



ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

目次

ONTAP tools for VMware vSphere	1
リリース ノート	2
リリース ノート	2
ONTAP tools for VMware vSphereの新機能	2
ONTAP tools for VMware vSphere 9 とONTAP tools for VMware vSphere 10 の機能比較	2
概念	5
ONTAP tools for VMware vSphereの概要	5
重要な概念と用語	5
ロールベース アクセス制御	8
ONTAP tools for VMware vSphereについて学ぶ	8
VMware vSphere を使用した RBAC	10
ONTAPを使用した RBAC	13
ONTAP tools for VMware vSphereの高可用性	16
ONTAPツールマネージャのユーザーインターフェース	17
ONTAP tools for VMware vSphereを導入する	19
ONTAP tools for VMware vSphereのクイック スタート	19
高可用性 (HA) 展開ワークフロー	21
ONTAP tools for VMware vSphere	21
システム要件	21
最低限のストレージとアプリケーションの要件	22
ポート要件	22
ONTAP tools for VMware vSphereを導入するための構成制限	24
ONTAP tools for VMware vSphere- ストレージ レプリケーション アダプタ (SRA)	25
始める前に...	25
展開ワークシート	26
ネットワークファイアウォールの構成	27
ONTAPストレージ設定	27
ONTAP tools for VMware vSphereを導入する	27
デプロイメントエラーコード	32
ONTAP Tools for VMware vSphereの設定	35
vCenter Serverインスタンスを追加する	35
VASA プロバイダを vCenter Server インスタンスに登録する	35
NFS VAAIプラグインのインストール	36
ESXiホスト設定を構成する	37
ESXi サーバーのマルチパスとタイムアウト設定を構成する	37
ESXiホストの値を設定する	38
ONTAPユーザーの役割と権限を構成する	39
SVM集約マッピング要件	40
ONTAPユーザーとロールを手動で作成する	40

ONTAP tools for VMware vSphereを10.3 ユーザーにアップグレードする	48
ONTAP tools for VMware vSphereを10.4 ユーザー向けにアップグレードする	50
ストレージバックエンドを追加する	50
ストレージ バックエンドを vCenter Server インスタンスに関連付ける	52
ネットワークアクセスを構成する	53
データストアを作成する	53
データストアと仮想マシンの保護	58
ホストクラスタ保護を使用して保護する	58
SRA保護を使用して保護する	59
データストアを保護するためにSRAを構成する	59
SANおよびNAS環境向けにSRAを構成する	59
大規模環境向けに SRA を構成する	61
VMware Live Site RecoveryアプライアンスでSRAを構成する	61
SRAクレデンシャルの更新	62
保護対象サイトとリカバリ サイトの設定	63
保護対象サイトとリカバリ サイトのリソースの設定	64
レプリケートされたストレージ システムの検証	68
ファンアウト保護	69
ONTAP tools for VMware vSphereを管理する	72
ONTAP tools for VMware vSphereの概要	72
ONTAPツールマネージャのユーザーインターフェース	73
ONTAP tools for VMware vSphereにおける igroup とエクスポート ポリシーを理解する	75
エクスポート ポリシー	79
ONTAPツールで管理されるigroupを理解する	80
ONTAP tools for VMware vSphereを有効にする	83
ONTAP tools for VMware vSphereを変更する	84
データストアの管理	85
NFSおよびVMFSデータストアをマウントする	85
NFSおよびVMFSデータストアのマウント解除	86
vVolデータストアのマウント	86
NFSおよびVMFSデータストアのサイズ変更	87
vVolsデータストアを拡張する	87
vVolsデータストアを縮小する	88
データストアを削除する	88
データストアのONTAPストレージビュー	89
仮想マシンのストレージビュー	90
ストレージしきい値を管理する	90
ストレージバックエンドの管理	90
ストレージを発見	91
ストレージバックエンドを変更する	91
ストレージバックエンドを削除する	91

ストレージバックエンドのドリルダウンビュー	92
vCenter Serverインスタンスを管理する	93
ストレージ バックエンドと vCenter Server インスタンスの関連付けを解除します。	93
vCenter Serverインスタンスを変更する	93
vCenter Serverインスタンスを削除する	93
証明書の管理	94
ONTAP tools for VMware vSphereにアクセスする	96
ONTAP tools for VMware vSphereの概要	96
リモート診断アクセスの設定	97
他のノードでSSHを起動する	98
vCenter ServerとONTAPの認証情報を更新する	98
ONTAPツールレポート	98
ログ ファイルの収集	99
仮想マシンの管理	100
仮想マシンの移行またはクローン作成に関する考慮事項	100
NFS および VMFS データストアを持つ仮想マシンをvVolsデータストアに移行する	101
VASAのクリーンアップ	101
仮想マシンからデータディスクを接続または切断する	102
ストレージ システムとホストの検出	102
ONTAP Toolsを使用したESXiホストの設定の変更	103
パスワードを管理する	104
ONTAPツールマネージャのパスワードを変更する	104
ONTAPツールマネージャのパスワードをリセットする	104
アプリケーションユーザーのパスワードをリセットする	105
メンテナンスコンソールのユーザーパスワードをリセットする	105
ホストクラスタ保護の管理	106
保護されたホスト クラスタを変更する	106
ホストクラスタ保護を削除する	109
AutoSupportを無効にする	109
AutoSupportプロキシ URL を更新する	110
NTPサーバーを追加する	110
ONTAPツールのセットアップのバックアップを作成し、復元する	110
バックアップを作成し、バックアップファイルをダウンロードする	111
リカバリ	111
ONTAP tools for VMware vSphereをアンインストールする	112
FlexVolボリュームを削除する	113
ONTAP tools for VMware vSphereのアップグレード	114
ONTAP tools for VMware vSphereから 10.4 へのアップグレード	114
アップグレードエラーコード	117
ONTAP tools for VMware vSphereを10.4 に移行する	122
ONTAP tools for VMware vSphereから 10.4 に移行する	122

VASA プロバイダーを移行し、SRA を更新する	122
VASAプロバイダーの移行手順	122
ストレージレプリケーションアダプタ(SRA)を更新する手順	125
REST APIを使用した自動化	127
ONTAP tools for VMware vSphereについて学ぶ	127
基盤としてのREST Webサービス	127
ONTAPツールマネージャ環境	127
ONTAP tools for VMware vSphereの実装の詳細	128
REST APIにアクセスする方法	128
HTTP の詳細	129
認証	130
同期リクエストと非同期リクエスト	130
ONTAP tools for VMware vSphereの最初の	130
開始する前に	131
ステップ1: アクセストークンを取得する	131
ステップ2: REST API呼び出しを発行する	131
ONTAP tools for VMware vSphereの API リファレンス	132
法律上の表示	133
著作権	133
商標	133
特許	133
プライバシー ポリシー	133
オープンソース	133

ONTAP tools for VMware vSphere

リリース ノート

リリース ノート

ONTAP tools for VMware vSphereで利用できる新機能と拡張機能について説明します。

新機能と強化機能の完全なリストについては、[ONTAP tools for VMware vSphereの新機能](#)。

ONTAP tools for VMware vSphere 9からONTAPツール10.4への移行がお客様の環境に適しているかどうかについて詳しくは、以下を参照してください。[ONTAP tools for VMware vSphere 9 とONTAP tools for VMware vSphere 10 の機能比較](#)。ONTAP tools for VMware vSphereからONTAP tools for VMware vSphereへの移行がサポートされています。

詳細については、"[ONTAP tools for VMware vSphereのリリース ノート](#)"。リリース ノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

ONTAP tools for VMware vSphereの新機能

ONTAP tools for VMware vSphereで利用できる新しい機能について説明します。

更新	説明
" クラスタあたり12ノードのASA r2システムのサポート "	ONTAP tools for VMware vSphereは、クラスタあたり最大 12 ノードのASA r2 ストレージ システムのワークフローをサポートし、データ管理の効率とスケーラビリティを向上させます。iSCSI および FC プロトコルを使用したvVolsデータストア、および iSCSI、FC、NVMe プロトコルを使用した VMFS データストアをサポートし、柔軟で強化されたストレージ オプションを提供します。
" ONTAPツールマネージャのユーザーインターフェースの強化 "	NTP サーバーを有効にして環境全体で正確な時刻同期を実現し、テレメトリ設定を構成してONTAPツール マネージャー インターフェイスからシステム パフォーマンスを監視および分析できるようになりました。これらの設定はメンテナンス コンソールでは利用できなくなりました。
強化されたセキュリティ機能	セキュリティ機能により、保護が強化され、業界標準に準拠できるようになり、管理者が VMware 環境をより効果的に管理できるように、強力でユーザーフレンドリーなエクスペリエンスが提供されます。
" 強化されたSRA災害復旧機能 "	ONTAP tools for VMware vSphereでは、SnapMirror のスケジュールされたスナップショット コピーに加えて、カスタム名のスナップショットを備えた Site Recovery Appliance (SRA) を使用した災害復旧操作がサポートされるようになりました。

