ONTAP tools for VMware vSphereの導入を開始する前に、ストレージバックエンドの基本要件、アプリケーション要件、およびライセンス要件を確認しておく必要があります。

VMware vSphere 用の ONTAP ツールを導入する前に、導入計画を作成し、環境で ONTAP ツールをどのように設定するかを決めておくことを推奨します。

最初のノードとその他の共通フィールド

- VASA Providerのユーザ名 (*)
- 管理者ユーザ名 (*)
- NTPサーバ (時刻同期のためにvCenterに提供)

証明書の詳細

- カスタムCA証明書を有効にする
- ルート証明書と中間証明書 (自己署名が有効な場合は無視)
- リーフ証明書と秘密鍵 (自己署名が有効な場合は無視されます)
- ドメイン名 (*) (自己署名が有効な場合は無視)

ロードバランサとAPIサーバの詳細

- ロードバランサIP (*)
- Kubernetesコントロールプレーンの仮想IP (*)
- ONTAPの詳細*
- ONTAP管理LIF (*) (クラスタ管理IP)
- ONTAPデータLIF (*)
- Storage VM (*)
- ONTAPクラスタユーザ名 (*)
- 移行を有効にする
- プライマリVM
- コンテンツライブラリ名 (*)
- OVFテンプレート名 (*)
- ホスト名 (*)
- ユーザ名 (*)

最初のノードネットワークの詳細

- ホスト名 (*)
- IPアドレス (*)
- プレフィックス長 (IPv6の場合のみ)
- ネットマスク (IPv4のみ) (*)
- ゲートウェイ (*)
- プライマリDNS (*)

- セカンダリDNS (*)
- 検索ドメイン (*)
- 2番目のノード-ノードネットワークの詳細*
- ホスト名 (*)
- IPアドレス (*)

第3ノード-ノードネットワークの詳細

- ホスト名 (*)
- IPアドレス (*)

ONTAP toolsの導入準備

ONTAP Tools for VMware vSphereは、VASA Providerを含む複数のvCenter Serverをサポートします。

ONTAP tools for VMware vSphereの導入を開始する前に、ストレージバックエンドの基本要件、アプリケーション要件、およびライセンス要件を確認しておく必要があります。VMware vSphere用のONTAPツールを導入する前に、導入計画を作成し、環境でONTAPツールをどのように設定するかを決めておくことを推奨します。

導入の準備

導入を進める前のONTAP toolsの要件を次に示します。

- vCenter Server環境を設定およびセットアップします。
- `_ova_` ファイルをダウンロードします。
- OVAを導入するホストまたはリソースプールに、* ONTAP toolsの導入要件*に記載されている最小限のリソースがあることを確認してください。
- ブラウザキャッシュを削除します。
- ロードバランサとKubernetes APIサーバ用に2つの仮想IPが必要です。導入に使用するVLANで2つの無料IPを取得します。このIPは導入後にサービスにアクセスするために使用されます。
- CA証明書（ルート証明書、リーフ証明書、中間証明書）を商用CAから取得します。
- カスタムCA証明書が必須であるvCenterを複数導入する場合は、証明書が発行される*ドメイン名*を*仮想IP*にマッピングします。ドメイン名に対してpingチェックを実行し、ドメインが目的のIPに解決されているかどうかを確認します。
- NFSを有効にしたONTAP上のStorage VMが必要です。Storage VMを設定するには、次の手順を実行します。
 - ONTAPシステムマネージャとONTAP CLIの両方を開いておきます。
 - 新しいStorage VMを作成する場合は、ONTAP System Managerにログインし、NFSを有効にしてStorage VMを作成してください。
 - 100GB以上のアグリゲートを追加してください。

- アグリゲートが正常に追加されたかどうかを確認します。

a) ONTAP CLIへのログイン

b) コマンド `vserver show -fields aggr-list` を実行します。

c) デフォルトのStorage VMにアグリゲートが表示されていない場合は、次のコマンドを実行します。
`vserver modify < storage VM name >-aggr-list <aggregate name>`

デフォルトのStorage VMに追加するアグリゲートの名前を確認するには、ONTAP CLIで次のコマンドを使用します。*aggr show*

このコマンドを実行すると、ストレージシステム上のアグリゲートのリストが表示され、使用する必要があるアグリゲートの名前が* Aggregate *列に表示されます。

- 導入設定には、クラスタのクレデンシャルとSVMのクレデンシャルまたは直接接続のSVMの2つのオプションがあります。直接接続型SVMの場合は、導入を開始する前に、SVM用の管理LIFを設定する必要があります。クラスタクレデンシャルの場合はスキップしてください。
- ネットワークルートが存在することを確認し、ONTAP CLIにログインして `network route show -vserver <storage VM name>` コマンドを実行します。

存在しない場合は、ONTAP CLIにログインして次のコマンドを実行します。`net route create -vserver <vserver name>-destination <destination IP>-gateway <gateway IP>-metric 20`

- Storage VMのエクスポートポリシーが存在することを確認してください。ONTAPシステムマネージャで、[ストレージ]>*>[ストレージVM名]>[設定]>[エクスポートポリシー]*の順に選択します。エクスポートポリシーがない場合は、次の手順を実行します。
- ONTAP CLIで次のコマンドを使用してエクスポートポリシールールを作成する

`vserver export-policy rule create -vserver <storage VM name>-policyname <export policy name>-clientmatch <ESXI-IP>-rorule any -rwrule any -superuser any`



`_superuser_value`がNOT_NONEでないことを確認してください。

非HAシングルノード構成の導入方法

非HAシングルノードは、小規模、中規模、大規模のいずれかの構成で構成できます。

- 小規模の非HA構成には、8個のCPUと16GBのRAMが搭載されています。
- 中規模の非HA構成には、12個のCPUと24GBのRAMが搭載されています。
- 大規模な非HA構成には、16個のCPUと32GBのRAMが搭載されています。

ネットワークルートが存在することを確認します。

例：`c1_sti67 -vsim -ucs154k_1679633108 : : : > network route create -vserver <SVM>-destination 0.0.0.0/0 -gateway <gateway_ip>`

- このタスクについて *

このタスクでは、小規模、中規模、または高可用性構成に非HAシングルノードをインストールする手順を説

明します。

• 手順 *

1. vSphereサーバにログインします。
2. OVAを導入するリソースプールまたはホストに移動します。
3. 目的のデータセンターを右クリックし、*[Deploy OVF template...]*を選択します。
4. `.ova_file`のURLを入力するか、または`.ova_file`が保存されているフォルダを参照して、*[Next]*を選択します。
5. 仮想マシンの名前とフォルダを選択し、*[Next]*を選択します。
6. ホストを選択して*[次へ]*を選択します。
7. テンプレートの概要を確認し、* Next *を選択します。
8. ライセンス契約を読んで同意し、* Next *を選択します。
9. で、*非HAシングルノード（小規模）、非HAシングルノード（中規模）、または*非HAシングルノード（大規模）*構成を選択します。
10. [設定]ウィンドウで、必要な非HAシングルノード構成のサイズを選択し、*[次へ]*を選択します。
11. OVAを導入するデータストアを選択し、*[次へ]*を選択します。
12. ソースとデスティネーションのネットワークを選択し、*[次へ]*を選択します。
13. >[システム構成]*ウィンドウを選択します。次の詳細を入力します。
 - a. VASA Providerのユーザ名とパスワード：このユーザ名とパスワードは、VASA ProviderをvCenterに登録する際に使用されます。
 - b. [Enable ASUP]*チェックボックスはデフォルトで選択されています。