ONTAP tools for VMware vSphere 9 とONTAP tools for VMware vSphere 10 の機能比較

ONTAP tools for VMware vSphere 9 からONTAP tools for VMware vSphere 10.1 以降のバージョンへの移行が適切かどうかを確認します。



最新の互換性情報については、["NetApp Interoperability Matrix Tool"](#)。

特徴	ONTAPツール9.13	ONTAPツール10.1	ONTAPツール10.2以降
主な価値提案	強化されたセキュリティ、コンプライアンス、自動化機能により、Day 0 から Day 2 の運用を合理化および簡素化します。	高可用性、パフォーマンス、スケールの限界を拡張しながら、ONTAPツール 10.x を 9.xx と同等に進化させます。	サポートが拡張され、VMFS およびvVolsの FC、および VMFS 専用の NVMe-oF/FC、NVMe-oF/TCP が含まれるようになりました。NetApp SnapMirrorの使いやすさ、vSphere メトリックストレージ クラスターのシンプルなセットアップ、および 3 サイトの VMware Live Site Recovery のサポート
ONTAPリリース認定	ONTAP 9.9.1 からONTAP 9.16.1	ONTAP 9.12.1 からONTAP 9.14.1	ONTAPツール 10.2 の場合はONTAP 9.12.1 からONTAP 9.15.1 まで。ONTAPツール 10.3 用のONTAP 9.14.1、9.15.1、9.16.0、および 9.16.1。ONTAPツール 10.4 用のONTAP 9.14.1、9.15.1、9.16.0、および 9.16.1。ASA r2 システムを使用する場合、ONTAPツール 10.4 にはONTAP 9.16.1P3 以降が必要です。
VMware リリースのサポート	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 から VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 から VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 から VMware Live Site Recovery 9.0
プロトコルのサポート	NFS および VMFS データストア: NFS (v3 および v4.1)、VMFS (iSCSI および FCP) vVolsデータストア: iSCSI、FCP、NVMe/FC、NFS v3	NFS および VMFS データストア: NFS (v3 および v4.1)、VMFS (iSCSI) vVolsデータストア: iSCSI、NFS v3	NFS および VMFS データストア: NFS (v3 および v4.1)、VMFS (iSCSI/FCP/NVMe-oF) vVolsデータストア: iSCSI、FCP、NFS v3
拡張性	ホストとVM: 300台のホスト、最大10K台のVM データストア: 600台のNFS、最大50台のVMFS、最大250台のvVols vVols: 最大14,000	ホストとVM: 600ホストvVols: 最大140,000	ホストとVM: 600ホストvVols: 最大140,000
可観測性	パフォーマンス、容量、ホストコンプライアンスダッシュボード 動的なVMとデータストアレポート	パフォーマンス、容量、ホストコンプライアンスダッシュボードの更新 動的VMおよびデータストアレポート	パフォーマンス、容量、ホストコンプライアンスダッシュボードの更新 動的VMおよびデータストアレポート

特徴	ONTAPツール9.13	ONTAPツール10.1	ONTAPツール10.2以降
データ保護	VMFSおよびNFSのSRAレプリケーション、vVolsのFlexVolベースのレプリケーション、SCV統合およびバックアップの相互運用性	iSCSI VMFSおよびNFS v3データストアのSRAレプリケーション	SMAS と VMware Live Site Recovery を組み合わせた iSCSI VMFS および NFS v3 データストアの 3 サイト保護の SRA レプリケーション。
VASAプロバイダーのサポート	VASA 4.0	VASA 3.0	VASA 3.0

概念

ONTAP tools for VMware vSphereの概要

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して、データストアのプロビジョニングを支援し、仮想マシンの基本的な保護を提供します。ONTAP tools for VMware vSphereは、Open Virtual Appliance (OVA) として導入される、水平方向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。このリリースでは、REST API とONTAPが統合されています。

ONTAP tools for VMware vSphereは、次のものから構成されます。

- 基本的な保護や災害復旧などの仮想マシン機能
- VMのきめ細かな管理を可能にするVASAプロバイダー
- ストレージポリシーベースの管理
- Storage Replication Adapter (SRA)

重要な概念と用語

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

ASA r2 システム

新しいNetApp ASA r2 システムは、SAN のみを利用するお客様のニーズに合わせた簡素化されたエクスペリエンスを実現する、統合されたハードウェアおよびソフトウェア ソリューションを提供します。["ASA r2 ストレージシステムについて学ぶ"](#)。

認証局 (CA)

CA は、Secure Sockets Layer (SSL) 証明書を発行する信頼できるエンティティです。

一貫性グループ (CG)

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。CG は、ストレージ ユニットおよびボリューム間でデータの一貫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 ["一貫性グループ"](#)。

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、中断のない操作のために HA ペアで構成されます。

論理ユニット番号 (LUN)

LUN は、ストレージ エリア ネットワーク (SAN) 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、通常はSCSI (Small Computer System Interface) プロトコルやそのカプセル化された派生プロトコルの1つを介してアクセスされる論理ディスクです。

NVMe名前空間とサブシステム

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および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ーに関連付けることで、関連付けられたイニシエーターがサブシステム内の名前空間にアクセスできるようになります。

ONTAPツールマネージャー

ONTAPツール マネージャーは、管理対象 vCenter Server インスタンスおよびオンボード ストレージ バックエンドに対するONTAP tools for VMware vSphereをより細かく制御できるようにします。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、およびログ バンドルのダウンロードの管理に役立ちます。

オープン仮想アプライアンス (OVA)

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 スタンドードです。

復旧ポイント目標 (RPO)

RPO は、データをバックアップまたは複製する頻度を測定します。業務を再開するために、障害後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、組織の RPO が 4 時間の場合、災害発生時に最大 4 時間分のデータの損失を許容できます。

SnapMirrorアクティブ同期

SnapMirrorアクティブ シンクにより、サイト全体の障害が発生した場合でもビジネス サービスは継続して稼働でき、セカンダリ コピーを使用してアプリケーションを透過的にフェイルオーバーできます。SnapMirror Active Sync でフェイルオーバーをトリガーするには、手動による介入やカスタム スクリプトは必要ありません。詳細はこちら ["SnapMirrorアクティブ同期"](#)。

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のファイル、データ、およびその他のリソースを保存するために使用する基盤となるストレージ インフラストラクチャです。これらにより、ESXi ホストは永続データにアクセスして管理できるようになり、仮想化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)

ONTAPクラスタ認証情報でのみ使用可能なグローバル ストレージ バックエンドは、ONTAPツール マネージャ インターフェイスを通じてオンボードされます。最小限の権限で追加することで、vVols管理に必要な重要

なクラスター リソースの検出が可能になります。グローバル クラスターは、vVols管理のために SVM ユーザーがローカルに追加されるマルチテナント 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 認証情報を持つローカル ストレージ バックエンドは、ONTAPツールのユーザー インターフェイスを通じて追加され、vCenter に制限されます。クラスタ認証情報をローカルで使用する場合、関連付けられた SVM は vCenter と自動的にマッピングされ、vVolsまたは VMFS を管理します。SRA を含む VMFS 管理の場合、ONTAPツールはグローバル クラスタを必要とせずに SVM 認証情報をサポートします。

Storage Replication Adapter (SRA)

SRA は、VMware Live Site Recovery アプライアンス内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。このアダプタにより、Storage Virtual Machine (SVM) レベルおよびクラスタ レベルの構成で、Site Recovery Manager とストレージ コントローラ間の通信が可能になります。

ストレージ仮想マシン (SVM)

SVM は、ONTAPにおけるマルチテナンシーの単位です。ハイパーバイザー上で実行される仮想マシンと同様に、SVM は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、データ ボリュームと、クライアントにデータを提供する 1 つ以上の LIF が含まれています。

均一な構成と非均一な構成

- 均一なホスト アクセス とは、2 つのサイトのホストが両方のサイトのストレージ クラスターへのすべてのパスに接続されていることを意味します。サイト間のパスは長距離にわたって伸びます。
- 非均一ホスト アクセス とは、各サイト内のホストが同じサイト内のクラスターにのみ接続されていることを意味します。サイト間パスと拡張パスは接続されません。



均一なホスト アクセスは、すべてのSnapMirrorアクティブ同期構成でサポートされます。不均一なホスト アクセスは、対称アクティブ / アクティブ構成でのみサポートされます。詳細はこちら ["ONTAPにおけるSnapMirrorアクティブ同期の概要"](#)。

Virtual Machine File System (VMFS)

VMFS は、VMware vSphere 環境で仮想マシン ファイルを保存するために設計されたクラスター化されたファイル システムです。

仮想ボリューム (vVols)

vVols は、仮想マシンで使用す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

VM ストレージ ポリシーは、vCenter Server のポリシーとプロファイルの下に作成されます。vVolsの場合、NetApp vVolsストレージ タイプ プロバイダーのルールを使用してルール セットを作成します。

VMware ライブサイトリカバリ

VMware Live Site Recovery (旧称 Site Recovery Manager (SRM)) は、VMware 仮想環境のビジネス継続性、災害復旧、サイト移行、および中断のないテスト機能を提供します。

VMware vSphere APIs for Storage Awareness (VASA)

VASA は、管理および運営のためにストレージ アレイを vCenter Server と統合する API セットです。アーキテクチャは、VMware vSphere とストレージ システム間の通信を処理する VASA プロバイダーを含む複数のコンポーネントに基づいています。

VMware vSphere ストレージ API - アレイ統合 (VAAI)

VAAI は、VMware vSphere ESXi ホストとストレージ デバイス間の通信を可能にする API セットです。API には、ホストがストレージ操作をアレイにオフロードするために使用する一連の基本操作が含まれています。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 Storage Cluster

vSphere Metro Storage Cluster (vMSC) は、ストレッチ クラスタ展開で vSphere を有効にして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) でサポートされています。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、お客様が選択した構成に基づいています。詳細はこちら ["VMware vSphere Metro ストレージ クラスタ"](#)。

vVolsデータストア

vVolsデータストアは、VASA プロバイダーによって作成および管理されるvVolsコンテナの論理データストア表現です。

RPOゼロ

RPO は目標復旧ポイントの略で、特定の時間内に許容できるとみなされるデータ損失の量です。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 アクセス制御

ONTAP tools for VMware vSphereについて学ぶ

ロールベース アクセス制御 (RBAC) は、組織内のリソースへのアクセスを制御するためのセキュリティ フレームワークです。RBAC は、個々のユーザーに承認を割り当てるのではなく、アクションを実行するための特定のレベルの権限を持つロールを定義することで管理を簡素化します。定義されたロールがユーザーに割り当てられるため、エラーのリスクが軽減され、組織全体のアクセス制御の管理が簡素化されます。

RBAC 標準モデルは、複雑さが増す複数の実装テクノロジーまたはフェーズで構成されています。その結果、実際の RBAC の展開は、ソフトウェア ベンダーとその顧客のニーズに基づいて、比較的単純なものから非常に複雑なものまで多岐にわたる可能性があります。

RBAC コンポーネント

大まかに言うと、すべての RBAC 実装に一般的に含まれるコンポーネントがいくつかあります。これらのコンポーネントは、承認プロセスの定義の一環として、さまざまな方法で結合されます。

権限

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

役割

ロール は、1 つ以上の権限を含むコンテナです。役割は通常、特定のタスクまたは職務機能に基づいて定義されます。ユーザーにロールが割り当てられると、そのロールに含まれるすべての権限がユーザーに付与されます。また、権限と同様に、実装には事前定義されたロールが含まれており、通常はカスタム ロールの作成も許可されます。

オブジェクト

オブジェクト は、RBAC 環境内で識別される実際のリソースまたは抽象リソースを表します。権限を通じて定義されたアクションは、関連付けられたオブジェクトに対して、または関連付けられたオブジェクトを使用して実行されます。実装に応じて、オブジェクト タイプまたは特定のオブジェクト インスタンスに権限を付与できます。

ユーザとグループ

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

権限

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

2つのRBAC環境

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

VMware vCenter Server

VMware vCenter Server の RBAC 実装は、vSphere Client ユーザー インターフェイスを通じて公開されるオブジェクトへのアクセスを制限するために使用されます。ONTAP tools for VMware vSphereのインストールの一環として、RBAC 環境が拡張され、ONTAPツールの機能を表す追加オブジェクトが含まれるようになります。これらのオブジェクトへのアクセスはリモートプラグインを通じて提供されます。["vCenter Server RBAC 環境"](#)詳細についてはこちらをご覧ください。

ONTAPクラスタ

ONTAP tools for VMware vSphereは、ONTAP REST API を介してONTAPクラスターに接続し、ストレージ関連の操作を実行します。ストレージ リソースへのアクセスは、認証時に提供されたONTAPユーザーに関連付けられたONTAPロールを通じて制御されます。見る["ONTAP RBAC環境"](#)詳細についてはこちらをご覧ください。

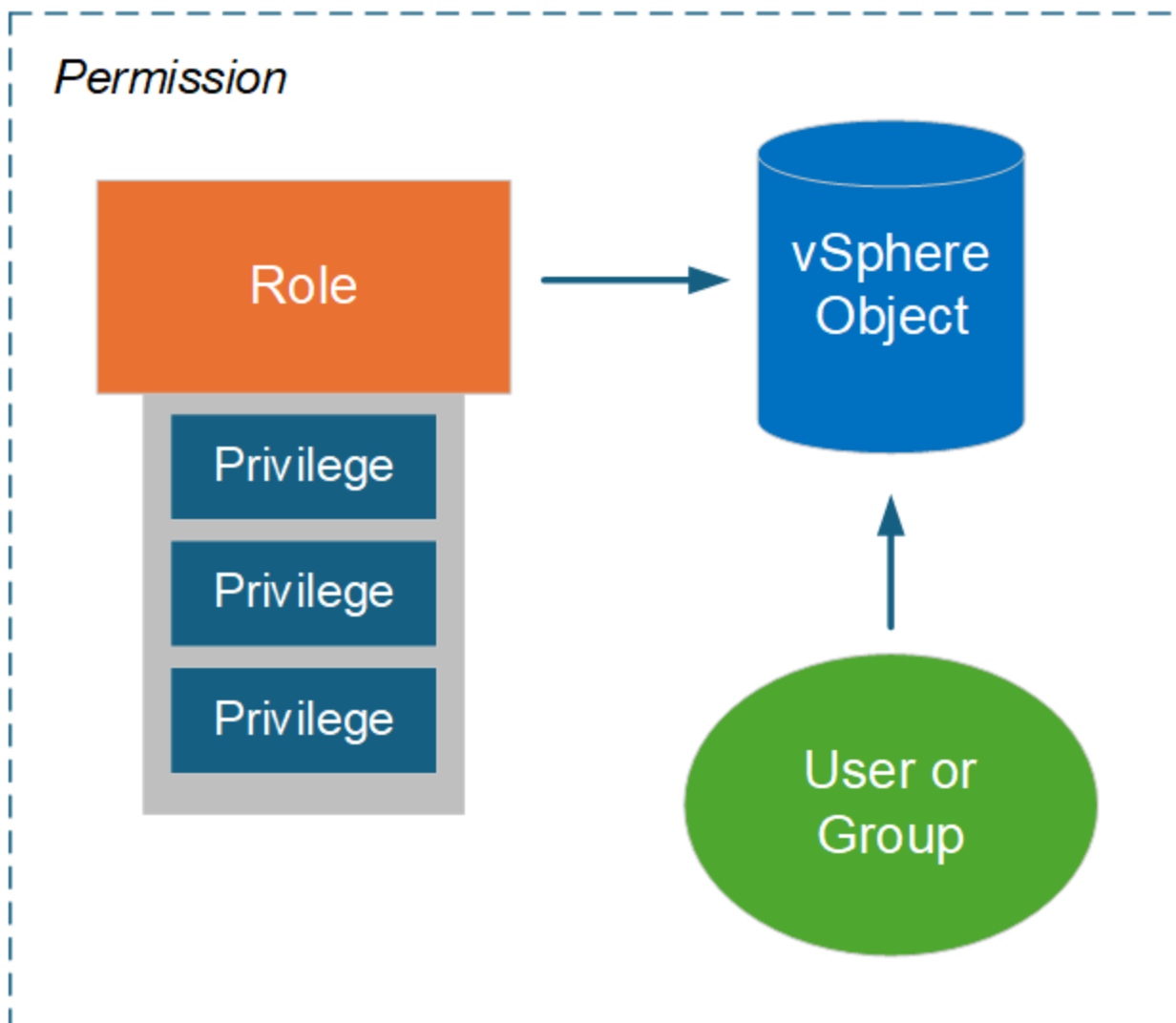
VMware vSphere を使用した RBAC

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

VMware vCenter Server は、vSphere オブジェクトへのアクセスを制御できる RBAC 機能を提供します。これは、vCenter の集中認証および承認セキュリティ サービスの重要な部分です。

vCenter Server 権限の図

権限は、vCenter Server 環境でアクセス制御を実施するための基盤です。これは、権限定義に含まれるユーザーまたはグループを持つ vSphere オブジェクトに適用されます。次の図に、vCenter 権限の概要を示します。



vCenter Server 権限のコンポーネント

vCenter Server 権限は、権限の作成時に結合される複数のコンポーネントのパッケージです。

vSphereオブジェクト

権限は、vCenter Server、ESXi ホスト、仮想マシン、データストア、データセンター、フォルダなどの vSphere オブジェクトに関連付けられます。オブジェクトに割り当てられた権限に基づいて、vCenter Server は各ユーザーまたはグループがオブジェクトに対して実行できるアクションまたはタスクを決定します。ONTAP tools for VMware vSphereに固有のタスクの場合、すべての権限は vCenter Server のルートまたはルート フォルダ レベルで割り当てられ、検証されます。見る["vCenter ServerでRBACを使用する"](#)詳細についてはこちらをご覧ください。