ASUPを有効または無効にできるのは導入時のみです。
 - c. 管理者ユーザ名と管理者パスワード：* ONTAPツールマネージャ* UIへのログインに使用するパスワードです。
 - d. NTPサーバ情報を*[NTP Servers]*フィールドに入力します。
 - e. メンテナンスユーザのパスワード：「メンテナンスコンソールオプション」へのアクセスを許可するために使用します。
14. [テンプレートのカスタマイズ]*>[VASA Provider証明書]*ウィンドウで、次の詳細を入力します。
 - a. Enable Custom CA certificateチェックボックスをオンにします。これは、マルチVCをイネーブルにするために必要です。マルチVC環境以外の場合は、このチェックボックスを無視します。証明書とドメイン名を指定する必要はなく、仮想IPの詳細だけを指定する必要があります。
 - b. ルート証明書と中間証明書をコピーして貼り付けます。
 - c. リーフ証明書と秘密鍵をコピーして貼り付けます。
 - d. 証明書の生成に使用したドメイン名を入力します。
 - e. ロードバランスIPの詳細を入力します。
15. [Customize template]*>*[Deployment Configuration *]*ウィンドウで、次の詳細情報を入力します。
 - a. [Virtual IP for K8s Control Plane]に空いているIPアドレスを入力します。これはKubernetes APIサーバに必要です。

- b. 直接接続型SVMを使用する場合は、*[SVMスコープを有効にする]*オプションのチェックボックスをオンにします。ONTAPクラスタを使用する場合は、このチェックボックスをオフにします。



SVMスコープを有効にした場合は、管理IPでのSVMサポートをすでに有効にしておく必要があります。

- c. 次の図に示す詳細を入力します。

Enable SVM scoping	Ignore when cluster scoping is required <input type="checkbox"/>
ONTAP/SVM Management LIF(*)	Specify the Management LIF for trident _____ ⓘ
ONTAP/SVM Data LIF(*)	Specify the Data LIF for trident _____ ⓘ
Storage VM	Specify the storage VM Name _____ Ignored when SVM scop_____
ONTAP/SVM Username(*)	Specify the OnTap Cluster Username _____ ⓘ
ONTAP/SVM Password(*)	Specify the OnTap Cluster Password Password _____ ⓘ Enter a password to enable authentication.

- d. [ONTAP / SVM管理LIF]*で、ONTAPクラスタまたはSVM管理IPを入力します。
- e. ONTAPクラスタまたはSVM * ONTAP/SVMデータLIF *を入力します。
- f. Storage VMの場合、ONTAPのデフォルトのStorage VMの詳細を指定するか、新しいStorage VMを作成するかを選択できます。[SVMスコープを有効にする]を選択した場合は、*[Storage VM]*フィールドに値を入力しないでください。このフィールドは無視されます。
- g. [ONTAP / SVMユーザ名]を入力します。
- h. ONTAP / SVMのパスワードを入力します。
- i. Enable Migrationはデフォルトで無効になっています。この選択は変更しないでください。
- j. プライマリVMはデフォルトで有効になっています。この選択は変更しないでください。
16. >[Node Configuration]*ウィンドウで、OVAのネットワークプロパティを入力します。



ここで提供された情報は、インストールプロセス中に適切なパターンについて検証されます。不一致がある場合は、Webコンソールにエラーメッセージが表示され、入力した誤った情報を修正するように求められます。

- a. ホスト名を入力します。
- b. ホスト名にマッピングされたIPアドレスを入力します。
- c. プレフィックス長 (IPv6の場合のみ)

- d. ネットマスク (IPv4の場合のみ)
 - e. ゲートウェイ
 - f. プライマリDNS
 - g. セカンダリDNS
 - h. 検索ドメイン
17. [選択内容の確認]ウィンドウで詳細を確認し、*[完了]*を選択します。
- タスクが作成されると、vSphereタスクバーに進捗状況が表示されます。
18. タスクが完了したら、VMの電源をオンにします。
- インストールが開始されます。インストールの進行状況は、VMのWebコンソールで追跡できます。インストールの一環として、ノードの設定が検証されます。OVFフォームの*カスタマイズテンプレート*の各セクションで提供される入力内容が検証されます。不一致がある場合は、修正措置を講じるように求めるダイアログが表示されます。
19. ダイアログプロンプトで必要な変更を行うには、次の手順に従います。
- a. Webコンソールをダブルクリックして、コンソールの操作を開始します。
 - b. キーボードの上矢印キーと下矢印キーを使用して、表示されているフィールド間を移動します。
 - c. キーボードの右矢印キーと左矢印キーを使用して、フィールドに指定された値の右端または左端に移動します。
 - d. Tabキーを使用してパネル内を移動し、* OK *または*キャンセル*の値を入力します。
 - e. ENTERを使用して、* OK または CANCEL *のいずれかを選択します。
20. [OK]*または[キャンセル]*を選択すると、指定した値が再度検証されます。値を3回修正するためのプロビジョニングがあります。3回以内に修正しなかった場合は、製品のインストールが停止し、新しいVMでインストールを試すことをお勧めします。
21. インストールが完了すると、WebコンソールにONTAP tools for VMware vSphereが正常な状態にあることを示すメッセージが表示されます。

HA 3ノード構成の導入方法

HA 3ノードは、小規模、中規模、大規模のいずれかの構成で構成できます。

- 小規模なHA 3ノード：各ノードに8個のCPUと16GBのRAMを搭載。
- 中規模HA (3ノード) 各ノードに12個のCPUと24GBのRAMが搭載されています。
- 大規模なHA 3ノードには、各ノードに16個のCPUと32GBのRAMが搭載されています。
- このタスクについて *

このタスクでは、小規模、中規模、または高可用性の構成にHA 3ノードを設置する手順を説明します。



コンテンツライブラリの作成は、HA 3ノード構成を導入するための必須の手順です。を参照してください ["ONTAP ツールのダウンロード方法"](#) を参照してください。



導入を進める前に、ONTAPツールのインストール中に、インベントリ上のクラスタのDistributed Resource Scheduler (DRS) を* conservative *に設定します。

• 手順 *

1. vSphereサーバにログインします。
2. コンテンツライブラリに移動し、コンテンツライブラリを選択します。
3. ページ右側の*を選択し、[Import item]*を選択してOVAファイルをインポートします。
4. OVAを導入するリソースプールまたはホストに移動します。
5. 目的のデータセンターを右クリックし、*[Deploy OVF template...]*を選択します。
6. `_ova_file`が保存されているコンテンツライブラリを選択し、*[次へ]*を選択します。
7. 仮想マシンの名前とフォルダを選択し、*[Next]*を選択します。
8. ホストを選択して*[次へ]*を選択します。
9. テンプレートの概要を確認し、* Next *を選択します。
10. ライセンス契約を読んで同意し、* Next *を選択します。
11. で、要件に応じて[HA Three Node (小規模)]、[HA Three Node (中規模)]、または[HA Three Node (大規模)]*構成を選択します。
12. 構成ファイルとディスクファイルのストレージを選択し、* Next *を選択します。
13. 各ソースネットワークのデスティネーションネットワークを選択し、*[Next]*を選択します。
14. >[システム構成]*ウィンドウを選択します。次の詳細を入力します。
 - a. VASA Providerのユーザ名とパスワード：このユーザ名とパスワードは、VASA ProviderをvCenterに登録する際に使用されます。
 - b. [Enable ASUP]*チェックボックスはデフォルトで選択されています。

ASUPを有効または無効にできるのは導入時のみです。
 - c. 管理者のユーザー名と管理者のパスワード：* ONTAP tools Manager* UIへのログインに使用するパスワードです。
 - d. NTPサーバ情報を*[NTP Servers]*フィールドに入力します。
 - e. メンテナンスユーザのパスワード：「メンテナンスコンソールオプション」へのアクセスを許可するために使用します。
15. [テンプレートのカスタマイズ]*>[VASA Provider証明書]*ウィンドウで、次の詳細を入力します。
 - a. Enable Custom CA certificateチェックボックスをオンにします。これは、マルチVCをイネーブルにするために必要です。マルチVC環境以外の場合は、このチェックボックスを無視します。証明書とドメイン名を指定する必要はなく、仮想IPの詳細だけを指定する必要があります。
 - b. ルート証明書と中間証明書をコピーして貼り付けます。
 - c. リーフ証明書と秘密鍵をコピーして貼り付けます。
 - d. 証明書の生成に使用したドメイン名を入力します。
 - e. ロードバランスIPの詳細を入力します。
16. [Customize template]*>*[Deployment Configuration *]*ウィンドウで、次の詳細情報を入力します。

- a. [Virtual IP for K8s Control Plane]に空いているIPアドレスを入力します。これはKubernetes APIサーバに必要です。
- b. 直接接続型SVMを使用する場合は、*[SVMスコープを有効にする]*オプションのチェックボックスをオンにします。ONTAPクラスタを使用する場合は、このチェックボックスをオフにします。



SVMスコープを有効にした場合は、管理IPでのSVMサポートをすでに有効にしておく必要があります。

- c. 次の図に示す詳細を入力します。

Enable SVM scoping	Ignore when cluster scoping is required <input type="checkbox"/>
ONTAP/SVM Management LIF(*)	Specify the Management LIF for trident _____ ⓘ
ONTAP/SVM Data LIF(*)	Specify the Data LIF for trident _____ ⓘ
Storage VM	Specify the storage VM Name Ignored when SVM scop_____
ONTAP/SVM Username(*)	Specify the OnTap Cluster Username _____ ⓘ
ONTAP/SVM Password(*)	Specify the OnTap Cluster Password Password _____ ⓘ Enter a password to enable authentication.

- d. [ONTAP / SVM管理LIF]*で、ONTAPクラスタまたはSVM管理IPを入力します。
- e. ONTAPクラスタまたはSVM * ONTAP/SVMデータLIF *を入力します。
- f. Storage VMの場合、ONTAPのデフォルトのStorage VMの詳細を指定するか、新しいStorage VMを作成するかを選択できます。[SVMスコープを有効にする]を選択した場合は、*[Storage VM]*フィールドに値を入力しないでください。このフィールドは無視されます。
- g. [ONTAP / SVMユーザ名]を入力します。
- h. ONTAP / SVMのパスワードを入力します。
 - i. Enable Migrationはデフォルトで無効になっています。この選択は変更しないでください。
 - j. プライマリVMはデフォルトで有効になっています。この選択は変更しないでください。
17. テンプレートのカスタマイズ>*コンテンツライブラリの詳細*ウィンドウで、コンテンツライブラリ名*と OVFテンプレート名*を入力します。
18. [テンプレートのカスタマイズ]*>[vCenter構成]*ウィンドウで、コンテンツライブラリがホストされているvCenterの詳細を入力します。
19. [テンプレートのカスタマイズ]*>[ノード構成]*ウィンドウで、3つすべてのノードのOVAのネットワークプロパティを入力します。



ここで提供された情報は、インストールプロセス中に適切なパターンについて検証されます。不一致がある場合は、Webコンソールにエラーメッセージが表示され、入力した誤った情報を修正するように求められます。

次の詳細を入力します。

- a. ホスト名。
 - b. ホスト名にマッピングされたIPアドレス。
 - c. プレフィックス長 (IPv6の場合のみ)
 - d. ネットマスク (IPv4の場合のみ)
 - e. ゲートウェイ
 - f. プライマリDNS
 - g. セカンダリDNS
 - h. 検索ドメイン
20. [テンプレートのカスタマイズ (Customize template)]*>[ノード2の構成 (Node 2 Configuration)]*および[ノード3の構成 (Node 3 Configuration)]*ウィンドウで、次の詳細を入力します。
- a. ホスト名
 - b. IP アドレス
21. [選択内容の確認]ウィンドウで詳細を確認し、*[完了]*を選択します。
- タスクが作成されると、vSphereタスクバーに進捗状況が表示されます。
22. タスクが完了したら、VMの電源をオンにします。
- インストールが開始されます。インストールの進行状況は、VMのWebコンソールで追跡できます。インストールの一環として、ノードの設定が検証されます。OVFフォームの*カスタマイズテンプレート*の各セクションで提供される入力内容が検証されます。不一致がある場合は、修正措置を講じるように求めるダイアログが表示されます。
23. ダイアログプロンプトで必要な変更を行うには、次の手順に従います。
- a. Webコンソールをダブルクリックして、コンソールの操作を開始します。
 - b. キーボードの上矢印キーと下矢印キーを使用して、表示されているフィールド間を移動します。
 - c. キーボードの右矢印キーと左矢印キーを使用して、フィールドに指定された値の右端または左端に移動します。
 - d. Tabキーを使用してパネル内を移動し、* OK *または*キャンセル*の値を入力します。
 - e. ENTERを使用して、* OK または CANCEL *のいずれかを選択します。
24. [OK]*または[キャンセル]*を選択すると、指定した値が再度検証されます。値を3回修正するためのプロビジョニングがあります。3回以内に修正しなかった場合は、製品のインストールが停止し、新しいVMでインストールを試すことをお勧めします。
25. インストールが完了すると、WebコンソールにONTAP tools for VMware vSphereが正常な状態にあることを示すメッセージが表示されます。

ONTAP ツールを設定する

ネットワークアクセスの管理

この機能を使用すると、データストアのマウント処理に許可する特定のESXiホストアドレスを指定できます。

ESXiホストに複数のIPアドレスがある場合は、検出されたホストのすべてのIPアドレスがエクスポートポリシーに追加されます。すべてのIPアドレスをエクスポートポリシーに追加しない場合は、ホワイトリストに登録されたIPアドレスを、カンマで区切ったリストまたは範囲またはCIDR、または3つすべての組み合わせでvCenterごとに指定します。

設定を指定しない場合は、マウント前の手順で検出したすべてのIPアドレスがエクスポートポリシーによって追加されます。この設定が指定されている場合、ONTAP toolsはホワイトリストに登録されたIPまたは範囲内のIPのみを追加します。ホワイトリストに登録されたIPにホストのIPが1つも属していない場合、そのホストでのマウントは失敗します。

デフォルトでは、すべてのホストIPがエクスポートポリシーに追加されます。

次のAPIを使用して、ホワイトリストに追加するIPアドレスを指定します。

```
patch /api/v1/vcenters/{vcguid}/settings/ip-whitelist

{
  value: string
}

GET /api/v1/vcenters/{vcguid}/settings/ip-whitelist

{
  value: string
}
```

ユーザロールと権限を設定

ONTAP toolsとONTAP System Managerに付属のJSONファイルを使用して、ストレージバックエンドを管理するための新しいユーザロールと権限を設定できます。

- 必要なもの *
- 次のコマンドを使用して、ONTAP PrivilegesファイルをONTAP toolsからダウンロードしておきます。
https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip



ユーザはクラスタレベルまたは直接Storage Virtual Machine (SVM) レベルで作成できません。user_roles.jsonファイルを使用せずにユーザを作成することもできます。作成した場合は、SVMレベルの最小限の権限セットが必要になります。

- ストレージバックエンドの管理者権限でログインしている必要があります。
- 手順 *
 1. ダウンロードした `https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip` ファイル。
 2. ONTAP システムマネージャにアクセスします。ONTAP System Managerにアクセスするには、クラスタのクラスタ管理IPを使用します。
 3. クラスタまたはSVMのユーザとしてログインします。
 4. >[設定]>[ユーザとロール]*ペインを選択します。
 5. [Users]で[Add]*を選択します。
 6. [ユーザーの追加*]ダイアログボックスで、[仮想化製品*]を選択します。
 7. [Browse]*を選択して、ONTAP Privileges JSONファイルを選択してアップロードします。
 プロダクトフィールドには、自動的に値が入力されます。
 8. 製品機能ドロップダウンメニューから必要な機能を選択します。
 [*役割* (*role*)] フィールドは、選択したプロダクト機能に基づいて自動的に入力されます。
 9. 必要なユーザ名とパスワードを入力します。
 10. ユーザに必要な権限 ([Discovery]、[Create Storage]、[Modify Storage]、[Destroy Storage]、[NAS/SAN Role]) を選択し、*[Add]*をクリックします。