Privilegesと役割

ONTAP tools for VMware vSphereで使用する vSphere 権限には 2 種類あります。この環境での RBAC の操作を簡素化するために、ONTAPツールは必要なネイティブ権限とカスタム権限を含むロールを提供します。権限には以下が含まれます:

- vCenter Server標準の権限

これらは vCenter Server によって提供される権限です。

- ONTAP Tools固有の権限

これらは、ONTAP tools for VMware vSphereに固有のカスタム権限です。

ユーザとグループ

Active Directory またはローカルの vCenter Server インスタンスを使用して、ユーザーとグループを定義できます。ロールと組み合わせることで、vSphere オブジェクト階層内のオブジェクトに対する権限を作成できます。この権限は、関連付けられたロールの権限に基づいてアクセスを許可します。ロールはユーザーに直接個別に割り当てられるのではなく、ユーザーとグループは、vCenter Server のより広範な権限の一部として、ロール権限を通じてオブジェクトへのアクセスを取得します。

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

vCenter Server を使用したONTAP tools for VMware vSphereには、実稼働環境で使用する前に考慮すべきいくつかの側面があります。

vCenter のロールと管理者アカウント

vSphere オブジェクトおよび関連する管理タスクへのアクセスを制限する場合にのみ、カスタム vCenter Server ロールを定義して使用する必要があります。アクセスを制限する必要がない場合は、代わりに管理者アカウントを使用できます。各管理者アカウントは、オブジェクト階層の最上位レベルで管理者ロールを使用して定義されます。これにより、ONTAP tools for VMware vSphereによって追加されたオブジェクトを含む vSphere オブジェクトへのフル アクセスが提供されます。

vSphere オブジェクト階層

vSphere オブジェクト インベントリは階層的に編成されます。たとえば、次のように階層を下に移動できます。

vCenter Server → Datacenter → Cluster → ESXi host → Virtual Machine

VAAI プラグイン操作を除くすべての権限は、vSphere オブジェクト階層で検証されます。VAAI プラグイン操

作は、ターゲット ESXi ホストに対して検証されます。

ONTAP tools for VMware vSphereに含まれるロール

vCenter Server RBAC での作業を簡素化するために、ONTAP tools for VMware vSphereでは、さまざまな管理タスクに合わせて事前定義されたロールが提供されます。



必要に応じて新しいカスタム ロールを作成できます。この場合、既存のONTAPツール ロールの 1 つを複製し、必要に応じて編集する必要があります。構成を変更した後、影響を受ける vSphere クライアント ユーザーは、変更を有効にするためにログアウトして再度ログインする必要があります。

ONTAP tools for VMware vSphereを表示するには、vSphere Client の上部にある メニュー を選択し、左側の 管理 をクリックしてから ロール をクリックします。以下に説明する 3 つの定義済みロールがあります。

VMware vSphere 管理者向けNetApp ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphereを実行するために必要な、すべてのネイティブ vCenter Server 権限とONTAPツール固有の権限を提供します。

ONTAP tools for VMware vSphereNetApp ONTAP ツール（読み取り専用）

ONTAP Toolsに対する読み取り専用アクセスが許可されます。これらのユーザーは、アクセス制御されているONTAP tools for VMware vSphereを実行できません。

VMware vSphere プロビジョニング用のNetApp ONTAP tools for VMware vSphere

ストレージのプロビジョニングに必要なネイティブ vCenter Server 権限とONTAPツール固有の権限の一部を提供します。次のタスクを実行できます。

- 新しいデータストアの作成
- データストアの管理

vSphere オブジェクトとONTAPストレージ バックエンド

2 つの RBAC 環境が連携して動作します。vSphere クライアント インターフェイスでタスクを実行する場合、最初に vCenter Server に定義されているONTAPツール ロールがチェックされます。操作が vSphere によって許可されている場合は、ONTAPロールの権限が検査されます。この 2 番目の手順は、ストレージ バックエンドが作成および構成されたときにユーザーに割り当てられたONTAPロールに基づいて実行されます。

vCenter Server RBAC の操作

vCenter Server の権限とアクセス許可を操作する際に考慮すべき点があります。

必要な権限

ONTAP tools for VMware vSphereにアクセスするには、ONTAPツール固有の View 権限が必要です。この権限なしで vSphere にサインインしてNetAppアイコンをクリックすると、ONTAP tools for VMware vSphereエラー メッセージが表示され、ユーザー インターフェイスにアクセスできなくなります。

vSphere オブジェクト階層内の割り当てレベルによって、アクセスできるユーザー インターフェイスの部分が決まります。ルート オブジェクトに表示権限を割り当てると、NetAppアイコンをクリックしてONTAP tools for VMware vSphereにアクセスできるようになります。

代わりに、別の下位の vSphere オブジェクト レベルに表示権限を割り当てることもできます。ただし、これにより、アクセスして使用できるONTAP tools for VMware vSphereが制限されます。

アクセス許可の割り当て

vSphere オブジェクトおよびタスクへのアクセスを制限する場合は、vCenter Server 権限を使用する必要があります。vSphere オブジェクト階層内で権限を割り当てる場所によって、ユーザーが実行できるONTAP tools for VMware vSphereが決まります。



より制限的なアクセスを定義する必要がない限り、通常はルート オブジェクトまたはルート フォルダー レベルで権限を割り当てることをお勧めします。

ONTAP tools for VMware vSphereで利用できる権限は、ストレージ システムなどの vSphere 以外のカスタム オブジェクトに適用されます。割り当てることができる vSphere オブジェクトがないため、可能であれば、これらの権限をONTAP tools for VMware vSphereに割り当てる必要があります。たとえば、ONTAP tools for VMware vSphereの「ストレージ システムの追加/変更/削除」権限を含むすべての権限は、ルート オブジェクト レベルで割り当てる必要があります。

オブジェクト階層の上位レベルで権限を定義する場合、その権限が子オブジェクトに渡され継承されるように構成できます。必要に応じて、親から継承した権限を上書きする追加の権限を子オブジェクトに割り当てることができます。

権限はいつでも変更できます。権限内のいずれかの権限を変更する場合、その権限に関連付けられているユーザーは vSphere からログアウトし、再度ログインして変更を有効にする必要があります。

ONTAPを使用した RBAC

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

ONTAP は、堅牢で拡張可能な RBAC 環境を提供します。RBAC 機能を使用すると、REST API および CLI を通じて公開されるストレージおよびシステム操作へのアクセスを制御できます。ONTAP tools for VMware vSphereを使用する前に、環境をよく理解しておくことで役立ちます。

管理オプションの概要

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



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

役割と権限の種類

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

- REST

REST ロールはONTAP 9.6 で導入され、通常は REST API を介してONTAPにアクセスするユーザーに適用されます。これらのロールに含まれる権限は、ONTAP REST API エンドポイントおよび関連するアクションへのアクセスの観点から定義されます。

- 伝統的

これらは、ONTAP 9.6 より前に含まれていたレガシー ロールです。これらは引き続き RBAC の基本的な側面です。権限は、ONTAP CLI コマンドへのアクセスの観点から定義されます。

REST ロールは最近導入されましたが、従来のロールにもいくつかの利点があります。たとえば、追加のクエリ パラメータをオプションで含めることができるため、権限が適用されるオブジェクトがより正確に定義されます。

Scope

ONTAPロールは、2つの異なるスコープのいずれかで定義できます。これらは、特定のデータ SVM (SVM レベル) またはONTAPクラスタ全体 (クラスタ レベル) に適用できます。

役割の定義

ONTAP は、クラスタ レベルと SVM レベルの両方で事前定義されたロールのセットを提供します。カスタムロールを定義することもできます。

ONTAP RESTロールの操作

ONTAP tools for VMware vSphereに含まれているONTAP REST ロールを使用する場合は、いくつかの考慮事項があります。

役割マッピング

従来のロールを使用する場合でも、REST ロールを使用する場合でも、すべてのONTAPアクセスの決定は、基盤となる CLI コマンドに基づいて行われます。ただし、REST ロールの権限は REST API エンドポイントに基づいて定義されるため、ONTAP は各 REST ロールに対してマップされた従来のロールを作成する必要があります。したがって、各 REST ロールは、基礎となる従来のロールにマッピングされます。これにより、ONTAP はロールの種類に関係なく、一貫した方法でアクセス制御の決定を行うことができます。並列にマップされたロールを変更することはできません。