新しいロールとユーザが追加され、設定したロールの詳細な権限が表示されます。



アンインストール処理では、ONTAPツールのロールは削除されませんが、ONTAPツール固有の権限のローカライズされた名前は削除され、プレフィックスが追加されます。xxx missing privilege 彼らにONTAP toolsを再インストールするか、新しいバージョンのONTAP toolsにアップグレードすると、標準のONTAP toolsロールとONTAP tools固有の権限がすべてリストアされます。

SVMアグリゲートのマッピングの要件

データストアのプロビジョニングに直接SVMのクレデンシャルを使用するために、内部ONTAPツールは、データストアのPOST APIで指定されたアグリゲートにボリュームを作成します。ONTAPでは、直接のSVMクレデンシャルを使用して、マッピングされていないアグリゲートにボリュームを作成することはできません。この問題を解決するには、ここで説明するREST APIまたはCLIを使用してSVMとアグリゲートをマッピングする必要があります。

REST API :

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI :

```

still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver          Aggregate          State          Size Type          SnapLock
Type-----
-----svm_test          still15_vsim_ucs630f_aggr1
online          10.11GB vmdisk  non-snaplock

```

ONTAPのユーザとロールを手動で作成する

このセクションの手順に従って、JSONファイルを使用せずにユーザとロールを手動で作成します。

1. ONTAP システムマネージャにアクセスします。ONTAP System Managerにアクセスするには、クラスタのクラスタ管理IPを使用します。
2. クラスタまたはSVMのユーザとしてログインします。
3. >[設定]>[ユーザとロール]*ペインを選択します。
4. ロールの作成：
 - a. テーブルの[追加]*を選択します。
 - b. 「* role name 」および「 Role Attributes *」の詳細を入力します。

ドロップダウンから* REST APIパス*とそれぞれのアクセスを追加します。
 - c. 必要なAPIをすべて追加し、変更を保存します。
5. ユーザの作成：
 - a. Users テーブルの Add *を選択します。
 - b. [ユーザの追加]ダイアログボックスで、*[System Manager]*を選択します。
 - c. 「* username *」を入力します。
 - d. 上記の*ロールの作成*ステップで作成したオプションから* role *を選択します。
 - e. アクセスを許可するアプリケーションと認証方法を入力します。ONTAPIとHTTPは必須のアプリケーションであり、認証タイプは* Password *です。
 - f. ユーザーの*パスワード*とユーザーの*保存*を設定します。

管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト

このセクションには、users JSONファイルを使用せずに作成された管理者以外のグローバル対象のクラスタユーザに必要な最小権限を記載します。

クラスタをローカルスコープで追加する場合は、jsonファイルを使用してユーザを作成することを推奨します。ONTAPツールでは、ONTAPでのプロビジョニングに読み取り権限だけでは不十分なためです。

APIの使用：

API	アクセスレベル	使用目的
/api/クラスタ	読み取り専用	クラスタ構成の検出

/api/cluster/licensing/licenses	読み取り専用	プロトコル固有のライセンスのライセンスチェック
/API/クラスタ/ノード	読み取り専用	プラットフォームタイプの検出
/API/ストレージ/アグリゲート	読み取り専用	データストア/ボリュームプロビジョニング時のアグリゲートスペースの確認
/API/ストレージ/クラスタ	読み取り専用	クラスタレベルのスペースと削減率のデータを取得するには
/API/ストレージ/ディスク	読み取り専用	アグリゲートに関連付けられているディスクを取得するには
/api/storage/qos/policies	読み取り/作成/変更	QoSとVMポリシーの管理
/api/SVM/SVMs	読み取り専用	クラスタがローカルに追加された場合にSVM構成を取得するため。
/api/network/ip/interfaces	読み取り専用	ストレージバックエンドの追加-管理LIFの範囲がクラスタ/SVMであることを確認します。
/API	読み取り専用	正しいストレージバックエンドステータスを取得するには、クラスタユーザにこの権限が必要です。それ以外の場合、ONTAP tools ManagerのUIに「unknown」ストレージバックエンドステータスが表示されます。

ONTAP Tools Managerユーザインターフェイス

ONTAP Tools for VMware vSphere 10.0は、複数のvCenterを管理するマルチテナントシステムです。管理者は、管理対象のvCenterと、オンボーディングするストレージバックエンドをより細かく制御する必要があります。

ONTAP tools Managerを使用すると、ONTAP tools管理者はより詳細な制御と機能を使用して、アプライアンス、テナント、ストレージバックエンドの全体的な管理を支援できます。

ONTAPツールは次の処理を実行します。

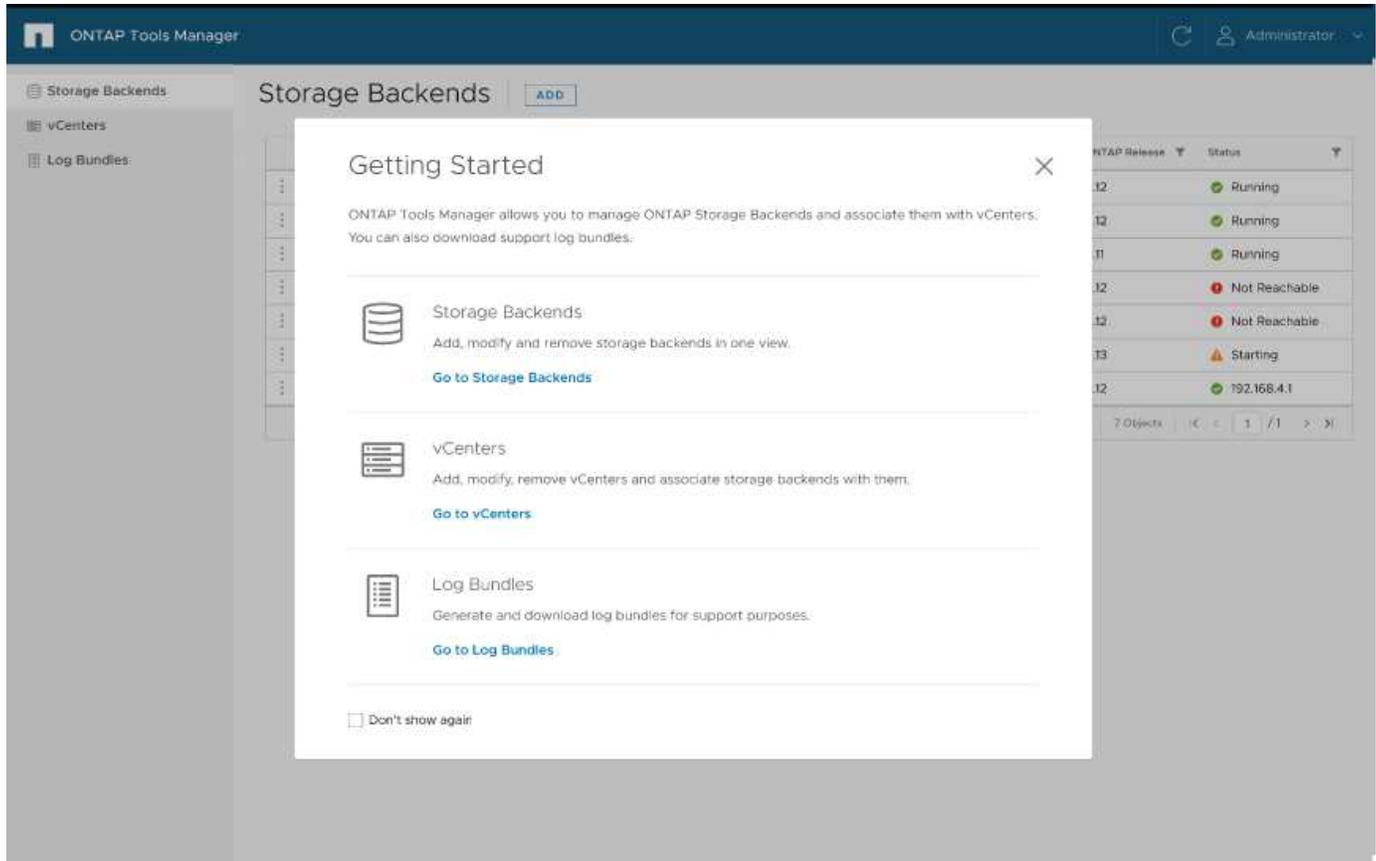
- vCenter管理- ONTAPツールへのvCenterの登録と登録解除
- ストレージバックエンド管理- ONTAPストレージクラスタをONTAPツールに登録および登録解除し、オンボードされたvCenterにグローバルにマッピングします。