CLI権限を使用してRESTロールを定義する

ONTAP は常に CLI コマンドを使用して基本レベルでのアクセスを決定するため、REST エンドポイントではなく CLI コマンド権限を使用して REST ロールを表現することができます。このアプローチの利点の1つは、従来のロールで利用できる追加の粒度です。

ONTAPロールを定義する際の管理インターフェース

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

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

ONTAPを使用したONTAP tools for VMware vSphereには、実稼働環境で使用する前に考慮すべきいくつかの側面があります。

構成プロセスの概要

ONTAP tools for VMware vSphereには、カスタム ロールを持つONTAPユーザーの作成のサポートが含まれています。定義は、ONTAPクラスターにアップロードできる JSON ファイルにパッケージ化されています。ユーザーを作成し、環境とセキュリティのニーズに合わせてロールをカスタマイズできます。

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

1. 準備

ONTAPツール マネージャーとONTAPクラスターの両方の管理者資格情報が必要です。

2. JSON定義ファイルをダウンロードする

ONTAP Tools Manager ユーザー インターフェイスにサインインした後、RBAC 定義を含む JSON ファイルをダウンロードできます。

3. ロールを持つONTAPユーザーを作成する

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

1. 左側の*クラスター*を選択し、次に*設定*を選択します。
2. *ユーザーとロール*までスクロールしてクリックします →。
3. *ユーザー*の下に*追加*を選択し、*仮想化製品*を選択します。
4. ローカルワークステーション上の JSON ファイルを選択し、アップロードします。

4. 役割を構成する

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

システムマネージャを使用してロールを構成する

System Manager を使用して新しいユーザーとロールの作成を開始し、JSON ファイルをアップロードしたら、環境とニーズに応じてロールをカスタマイズできます。

コアユーザーとロールの構成

RBAC 定義は、VSC、VASA プロバイダー、SRA の組み合わせを含む複数の製品機能としてパッケージ化されています。RBAC サポートが必要な環境を選択する必要があります。たとえば、ロールでリモート プラグイン機能をサポートする場合は、VSC を選択します。ユーザー名と関連するパスワードも選択する必要があります。

権限

ロール権限は、ONTAPストレージに必要なアクセス レベルに基づいて 4 つのセットに分類されます。ロールのベースとなる権限は次のとおりです。

- Discovery

ストレージ システムを追加できます。

- ストレージの作成

ストレージを作成できます。また、検出ロールに関連付けられているすべての権限も含まれます。

- ストレージを変更する

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

- ストレージを破壊する

ストレージを破壊できます。また、検出、ストレージの作成、ストレージ ロールの変更に関連するすべての権限も含まれます。

ロールを持つユーザーを生成する

環境の設定オプションを選択したら、[追加] をクリックすると、ONTAPによってユーザーとロールが作成されます。生成されたロールの名前は、次の値の連結になります。

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

例

OTV_10_VSC_Discovery_Create

新しいユーザーは、「ユーザーとロール」 ページのリストに追加されます。HTTP と ONTAPI の両方のユーザー ログイン方法がサポートされていることに注意してください。

ONTAP tools for VMware vSphereの高可用性

ONTAP tools for VMware vSphere は、高可用性 (HA) 構成をサポートしており、障害発生時にONTAP tools for VMware vSphereの機能が中断されることなく提供されるようになります。

高可用性 (HA) ソリューションは、次の原因でシステムが停止した場合に迅速なリカバリを提供します。

- ホストの障害



単一ノード障害のみがサポートされます。

- ネットワークの障害
- 仮想マシンの障害 (ゲストOSの障害)
- アプリケーション (ONTAP Tools) のクラッシュ

ONTAP tools for VMware vSphereで高可用性 (HA) を実現するために追加の構成は必要ありません。



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

HA 機能を有効にするには、導入時またはその後のONTAP tools for VMware vSphereで、CPU ホット アド とメモリ ホット プラグを有効にする必要があります。

ONTAP ツール マネージャのユーザーインターフェース

ONTAP tools for VMware vSphereは、複数の vCenter Server インスタンスを管理できる マルチテナント システムです。ONTAP ツール マネージャーは、管理対象 vCenter Server インスタンスとオンボード ストレージ バックエンドに対するONTAP tools for VMware vSphere管理者のより詳細な制御機能を提供します。

ONTAP ツール マネージャーは次のことに役立ちます。

- vCenter Server インスタンス管理 - ONTAP ツールに vCenter Server インスタンスを追加および管理します。
- ストレージ バックエンド管理 - ONTAP ストレージ クラスターをONTAP tools for VMware vSphereに追加して管理し、オンボードされた vCenter Server インスタンスにグローバルにマッピングします。
- ログ バンドルのダウンロード - ONTAP tools for VMware vSphereのログ ファイルを収集します。
- 証明書管理 - 自己署名証明書をカスタム CA 証明書に変更し、VASA プロバイダーおよびONTAP ツールのすべての証明書を更新またはリフレッシュします。
- パスワード管理 - ユーザーの OVA アプリケーション パスワードをリセットします。

ONTAP ツール マネージャにアクセスするには、`https://<ONTAPtoolsIP>:8443/virtualization/ui/` ブラウザから、導入時に指定したONTAP tools for VMware vSphere管理者の認証情報を使用してログインします。

ONTAP ツール マネージャの概要セクションは、サービス管理、ノード サイズの拡大、高可用性 (HA) の有効化などのアプライアンス構成の管理に役立ちます。また、健全性、ネットワークの詳細、アラートなど、ノードに関連するONTAP ツールの全体的な情報を監視することもできます。

ONTAP tools Manager

Overview | EDIT APPLIANCE SETTINGS

Appliance

Size: Small
HA: Enabled
VASA provider: Enabled
SRA: Enabled

Healthy

VIEW DETAILS

Alerts (Last 24 hours)

Error 3, Warning 2, Info 5

VIEW ALL ALERTS (43)

ONTAP tools nodes

nodename_01: Online, demo_vm1
nodename_02: Online, demo_vm2
nodename_03: Online, demo_vm3

VIEW DETAILS (for each node)

カード	説明
家電カード	アプライアンス カードは、ONTAPツール アプライアンスの全体的なステータスを提供します。アプライアンスの構成の詳細と有効なサービスのステータスが表示されます。ONTAPツール アプライアンスの追加情報については、[詳細を表示] リンクを選択してください。アプライアンス設定アクション ジョブの編集が進行中の場合、アプライアンス ポートレットにジョブのステータスと詳細が表示されます。
アラートカード	アラート カードには、HA ノード レベルのアラートを含む、ONTAPツールのアラートがタイプ別にリストされます。カウントテキスト (ハイパーリンク) を選択すると、アラートのリストを表示できます。リンクをクリックすると、選択したタイプでフィルタリングされたアラート表示ページに移動します。
vCenter	vCenter カードには、システム内の vCenter の健全性状態が表示されます。
ストレージバックエンド	ストレージ バックエンド カードには、システム内のストレージ バックエンドの正常性状態が表示されます。
ONTAPツールノードカード	ONTAPツール ノード カードには、ノード名、ノード VM 名、ステータス、およびすべてのネットワーク関連データを含むノードのリストが表示されます。*詳細を表示*を選択すると、選択したノードに関連する追加の詳細を表示できます。[注意] 非 HA セットアップでは、1つのノードのみが表示されます。HA セットアップでは、3つのノードが表示されます。

ONTAP tools for VMware vSphereを導入する

ONTAP tools for VMware vSphereのクイック スタート

このクイック スタート セクションで、ONTAP tools for VMware vSphereをセットアップします。

最初に、NFS および VMFS データストアをサポートするコア サービスを提供する小規模な単一ノード構成として、ONTAP tools for VMware vSphereを展開します。vVolsデータストアと高可用性 (HA) を使用するために構成を拡張する必要がある場合は、このワークフローを完了した後に拡張します。詳細については、["HA 導入ワークフロー"](#)。

1

展開を計画する

vSphere、ONTAP、ESXiホストのバージョンがONTAPツールのバージョンと互換性があることを確認してください。十分なCPU、メモリ、ディスク容量を割り当ててください。セキュリティルールによっては、ネットワークトラフィックを許可するためにファイアウォールなどのセキュリティツールを設定する必要がある場合があります。

vCenter Server がインストールされ、アクセス可能であることを確認します。

- ["Interoperability Matrix Tool"](#)
- ["ONTAP tools for VMware vSphere"](#)
- ["始める前に"](#)