ストレージバックエンドは、ONTAP tools Manager APIまたはCommons APIから追加するとグローバルになり、vCenter APIから追加するとローカルになります。

例：マルチテナントセットアップでは、ストレージバックエンド（クラスタ）をグローバルに追加し、SVMをローカルに追加してSVMの直接のクレデンシャルを使用できます。

- ログバンドルのダウンロード

ONTAP toolsのUIにアクセスするには、<https://loadBalanceIP:8443/virtualization/ui/> ブラウザから、導入時に指定したONTAP tools管理者のクレデンシャルを使用してログインします。



[今後表示しない]オプションを選択すると、同じブラウザから再度ログインしたときにこのポップアップが表示されなくなります。

vCenterの追加

vCenterは、ホスト、仮想マシン（VM）、およびストレージバックエンドを制御できる一元管理プラットフォームです。

- このタスクについて *

VMware vCenter 10.0向けONTAPツールの1つのインスタンスを使用して、複数のvCenterを追加および管理できます。

- 手順 *

1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーから[vCenters]を選択します。
3. vCenterのIPアドレス/ホスト名、ユーザ名、パスワード、およびポートを持つオンボードvCenterに* add *を選択します。

を参照してください "[管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト](#)".

ストレージバックエンドの追加

ストレージバックエンドは、EXSiホストがデータストレージに使用するシステムです。

- このタスクについて *

このタスクは、ONTAPクラスタのバインドに役立ちます。

- 手順 *

1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーから* Storage backends *を選択します。
3. 「* 追加」を選択します。
4. サーバのIPアドレスまたはFQDN、ユーザ名、およびパスワードの詳細を入力し、*[追加]*を選択します。



IPv4管理LIFのみがサポートされます。

ストレージバックエンドとvCenterの関連付け

vCenterのリストページに、関連付けられているストレージバックエンドの数が表示されます。各vCenterには、ストレージバックエンドを関連付けるオプションがある

- このタスクについて *

このタスクでは、ストレージバックエンドとオンボードされたvCenterの間のマッピングをグローバルに作成できます。

- 手順 *

1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーから[vCenters]を選択します。
3. ストレージバックエンドに関連付けるvCenterの縦の省略記号をクリックします。
4. ポップアップのドロップダウンからストレージバックエンドを選択します。
5. vCenterを必要なストレージバックエンドに関連付けるには、*[ストレージバックエンドの関連付け]* オプションを選択します。

を参照してください ["管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト"](#)。

vCenterを使用したオンボードストレージバックエンド（SVMまたはクラスタ）

次のAPIを使用してストレージバックエンドをオンボードし、SVMをvCenterにローカルでマッピングします。を参照してください ["ユーザロールと権限を設定"](#) セクションを参照してくださいONTAP。

```
POST /virtualization/api/v1/vcenters/<vcguid>/storage-backends

{
  "hostname_or_ip": "172.21.103.107",
  "username": "svm11",
  "password": "xxxxxxx"
}
```



上記のAPI応答のIDは検出で使用されます。

APIにはx-authを渡す必要があります。このx-authは、SwaggerのAuthに追加された新しいAPIから生成できません。

```
/virtualization/api/v1/auth/vcenter-login
```

VASA ProviderをvCenterに登録

自己署名証明書またはCA署名証明書を使用してVASA ProviderをvCenterに登録できません。自己署名証明書は、VMware CAハンドシェイクを使用して生成されます。

- このタスクについて *

CA署名証明書を使用する場合は、CA署名証明書をvCenterに配置する必要があります。

- 手順 *

1. vCenter Serverに移動します。
2. [設定]>[ストレージプロバイダ]*を選択します。
3. [追加]*アイコンをクリックします。
4. ストレージプロバイダの接続情報を入力します。
 - a. name：「ScaleoutVP」などのユーザフレンドリな名前
 - b. URL：https://<name>/virtualization/version.xml - URL内の名前は、単一vCenter環境の場合はOVA導入時に指定された仮想IP（または複数vCenter環境の場合はドメイン名）に対応します。証明書をURLに追加します。同じ証明書がvCenterに公開されます。
 - c. OVAの導入時に入力されたクレデンシャル：<VASA Provider username>/<VASA Provider

password>

5. VASAを登録したら、*[OK]*をクリックします。
[Storage Provider]の下に表示され、ステータスが[Online]になっていることを確認します。

CA署名証明書をvCenterに配置した場合は、CA署名証明書でVASAの登録が続行されます。そうしないと、ハンドシェイクが失敗し、登録のデフォルトはSSA証明書になります。

6. 複数のvCenterを1つのスケールアウトVPインスタンスに登録できます。
上記の手順を繰り返して、複数のvCenterに登録します。

vVolデータストアの作成

vVolデータストアは、新しいボリュームまたは既存のボリュームを使用して作成できます。既存のボリュームと新しいボリュームを組み合わせてvVolデータストアを作成することもできます。



ルートアグリゲートがSVMにマッピングされていないことを確認します。

APIにはx-authを渡す必要があります。このx-authは、SwaggerのAuthに追加された新しいAPIから生成できません。

```
/virtualization/api/v1/auth/vcenter-login
```

1. 新しいボリュームでvVolデータストアを作成する。
ONTAP REST APIを使用して、アグリゲートIDとストレージID (SVM UUID) を取得します。

```
POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores
```

次のURIを使用してステータスを確認します。

```
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?includeSubJobsAndTasks=true`
```

NFSデータストアのRequest Body

```
{
  "name": "nfsds1",
  "protocol": "nfs",
  "platform_type": "aff",
  "moref": "domain-c8",
  "volumes": [
    {
      "is_existing": false,
      "name": "vol_nfs_pvt",
      "size_in_mb": 2048000,
      "space_efficiency": "thin",
      "aggregate": {
        "id": "d7078b3c-3827-4ac9-9273-0a32909455c2"
      },
      "qos": {
        "min_iops": 200,
        "max_iops": 5000
      }
    }
  ],
  "storage_backend": {
    "storage_id": "654c67bc-0f75-11ee-8a8c-00a09860a3ff"
  }
}
```

iSCSIデータストアの要求本文：

```
{
  "name" : "iscsi_custom",
  "protocol" : "iscsi",
  "platform_type": "aff",
  "moref" : "domain-c8",
  "volumes" : [
    {
      "is_existing" : false,
      "name" : "iscsi_custom",
      "size_in_mb" : 8034,
      "space_efficiency" : "thin",
      "aggregate" : {
        "id" : "54fe5dd4-e461-49c8-bb2d-6d62c5d75af2"
      }
    }
  ],
  "custom_igroup_name": "igroup1",
  "storage_backend": {
    "storage_id": "eb9d33ab-1960-11ee-9506-00a0985c6d9b"
  }
}
```

1. 既存のボリュームを使用してvVolデータストアを作成する。

ONTAP REST APIを使用してaggregate_idとvolume_idを取得します。

```
POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores
```

リクエストボディ

```
{
  "name" : "nfsds2",
  "protocol" : "nfs",
  "platform_type": "aff",
  "moref" : "domain-c8",
  "volumes" : [
    {
      "is_existing": true,
      "id": "e632a632-1412-11ee-8a8c-00a09860a3ff"
    }
  ],
  "storage_backend": {
    "storage_id": "33a8b6b3-10cd-11ee-8a8c-00a09860a3ff"
  }
}
```

登録したSVMの確認

オンボードしたSVMがvCenter UIのVASA Providerの下に表示されていることを確認します。

• 手順 *

1. vCenter Serverに移動します。
2. 管理者のクレデンシャルでログインします。
3. [ストレージプロバイダ]*を選択します。
4. 「* Configure *」を選択します。
5. [Storage Provider/storage backends]で、オンボードしたSVMが正しく表示されていることを確認します。

ONTAP ツールを管理します

データストアを管理します

VVolデータストアのストレージの拡張または縮小

使用可能なストレージを増減するAPIが用意されています。

- 手順 *

vVolデータストアを拡張または縮小するには、次のAPIを使用します。

```
PATCH
/virtualization/api/v1/vcenters/{vcguid}/v vols/datastores/{moref}/volumes
```

例

- 新しいボリュームを追加するためにvVolデータストアを変更する

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/v vols/datastores/datastore-24/volumes
```

Request Body

```
{
  "operation": "grow",
  "volumes": [{
    "is_existing": false,
    "name": "exp3",
    "size_in_mb": 51200,
    "space_efficiency": "thin",
    "aggregate": {
      "id": "1466e4bf-c6d6-411a-91d5-c4f56210e1ab"
    },
    "storage_backend": {
      "storage_id": "13d86e4f-1fb1-11ee-9509-005056a75778"
    },
    "qos": {
      "max_iops": 5000
    }
  }]
}
```

- 既存のボリュームを追加するためにvVolデータストアを変更する

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores/datastore-24/volumes
```

Request Body

```
{
  "operation": "grow",
  "volumes": [{
    "is_existing": true,
    "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
  }]
}
```

- vVolデータストアの変更によるボリュームの削除とストレージからのボリュームの削除

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=true
```

Request Body

```
{
  "operation": "shrink",
  "volumes": [{
    "is_existing": true,
    "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
  }]
}
```

- ボリュームの削除にvVolデータストアを変更し、ストレージからボリュームは削除しない

```
PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=false
```

Request Body

```
{
  "operation": "shrink",
  "volumes": [{
    "is_existing": true,
    "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
  }]
}
```

vVolデータストアの削除

このAPIは、VMware Virtual Volumes (VVol) データストアをストレージから削除しま

す。

- このタスクについて *

VVOL データストアは、データストアに使用可能な FlexVol ボリュームが少なくとも 1 つあれば配置されます。HA クラスターで vVol データストアを削除する場合は、まず HA クラスター内のすべてのホストからデータストアをアンマウントしてから、vCenter サーバのユーザインターフェイスを使用して `_vsphere-ha_folder` を手動で削除します。

- 手順 *

vVol データストアを削除するには、次の API を使用します。

```
DELETE
/virtualization/api/v1/vcenters/{vcguid}/v vols/datastores/{moref}
```

例

- vVol データストアの削除とストレージからのボリュームの削除

```
DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/v vols/datastores/datastore-28?delete_volumes=true
```



vVol データストアの削除ワークフローでは、`datastore-volume` が管理されているかどうかに関係なく、`delete_volume` フラグが `true` に設定されている場合、`datastore-volumes` が削除されます。

- vVol データストアを削除し、ストレージからボリュームは削除しない

```
DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/v vols/datastores/datastore-28?delete_volumes=false
```

対応：

```
{
  "id": "1889"
}
```

vVol データストアのマウントとアンマウント

VMware 仮想ボリューム (vVol) データストアは、Mount VVOLs Datastore (vVol データストアのマウント) ダイアログボックスを使用して、1 つ以上の追加のホストにマ

ウントできます。データストアをマウントすると、他のホストからストレージにアクセスできるようになります。vVolデータストアをアンマウントすることもできます。

vVolデータストアをマウントまたはアンマウントするには、次のAPIを使用します。APIにはx-authを渡す必要があります。このx-authは、SwaggerのAuthに追加された新しいAPIから生成できません。

```
/virtualization/api/v1/auth/vcenter-login
```

```
PATCH  
/virtualization/api/v1/vcenters/{vcguid}/vvols/datastores/{moref}/hosts
```

vCenterからVVolデータストアMORefを取得します。

リクエストボディ

```
{  
  "operation": "mount",  
  "morefs": [  
    "host-7044"  
  ],  
}
```

例

- 追加ホストにマウント

追加のホストにマウントするには、次のAPIを使用します。

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-  
691250bfe2df/vvols/datastores/datastore-24/hosts
```

Request Body

```
{  
  "operation": "mount",  
  "morefs": ["host-13"],  
}
```

- 追加ホストでアンマウント

追加のホストでアンマウントするには、次のAPIを使用します。

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/datastores/datastore-24/hosts
```

Request Body

```
{  
  "operation": "unmount",  
  "morefs": ["host-13"],  
}
```

ストレージバックエンドの管理

ストレージバックエンドは、EXSiホストがデータストレージに使用するシステムです。

ストレージバックエンドの追加

ストレージバックエンドを追加するには、次の手順を実行します。

- 手順 *
 1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
 2. サイドバーから* Storage backends *を選択します。
 3. 「* 追加」を選択します。

ストレージバックエンドの変更

既存のストレージバックエンドを変更するには、次の手順を実行します。

1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーからストレージバックエンドを選択します。
3. 変更する*ストレージバックエンド*を選択します。
4. 縦の省略記号メニューをクリックし、*修正*を選択します。
5. ストレージバックエンドを変更するには、**[Username]***と**[Password]***を入力します。

ストレージバックエンドの削除

ストレージバックエンドを削除する前に、ストレージバックエンドに接続されているすべてのデータストアを削除する必要があります。

ストレージバックエンドを削除するには、次の手順を実行します。

1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーから* Storage backends *を選択します。

3. 削除するストレージバックエンドを選択してください
4. 縦の省略記号メニューをクリックし、*[削除]*を選択します。

vCenterの管理

vCenterは、ホスト、仮想マシン、およびストレージバックエンドを制御できる一元管理プラットフォームです。

vCenterの追加

VMware vCenter 10.0向けONTAPツールの1つのインスタンスを使用して、複数のvCenterを追加および管理できます。

• 手順 *

1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーから[vCenters]を選択します。
3. vCenterのIPアドレス/ホスト名、ユーザ名、パスワード、およびポートを持つオンボードvCenterに*add *を選択します。
4. ストレージバックエンド*ページに移動し、[ホスト名、ユーザ名、パスワード、およびポートを指定してオンボードストレージバックエンド（ONTAPクラスタ）に追加する]を選択します。

を参照してください ["管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト"](#)。

vCenterへのストレージバックエンドの関連付けまたは関連付け解除

vCenterのリストページに、関連付けられているストレージバックエンドの数が表示されます。各vCenterでストレージバックエンドの関連付けまたは関連付け解除を選択可能
このタスクでは、ストレージバックエンドとオンボードされたvCenterの間のマッピングをグローバルに作成できます。

• 手順 *

1. を起動します <https://loadBalanceIP:8443/virtualization/ui/> 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーから[vCenters]を選択します。
3. ストレージバックエンドに関連付ける、またはストレージバックエンドとの関連付けを解除するvCenterの縦の省略記号をクリックします。
4. 実行するアクションに応じて*[ストレージバックエンドの関連付け]または[関連付け解除]*を選択します。

を参照してください ["管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト"](#)。

vCenterの変更

vCenterを変更するには、次の手順に従います。

1. を起動します `https://loadBalanceIP:8443/virtualization/ui/` 導入時に指定したONTAP tools 管理者のクレデンシャルをブラウザから使用
2. サイドバーから[vCenters]を選択します。
3. 変更するvCenterの縦の省略記号をクリックし、*[変更]*を選択します。
4. vCenterの詳細を変更し、*[変更]*を選択します。

vCenterの削除

vCenterを削除する前に、vCenterに接続されているすべてのストレージバックエンドを削除する必要があります。

1. を起動します `https://loadBalanceIP:8443/virtualization/ui/` 導入時に指定したONTAP tools 管理者のクレデンシャルをブラウザから使用
2. サイドバーから[vCenters]を選択します。
3. 削除するvCenterの縦の省略記号をクリックし、*[Remove]*を選択します。



削除したvCenterはアプリケーションで管理されなくなります。

ストレージしきい値の管理

次のGETしきい値APIを使用して、ボリュームおよびアグリゲートに設定されているストレージしきい値の制限を取得します。