2

ONTAP tools for VMware vSphereを導入する

まず、ONTAP tools for VMware vSphereを、NFS および VMFS データストアをサポートするコアサービスを提供する小規模なシングルノード構成として導入します。vVolsデータvVolsと高可用性 (HA) を使用するように構成を拡張する予定がある場合は、このワークフローを完了した後に拡張してください。HA構成に拡張するには、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てください。

- ["ONTAP tools for VMware vSphereを導入する"](#)

3

vCenter Serverインスタンスを追加する

ONTAP tools for VMware vSphereに vCenter Server インスタンスを追加して、vCenter Server 環境内の仮想データストアを構成、管理、保護します。

- ["vCenter Serverインスタンスを追加する"](#)

4

ONTAPユーザーの役割と権限を構成する

ONTAP tools for VMware vSphere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ー ロールと権限を構成します。

- ["ONTAPユーザーの役割と権限を構成する"](#)

5

ストレージバックエンドを構成する

ONTAPクラスターにストレージ バックエンドを追加します。vCenter が関連付けられた SVM を持つテナントとして機能するマルチテナント設定の場合は、ONTAPツール マネージャを使用してクラスタを追加します。ストレージ バックエンドを vCenter Server に関連付けて、オンボードされた vCenter Server インスタンスにグローバルにマップします。

ONTAPツールのユーザー インターフェイスを使用して、クラスタまたは SVM 認証情報を持つローカル ストレージ バックエンドを追加します。これらのストレージ バックエンドは、単一の vCenter に制限されます。クラスタ認証情報をローカルで使用する場合、関連付けられた SVM は自動的に vCenter にマッピングされ、vVolsまたは VMFS を管理します。SRA を含む VMFS 管理の場合、ONTAPツールはグローバル クラスタを必要とせずに SVM 認証情報をサポートします。

- ["ストレージバックエンドを追加する"](#)
- ["ストレージバックエンドをvCenter Serverインスタンスに関連付ける"](#)

6

複数の vCenter Server インスタンスを使用している場合は証明書をアップグレードします

複数の vCenter Server インスタンスで作業する場合は、自己署名証明書を証明機関 (CA) 署名証明書にアップグレードします。

- ["証明書の管理"](#)

7

(オプション) SRA保護を構成する

SRA 機能を有効にして災害復旧を構成し、NFS または VMFS データストアを保護します。

- ["ONTAP tools for VMware vSphereを有効にする"](#)
- ["VMware Live Site RecoveryアプライアンスでSRAを構成する"](#)

8

(オプション) SnapMirrorアクティブ同期保護を有効にする

SnapMirrorアクティブ同期のホスト クラスタ保護を管理するには、ONTAP tools for VMware vSphereを構成します。SnapMirrorアクティブ同期を使用するには、ONTAPシステムでONTAPクラスタと SVM ピアリングを実行します。これは VMFS データストアにのみ適用されます。

- ["ホストクラスタ保護を使用して保護する"](#)

9

ONTAP tools for VMware vSphereのバックアップとリカバリを設定する

障害発生時にセットアップを回復するために使用できる、ONTAP tools for VMware vSphereのバックアップをスケジュールします。

- ["ONTAPツールのセットアップのバックアップを作成し、復元する"](#)

高可用性 (HA) 展開ワークフロー

vVolsデータストアを使用している場合は、ONTAPツールの初期導入を高可用性 (HA) 構成に拡張し、VASA プロバイダ サービスを有効にする必要があります。

1

展開を拡大する

ONTAP tools for VMware vSphereをスケールアップして、展開内のノードの数を増やし、構成を HA セットアップに変更できます。

- ["ONTAP tools for VMware vSphereを変更する"](#)

2

サービスを有効にする

vVolsデータストアを構成するには、VASA プロバイダー サービスを有効にする必要があります。VASA プロバイダーを vCenter に登録し、適切なネットワークとストレージの構成を含むストレージ ポリシーが HA 要件を満たしていることを確認します。

SRA サービスを有効にして、VMware Site Recovery Manager (SRM) または VMware Live Site Recovery (VLSR) 用のONTAPツール ストレージ レプリケーション アダプタ (SRA) を使用します。

- ["VASAプロバイダーとSRAサービスを有効にする"](#)

3

証明書をアップグレードする

複数の vCenter Server インスタンスで vVol データストアを使用している場合は、自己署名証明書を証明機関 (CA) 署名証明書にアップグレードします。

- ["証明書の管理"](#)

ONTAP tools for VMware vSphere

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について理解しておく必要があります。

VMware vCenter Server Virtual Appliance (vCSA) では、ONTAP tools for VMware vSphereを使用できます。ESXi システムを含むサポートされている vSphere クライアントに、ONTAP tools for VMware vSphereを展開する必要があります。

システム要件

- 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
 - 15GB - シンプルビジョニングの場合
 - 348GB - シックプロビジョニングの場合
- ホスト システムのサイズ要件 展開のサイズに応じて推奨されるメモリは以下の表のとおりです。高可用性 (HA) を展開するには、表に指定されているアプライアンス サイズの 3 倍が必要になります。

展開の種類	ノードあたりのCPU数	ノードあたりのメモリ (GB)	ノードあたりのシックプロビジョニングされたディスク容量 (GB)
小規模	9	18	350
中	13	26	350
大規模注: 大規模展開は HA 構成専用です。	17	34	350



バックアップを有効にすると、各ONTAPツール クラスターには、VM が展開されるデータストア上にさらに 50 GB のスペースが必要になります。したがって、非 HA では 400 GB、HA では合計 1100 GB のスペースが必要になります。

最低限のストレージとアプリケーションの要件

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	9.14.1、9.15.1、9.16.0、9.16.1、および 9.16.1P3 FAS、ASAA シリーズ、ASA C シリーズ、AFF A シリーズ、AFF C シリーズ、およびASA r2。
ONTAPツールがサポートするESXiホスト	7.0.3以降
ONTAPツールはvCenter Serverでサポートされています	7.0U3以降
VASA Provider	3.0
OVAアプリケーション	10.4
ONTAPツール仮想マシンを展開するためのESXiホスト	7.0U3と8.0U3
ONTAPツール仮想マシンを展開するためのvCenter Server	7.0と8.0



ONTAP tools for VMware vSphere以降、仮想マシンのハードウェアがバージョン 10 から 17 に変更されます。

相互運用性マトリックス ツール (IMT) には、サポートされている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に関する最新情報が含まれています。

["Interoperability Matrix Tool"](#)

ポート要件

以下の表は、NetAppが使用するネットワーク ポートとその用途の概要を示しています。システム内で適切な動作と通信を行うために、これらのポートが開いていてアクセス可能であることを確認してください。関連サービスが正しく機能するために、これらのポートのトラフィックを許可するために必要なネットワーク構成が整っていることを確認してください。セキュリティ ポリシーによっては、ネットワーク内でこれらのトラフィックを許可するようにファイアウォールやその他のセキュリティ アプライアンスを設定する必要がある場合があります。

ポート	プロトコル	説明
8143	TCP	ONTAPツールの HTTP/HTTPS 接続。
8043	TCP	ONTAPツールの HTTP/HTTPS 接続。
9060	TCP	ONTAPツールの HTTP/HTTPS 接続。
22	TCP	Ansible は、クラスターのプロビジョニング中に通信にこの SSH ポートを使用します。このポートは、メンテナンス ユーザーのパスワードやステータス メッセージの変更、HA 構成の場合の 3 つのノードすべての値の更新などの機能に必要です。
443	TCP	これは、VASA プロバイダー サービスの着信通信用のパススルー ポートです。VASA プロバイダーの自己署名証明書とカスタム CA 証明書はこのポートでホストされます。
8443	TCP	このポートは、Swagger および Manager ユーザー インターフェイス アプリケーションを通じて API ドキュメントをホストします。
2379	TCP	これは、etcd キー値ストア内のキーの取得、配置、削除、監視などのクライアント要求のデフォルトポートです。
2380	TCP	これは、etcd がデータの複製と一貫性のために依存している raft コンセンサス アルゴリズムに使用される etcd クラスターのサーバー間通信のデフォルト ポートです。
7472	TCP/UDP	これは Prometheus メトリック サービス ポートです。
7946	TCP/UDP	このポートは、Docker のコンテナネットワーク検出に使用されます。
9083	TCP	このポートは、VASA プロバイダー サービスの内部で使用されるサービス ポートです。
1162	UDP	これは SNMP トラップ パケット ポートです。
6443	TCP	ソース: RKE2 エージェント ノード。宛先: REK2 サーバー ノード。 説明: Kubernetes API