```
GET/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

例

vCenter GUIDによるvCenterごとのストレージしきい値の取得

```
GET "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-thresholds"
```

次のパッチ設定アラームをボリュームとアグリゲートに対して使用して、設定したしきい値に達したときに通知を生成します。

```
PATCH/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

例

vCenter GUIDを使用して、vCenterごとのストレージしきい値を更新します。デフォルトの制限は、「ほぼフル」が80%、「フル」が90%です。

すべてのしきい値設定の変更

```
{{{PATCH "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-
thresholds"
Request Body
{
"volume":

{ "nearly_full_percent": 80, "full_percent": 90 }
,
"aggregate": {
"nearly_full_percent": 80,
"full_percent": 90
}
}}}}}}
```

VVolライフサイクルの管理

VMware vCenterユーザインターフェイスを使用してVirtual Volumes (VVol) を管理できます。詳細については、[を参照してください "VMware のドキュメント"](#)。

管理対象のigroupとエクスポートポリシー

ONTAPでは、エクスポートポリシーを使用してホストへのボリュームデータパスにアクセスし、イニシエータグループ (igroup) を使用してESXiホストへの論理ユニット番号 (LUN) データパスにアクセスします。

仮想ボリュームデータストアを作成またはvCenterのホストにマウントする際には、データストアのプロトコルタイプに応じて、それらのホストにボリューム (NFS) またはLUN (iSCSI) へのアクセスを許可する必要があります。

エクスポートポリシーは動的で、新しいエクスポートポリシーがtrident-uuid形式で作成されます。ONTAPシステムマネージャで、**[ストレージ]>*>[ストレージVM名]>[設定]>[エクスポートポリシー]***の順に選択し、エクスポートポリシーを確認します。

ONTAP toolsのigroupとエクスポートポリシーは効率的に管理されるため、次のようなメリットがあります。

- 移行されたエクスポートポリシーとigroupをサポートします。
- 仮想マシンの入出力操作が中断されることはありません。
- 手動操作なしで追加ホストへのマウントをサポートします。
- igroupとエクスポートポリシーの数を最小限に抑えることができます。
- ガベージコレクタは、未使用の管理対象igroupとエクスポートポリシーをすべて定期的に自動的に削除します。
- データストアがホストクラスタレベルでプロビジョニングされている場合は、igroupが作成され、そ

のigroupに追加されたホストクラスタの下にあるすべてのホストイニシエータが含まれます。

ONTAP ツールのメンテナンスコンソールにアクセスします

ONTAP ツールメンテナンスコンソールの概要

ONTAP ツールのメンテナンスコンソールを使用して、アプリケーション、システム、およびネットワークの構成を管理できます。管理者パスワードとメンテナンスパスワードを変更することができます。サポートバンドルの生成、異なるログレベルの設定、TLS設定の表示と管理、およびリモート診断の開始を行うこともできます。

ONTAP ツールを導入したあと、メンテナンスコンソールにアクセスするために VMware ツールをインストールしておく必要があります。を使用する必要があります maint 導入時に設定したユーザ名とパスワードを使用して、ONTAP toolsのメンテナンスコンソールにログインします。maintまたはrootログインコンソールでファイルを編集するには、* nano *を使用する必要があります。



のパスワードを設定する必要があります diag ユーザがリモート診断を有効にしています。

導入した ONTAP ツールの * Summary * タブを使用して、メンテナンスコンソールにアクセスする必要があります。をクリックします  をクリックすると、メンテナンスコンソールが起動します。

* コンソール・メニュー *	* オプション *
アプリケーションの設定	<ol style="list-style-type: none">1. サーバステータスの概要を表示します2. VASA Providerサービスのログレベルの変更
System Configuration (システム設定)	<ol style="list-style-type: none">1. 仮想マシンをリブートします2. 仮想マシンをシャットダウンします3. 「maint」ユーザのパスワードを変更します4. タイムゾーンを変更します5. 新しいNTPサーバを追加します6. jail ディスクサイズ (/jail) の拡張7. アップグレード8. VMware Tools をインストールします

ネットワーク構成：	<ol style="list-style-type: none"> 1. IP アドレス設定を表示します 2. ドメイン名検索設定を表示します 3. ドメイン名検索設定を変更します 4. 静的ルートを表示します 5. 静的ルートを変更します 6. 変更をコミットします 7. ホストに ping を実行します 8. デフォルト設定に戻します
サポートと診断	<ol style="list-style-type: none"> 1. 診断シェルにアクセスします 2. リモート診断アクセスを有効にします

リモート診断アクセスを設定します

diag ユーザの SSH アクセスを有効にするように ONTAP ツールを設定することができます。

- 必要なもの *

vCenter Server インスタンスの VASA Provider 拡張機能を有効にする必要があります。

- このタスクについて *

SSH を使用して diag ユーザアカウントにアクセスする際は次の制限があります。

- SSH をアクティブ化した場合、使用できるログインアカウントは 1 つだけです。
- diag ユーザアカウントへの SSH アクセスは、次のいずれかの状況になると無効になります。
 - タイムアウトした場合。

ログインセッションの有効期限は翌日の午前 0 時までです。

- SSH を使用して diag ユーザとして再度ログインした場合。

- 手順 *

1. vCenter Server で、 VASA Provider へのコンソールを開きます。
2. maintenance ユーザとしてログインします。
3. 入力するコマンド 4 [Support and Diagnostics]を選択します。
4. 入力するコマンド 3 [Enable remote diagnostics access]を選択します。
5. 入力するコマンド y [確認]ダイアログボックスで、リモート診断アクセスを有効にします。
6. リモート診断アクセス用のパスワードを入力します。

他のノードでSSHを開始する

アップグレードの前に、他のノードでSSHを開始する必要があります。

- 必要なもの *

vCenter Server インスタンスの VASA Provider 拡張機能を有効にする必要があります。

- このタスクについて *

アップグレードの前に、各ノードでこの手順を実行してください。

- 手順 *

1. vCenter Server で、 VASA Provider へのコンソールを開きます。
2. maintenance ユーザとしてログインします。
3. 入力するコマンド 4 [Support and Diagnostics]を選択します。
4. 入力するコマンド 1 [Access diagnostic shell]を選択します。
5. 入力するコマンド `y` 続行してください。
6. コマンド `_sudo systemctl restart ssh_` を実行します。

vCenterとONTAPのクレデンシャルを更新する

メンテナンスコンソールを使用して、vCenterとONTAPのクレデンシャルを更新できます。

- 必要なもの *

maintユーザのログインクレデンシャルが必要です。

- このタスクについて *

導入後にvCenter、ONTAP、またはDatalifのクレデンシャルを変更した場合は、この手順を使用してクレデンシャルを更新する必要があります。

- 手順 *

1. vCenter Server で、 VASA Provider へのコンソールを開きます。
2. maintenance ユーザとしてログインします。
3. 入力するコマンド 4 [Support and Diagnostics]を選択します。
4. 入力するコマンド 1 [Access diagnostic shell]を選択します。
5. 入力するコマンド `y` 続行してください。
6. 必要に応じてクレデンシャルを更新します。
 - a. ONTAPクレデンシャルを更新するには、次のコマンドを実行します。