9345	TCP	ソース: RKE2 エージェント ノード。宛先: REK2 サーバー ノード。説明: REK2 スーパーバイザー API
8472	TCP+UDP	フランネル VXLAN を使用する場 合、すべてのノードが UDP ポート 8472 を介して他のノードにアクセ スする必要があります。ソース: すべての RKE2 ノード。宛先: すべ ての REK2 ノード。説明: VXLAN を使用した Canal CNl
10250	TCP	ソース: すべての RKE2 ノード。宛 先: すべての REK2 ノード。説明: Kubelet メトリクス
30000-32767	TCP	ソース: すべての RKE2 ノード。宛 先: すべての REK2 ノード。説明: NodePort ポート範囲
123	TCP	Ntpd はこのポートを使用して NTP サーバーの検証を実行します。
137-139	TCP/UDP	SMB/Windows 共有パケット。
6789	TCP	Ceph モニター (MON)
3300	TCP	Ceph モニター (MON)
6800-7300	TCP	Ceph マネージャー、OSD、および ファイルシステム (MDS)。
80	TCP	Ceph RADOS ゲートウェイ (RGW)
9080	TCP	VP HTTP/HTTPS 接続 (IPv4 の場 合は 127.0.0.0/8、IPv6 の場合は ::1/128 からのみ)。

ONTAP tools for VMware vSphereを導入するための構成制限

次の表をガイドとして使用して、ONTAP tools for VMware vSphereを構成することができます。

展開	タイプ	* vVolsの数*	ホスト数
HA 認定外	小 (S)	約12K	32
HA 認定外	ミディアム (M)	約24K	64
高可用性	小 (S)	約24K	64
高可用性	ミディアム (M)	約5万	128
高可用性	ラージ (L)	約10万	256 [注意] 表内のホストの 数は、複数の vCenter から のホストの合計数を示 しています。

ONTAP tools for VMware vSphere- ストレージ レプリケーション アダプタ (SRA)

次の表は、ONTAP tools for VMware vSphereを使用して VMware Live Site Recovery インスタンスごとにサポートされる数を示しています。

vCenter 展開サイズ	小さい	中くらい
アレイベースのレプリケーションを使用して保護するように構成された仮想マシンの合計数	2000	5000
アレイベースのレプリケーション保護グループの合計数	250	250
復旧計画ごとの保護グループの合計数	50	50
複製されたデータストアの数	255	255
VM 数	4000	7000

次の表は、ONTAP tools for VMware vSphereを示しています。

VMware Live Site Recovery インスタンスの数	* ONTAPツールの導入サイズ*
最大4	小規模
4～8	中
8以上	大規模

<https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0/overview/site-recovery-manager-system-requirements/operational-limits-of-site-recovery-manager.html> ["VMware Live Site Recovery の運用上の制限"]。

始める前に...

展開を続行する前に、次の要件が満たされていることを確認してください。

要件	あなたのステータス
vSphere バージョン、ONTAPバージョン、ESXi ホストバージョンは、ONTAP ツール バージョンと互換性があります。	☐ はい ☐ いいえ
vCenter Server環境がセットアップされ構成されている	☐ はい ☐ いいえ
ブラウザのキャッシュが削除されました	☐ はい ☐ いいえ
親vCenter Serverの認証情報を持っている	☐ はい ☐ いいえ

要件	あなたのステータス
ONTAP tools for VMware vSphereが導入後に登録のために接続する vCenter Server インスタンスのログイン認証情報を持っていること	☐ はい ☐ いいえ
証明書が発行されるドメイン名は、カスタム CA 証明書が必須であるマルチ vCenter 展開内の仮想 IP アドレスにマッピングされます。	☐ はい ☐ いいえ
ドメイン名に対して nslookup チェックを実行し、ドメインが意図した IP アドレスに解決されているかどうかを確認します。	☐ はい ☐ いいえ
証明書は、ドメイン名とONTAPツールの IP アドレスを使用して作成されます。	☐ はい ☐ いいえ
ONTAPツール アプリケーションと内部サービスは、vCenter Server からアクセスできます。	☐ はい ☐ いいえ
マルチテナント SVM を使用する場合、各 SVM に SVM 管理 LIF が存在します。	☐ はい ☐ いいえ

展開ワークシート

単一ノード展開の場合

次のワークシートを使用して、ONTAP tools for VMware vSphereに必要な情報を収集します。

要件	あなたの価値
ONTAPツール アプリケーションの IP アドレス。これは、ONTAPツールのWebインターフェースにアクセスするためのIPアドレスです。	
内部通信用のONTAPツール仮想 IP アドレス。この IP アドレスは、複数のONTAPツール インスタンスを含むセットアップでの内部通信に使用されます。この IP アドレスは、ONTAPツール アプリケーションの IP アドレスと同じにしないでください。	
最初のノードのDNSホスト名	
プライマリDNSサーバー	
セカンダリDNSサーバー	
DNS検索ドメイン	
最初のノードの IPv4 アドレス。これは、管理ネットワーク上のノード管理インターフェイスの一意の IPv4 アドレスです。	
IPv4アドレスのサブネットマスク	
IPv4アドレスのデフォルトゲートウェイ	
IPv6アドレス（オプション）	
IPv6プレフィックス長（オプション）	

要件	あなたの価値
IPv6 アドレスのゲートウェイ (オプション)	



上記のすべての IP アドレスの DNS レコードを作成します。ホスト名を割り当てる前に、それらを DNS 上の空いている IP アドレスにマッピングします。すべての IP アドレスは、展開用に選択された同じ VLAN 上にある必要があります。

高可用性 (HA) 展開の場合

単一ノードの展開要件に加えて、HA 展開には次の情報が必要です。

要件	あなたの価値
プライマリDNSサーバー	
セカンダリDNSサーバー	
DNS検索ドメイン	
2番目のノードのDNSホスト名	
2番目のノードのIPアドレス	
3番目のノードのDNSホスト名	
3番目のノードのIPアドレス	

ネットワークファイアウォールの構成

ネットワーク ファイアウォールで IP アドレスに必要なポートを開きます。ONTAPツールはポート 443 を介してこの LIF にアクセスできる必要があります。参照["ポート要件"最新情報](#)については。

ONTAPストレージ設定

ONTAPストレージとONTAP tools for VMware vSphereとのシームレスな統合を確保するには、次の設定を考慮してください。

- ストレージ接続にファイバ チャネル (FC) を使用している場合は、FC スイッチのゾーニングを構成して、ESXi ホストを SVM の FC LIF に接続します。 ["ONTAPシステムによる FC および FCoE ゾーニングについて学習します"](#)
- ONTAPツールで管理されるSnapMirrorレプリケーションを使用するには、ONTAPストレージ管理者は ["ONTAPクラスタピア関係"](#)そして ["ONTAPクラスタ間 SVM ピア関係"](#)SnapMirrorを使用する前に、ONTAPで。

ONTAP tools for VMware vSphereを導入する

ONTAP tools for VMware vSphereは、NFSおよびVMFSデータストアをサポートするコアサービスを備えた小規模な単一ノードとして導入されます。ONTAPONTAPの導入プロセスには最大45分かかる場合があります。

開始する前に

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、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デプロイメントは、ネットワーク接続に依存しないため、シームレスなエクスペリエンスを実現します。



クラスター内のすべてのホストがアクセスできるように、コンテンツ ライブラリを共有データストアに保存する必要があります。アプライアンスを HA 構成にする前に、OVA を保存するためのコンテンツ ライブラリを作成します。デプロイ後にコンテンツ ライブラリ テンプレートを削除しないでください。



後で HA 展開を有効にするには、ONTAP ツールをホストする仮想マシンを ESXi ホストに直接展開しないでください。代わりにクラスターまたはリソース プールにデプロイします。

コンテンツ ライブラリがない場合は、次の手順に従って作成してください。

コンテンツ ライブラリの作成 小規模な単一ノード展開のみを使用する予定の場合は、コンテンツ ライブラリを作成する必要はありません。

1. ONTAP tools for VMware vSphere のバイナリ (.ova) と署名付き証明書を含むファイルを次の場所からダウンロードします。 ["NetApp サポート サイト"](#)。
2. vSphere クライアントにログインする
3. vSphere クライアント メニューを選択し、コンテンツ ライブラリ を選択します。
4. ページの右側にある*作成*を選択します。
5. ライブラリの名前を指定して、コンテンツ ライブラリを作成します。
6. 作成したコンテンツ ライブラリに移動します。
7. ページの右側にある*アクション*を選択し、*アイテムのインポート*を選択して、OVA ファイルをインポートします。



詳細については、 ["コンテンツライブラリの作成と使用"](#) ブログ。



デプロイメントを続行する前に、インベントリ上のクラスターの分散リソース スケジューラ (DRS) を「保守的」に設定します。これにより、インストール中に VM が移行されないようになります。

ONTAP tools for VMware vSphere は、最初は非 HA セットアップとして導入されます。HA 展開に拡張するには、CPU ホット プラグとメモリ ホット プラグインを有効にする必要があります。この手順は、デプロイメント プロセスの一部として実行することも、デプロイメント後に VM 設定を編集することもできます。