```
otv-update --ontapUsername <new username>-- ontapPassword <new password>
```

b. vCenterクレデンシャルを更新するには、次のコマンドを実行します。

```
otv-update --vcenterUsername <new username>-- vcenterPassword <new password>
```

c. datalifを更新するには、次のコマンドを実行します。

```
otv-update --dataLif <新しいDatalif IP>
```

ログファイルを収集します

ONTAP tools Managerのユーザインターフェイスのオプションを使用して、ONTAP tools for VMware vSphereのログファイルを収集できます。テクニカルサポートに問題のトラブルシューティングを依頼すると、ログファイルの収集を求められることがあります。

• 手順 *

1. を起動します `https://loadBalanceIP:8443/virtualization/ui/` 導入時に指定したONTAP tools管理者のクレデンシャルをブラウザから使用
2. サイドバーから* Log Bundles *を選択します。

この処理には数分かかることがあります。

3. [生成]*を選択して、ログファイルを生成します。
4. [Log Bundle]のラベルを入力し、*[generate]*を選択します。

tar.gzファイルをダウンロードし、テクニカルサポートに送信します。

検出

検出間隔は、コンフィギュレーションマップの一部として設定できます。スケジュールされた検出は60分ごとに実行されます。ここで指定するAPIは、ローカルスコープに追加された特定のストレージバックエンドに対してオンデマンドで検出を実行するためのものです。

次のAPIを使用して検出を実行します。

```
POST
/virtualization/api/v1/vcenters/{vcguid}/storage-backends/{id}/discovery-
jobs
```



を参照してください "[オンボードストレージバックエンド \(SVMまたはクラスタ\)](#) " セクションにアクセスし、ストレージバックエンドAPIの応答からIDを取得します。

このAPIエンドポイントからの検出は、ローカルを対象としたストレージバックエンドでのみサポートされ、グローバルを対象としたストレージバックエンドではサポートされません。

ストレージバックエンドのタイプがclusterの場合は、子SVMに対して暗黙的に検出が実行されます。ストレージバックエンドのタイプがSVMの場合、選択したSVMに対してのみ検出が実行されます。

例

IDで指定したストレージバックエンドで検出を実行するには

```
POST
/api/v1/vcenters/3fa85f64-5717-4562-b3fc-2c963f66afa6/storage-
backends/74e85f64-5717-4562-b3fc-2c963f669dde/discovery-jobs
```

APIにはx-authを渡す必要があります。このx-authは、SwaggerのAuthに追加された新しいAPIから生成できません。

```
/virtualization/api/v1/auth/vcenter-login
```

ONTAPツールの移行

最新リリースのONTAP toolsに移行する

ストレージデータを移行する際、ストレージバックエンドはREST APIを使用して手動でオンボーディングされます。VASA Providerのデータを移行すると、既存のDerbyデータベースからデータがエクスポートされ、MongoDBデータベースにインポートされます。



従来のセットアップは、VASA Provider機能のみを実行する場合にのみ移行することを推奨します。従来の/NVMeデータストアやVVolレプリケーションなどの機能がある場合や、従来のSRAが有効になっている場合は、ONTAP tools for VMware vSphere 10.0にセットアップを移行することは推奨されません。

- このタスクについて *

ONTAP tools for VMware vSphere 9.10D2および9.11D4リリースから10.0リリースへの移行がサポートされます。移行元：

* ONTAP tools for VMware vSphere 9.10リリース。最初に9.10D2リリースにアップグレードしてから10.0リリースに移行します。

* ONTAP tools for VMware vSphere 9.11リリース。最初に9.11D4リリースにアップグレードしてから、10.0リリースに移行します。



既存のユーザは、9.10Dパッチまたは9.11Dパッチにアップグレードする前に、9.10/9.11からOVAバックアップを作成する必要があります。

- 手順 *

1. 既存のONTAP tools for VMware vSphere 9.10D2および9.11D4でDerbyポート1527を有効にします。ポートを有効にするには、rootユーザでCLIにログインし、次のコマンドを実行します。

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. ONTAP tools for VMware vSphere 10.0リリース向けOVAを導入します。を参照してください "[ONTAP ツールクイックスタート](#)"
3. 移行するvCenterをONTAP tools for VMware vSphere 10.0リリースに追加します。を参照してください "[vCenterの追加](#)"。
4. リモートプラグインのvCenter APIからローカルでストレージバックエンドをオンボードする。を参照してください "[オンボードストレージバックエンド](#)"。移行対象としてローカルスコープのストレージを追加します。
5. 次のAPIを使用して移行します。

```
/api/v1/vcenters/{vcguid}/migration-jobs

{
  "otv_ip": "10.10.10.10",
  "vasa_provider_credentials": {
    "username": "Administrator",
    "password": "password"
  }
}
```

上記のAPI呼び出しは、ステータスチェックに使用できるjobidを返します。

6. 次のURIを使用してステータスを確認します。

```
https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?includeSubJobsAndTasks=true
```

7. ジョブが完了したら、移行レポートを検証します。job-responseからレポートをJobDataの一部として表示できます。
8. ONTAP toolsのストレージプロバイダ10.0をvCenterと ["VASA ProviderをvCenterに登録"](#)。
9. ONTAP toolsストレージプロバイダ9.10 / 9.11 VASA Providerサービスを停止します（maintコンソールからVASA Providerを停止します）。

NetAppでは、VASAプロバイダを削除しないことを推奨しています。

古いVASAプロバイダが停止すると、vCenterはONTAP tools for VMware vSphere 10.0にフェイルオーバーします。すべてのデータストアとVMにアクセスし、ONTAP Tools for VMware vSphere 10.0からアクセスできるようになります。

10. 次のAPIを使用してパッチの移行を実行します。

```
/virtualization/api/v1/vcenters/{vcguid}/migration-jobs/{migration_id}
```

PATCH処理の要求の本文が空です。



UUIDは、移行後のAPIの応答で返された移行UUIDです。

パッチ移行APIが正常に完了すると、すべてのVMがストレージポリシーに準拠するようになります。

移行用の削除APIは次のとおりです。

```
Delete /virtualization/api/v1/vcenters/{vcguid}/migration-  
jobs/{migration_id}
```

このAPIは、移行IDによる移行を削除し、指定したvCenter上の移行を削除します。

移行が完了したら、ONTAP tools 10.0をvCenterに登録したら、次の手順を実行します。

- すべてのホストで証明書を更新します。
- しばらくしてからデータストア (DS) および仮想マシン (VM) の処理を実行します。待機時間は、セットアップに含まれるホスト、DS、VMの数によって異なります。待機しないと、操作が断続的に失敗する可能性があります。

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

プライバシーポリシー

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

["ONTAP tools for VMware vSphere 10.0に関する注意事項"](#)

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。