手順

1. ONTAP tools for VMware vSphere のバイナリ (.ova) と署名済み証明書が含まれているファイルをからダウンロードします ["NetApp サポート サイト"](#)。OVA をコンテンツ ライブラリにインポートした場合は、この手順をスキップして次の手順に進むことができます
2. vSphere サーバーにログインします。
3. OVA を展開するリソース プール、クラスター、またはホストに移動します。



ONTAP tools for VMware vSphere を、管理する vVols データストアに保存しないでください。

4. OVA は、コンテンツ ライブラリまたはローカル システムから展開できます。

ローカルシステムから	コンテンツライブラリから
a. 右クリックして、[OVF テンプレートのデプロイ...] を選択します。b. URL から OVA ファイルを選択するか、その場所を参照して、[次へ] を選択します。	a. コンテンツライブラリに移動し、展開するライブラリ項目を選択します。b. [アクション] > [このテンプレートから新しいVMを作成] を選択します。

5. 名前とフォルダを選択 フィールドに仮想マシンの名前を入力し、その場所を選択します。

- vCenter Server 8.0.3 バージョンを使用している場合は、[この仮想マシンのハードウェアをカスタマイズする] オプションを選択します。これにより、[完了の準備完了] ウィンドウに進む前に、[ハードウェアのカスタマイズ] という追加の手順がアクティブになります。
- vCenter Server 7.0.3 バージョンを使用している場合は、デプロイの最後にある「次の手順」セクションの手順に従ってください。

netapp-ontap-tools-for-vmware-vsphere-10.4-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder
- 4 Select a compute resource
- 5 Review details
- 6 Select storage
- 7 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: demo01v

Select a location for the virtual machine.

vcf-vc01.ontappmtme.openenglab.netapp.com
> Raleigh

- ☐ Customize the operating system
- ☐ Customize this virtual machine's hardware

CANCEL

BACK

NEXT

6. コンピュータ リソースを選択し、[次へ] を選択します。オプションで、デプロイされた **VM** を自動的にパワーオンする のボックスをオンにします。

7. テンプレートの詳細を確認し、[次へ] を選択します。

8. ライセンス契約を読んで同意し、[次へ] を選択します。

9. 構成のストレージとディスク フォーマットを選択し、[次へ] を選択します。
10. 各ソース ネットワークの宛先ネットワークを選択し、[次へ] を選択します。
11. *テンプレートのカスタマイズ*ウィンドウで、必須フィールドに入力し、*次へ*を選択します。

netapp-ontap-tools-for-vmware-vsphere-10.4-1743069300 - New Virtual Machine from Content Library

- 1 Select a name and folder
- 2 Select a compute resource
- 3 Review details
- 4 License agreements
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

Customize template ✕

NTP Servers	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware tools based time synchronization will be used
▼ Deployment Configuration 2 settings	
ONTAP tools IP address*	This will be the primary interface for communication with ONTAP tools
ONTAP tools virtual IP address*	ONTAP tools uses this IP address for internal communication
▼ Node Configuration 10 settings	
HostName*	
Primary DNS*	
Secondary DNS*	
Search domains*	Specify the search domain name to use when resolving the hostname
IPv4 address*	
IPv4 subnet mask*	

CANCEL
BACK
NEXT

- 情報はインストール中に検証されます。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、修正するように求められます。
- ホスト名には、文字 (AZ、az)、数字 (0-9)、ハイフン (-) を含める必要があります。デュアル スタックを構成するには、IPv6 アドレスにマッピングされたホスト名を指定します。



純粋な IPv6 はサポートされていません。混合モードは、IPv6 アドレスと IPv4 アドレスの両方を含む VLAN でサポートされます。

- ONTAPツールの IP アドレスは、ONTAPツールと通信するための主要なインターフェイスです。
- IPv4 はノード構成の IP アドレス コンポーネントであり、デバッグやメンテナンスの目的でノード上で診断シェルや SSH アクセスを有効にするために利用できます。

12. vCenter Server 8.0.3 バージョンを使用する場合は、[ハードウェアのカスタマイズ] ウィンドウで [CPU ホット アド] オプションと [メモリ ホット プラグ] オプションを有効にして、HA 機能を有効にします。

netapp-ontap-tools-for-vmware-vsphere-10.4-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder
- 4 Select a compute resource
- 5 Review details
- 6 License agreements
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Customize hardware**
- 11 Ready to complete

Customize hardware

Virtual Hardware VM Options Advanced Parameters

ADD NEW DEVICE ▾

CPU * 9 ⓘ

Cores per Socket 1 ▾
Sockets: 9

CPU Hot Plug ☒ Enable CPU Hot Add

Reservation 0 ▾ MHz ▾

Limit Unlimited ▾ MHz ▾

Shares Normal ▾ 1000 ▾

Hardware virtualization ☐ Expose hardware assisted virtualization to the guest OS

Performance Counters ☐ Enable virtualized CPU performance counters

Scheduling Affinity ⓘ

Memory * 18 ▾ GB ▾

Reservation 0 ▾ MB ▾
☐ Reserve all guest memory (All locked)

Limit Unlimited ▾ MB ▾

Shares Normal ▾ 368640 ▾

Memory Hot Plug ☒ Enable

CANCEL BACK NEXT

13. *完了準備完了*ウィンドウで詳細を確認し、*完了*を選択します。

デプロイメント タスクが作成されると、vSphere タスク バーに進行状況が表示されます。

14. VM を自動的にパワーオンするオプションが選択されていない場合は、タスクの完了後に VM をパワーオンします。

VM の Web コンソール内でインストールの進行状況を追跡できます。

OVF フォームに不一致がある場合は、ダイアログ ボックスが表示され、修正アクションが促されます。タブ ボタンを使用して移動し、必要な変更を加えて、[OK] を選択します。問題を解決するには 3 回試みることができます。3 回試行しても問題が解決しない場合は、インストール プロセスが停止し、新しい仮想マシンでインストールを再試行することをお勧めします。

次は何？

vCenter Server 7.0.3 を使用したONTAP tools for VMware vSphereがある場合は、デプロイメント後に次の手順を実行します。

1. vCenterクライアントにログインします。
2. ONTAPツール ノードの電源をオフにします。

3. インベントリ の下にあるONTAP tools for VMware vSphereに移動し、設定の編集 オプションを選択します。
4. *CPU*オプションで、*CPUホットアドを有効にする*チェックボックスをオンにします。
5. メモリ オプションの下で、メモリ ホット プラグ の 有効 チェックボックスをオンにします。

デプロイメントエラーコード

ONTAP tools for VMware vSphereの実行中にエラー コードが発生する場合があります。エラー コードは 5 桁で、最初の 2 桁は問題が発生したスクリプトを表し、最後の 3 桁はそのスクリプト内の特定のワークフローを表します。

すべてのエラー ログは ansible-perl-errors.log ファイルに記録され、問題を簡単に追跡して解決できるようになります。このログ ファイルには、エラー コードと失敗した Ansible タスクが含まれています。



このページに記載されているエラー コードは参考用です。エラーが解決しない場合、または解決策が記載されていない場合は、サポート チームにお問い合わせください。

次の表に、エラー コードと対応するファイル名を示します。

エラーコード	スクリプト名
00	firstboot-network-config.pl、モードデプロイ
01	firstboot-network-config.pl、モードのアップグレード
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl、デプロイ、HA
04	firstboot-deploy-otv-ng.pl、デプロイ、非 HA
05	firstboot-deploy-otv-ng.pl、再起動
06	firstboot-deploy-otv-ng.pl、アップグレード、HA
07	firstboot-deploy-otv-ng.pl、アップグレード、非HA
08	firstboot-otv-recovery.pl
09	デプロイ後のアップグレード.pl

エラー コードの最後の 3 桁は、スクリプト内の特定のワークフロー エラーを示します。

デプロイメントエラーコード	ワークフロー	解決
049	ネットワークと検証については、Perlスクリプトがすぐに割り当てます。	-
050	SSHキーの生成に失敗しました	プライマリ仮想マシン (VM) を再起動します。

053	RKE2のインストールに失敗しました	次のコマンドを実行してプライマリ VM を再起動するか、再デプロイします: <code>sudo rke2-killall.sh</code> (すべての VM)、 <code>sudo rke2-uninstall.sh</code> (すべての VM)。
054	kubeconfigの設定に失敗しました	再導入
055	レジストリのデプロイに失敗しました	レジストリ ポッドが存在する場合は、ポッドの準備が整うまで待ってからプライマリ VM を再起動するか、再デプロイします。
059	KubeVipのデプロイメントに失敗しました	Kubernetes コントロール プレーンとONTAPツールの仮想 IP アドレス、つまり導入時に提供される IP アドレスが同じ VLAN に属し、空き IP アドレスであることを確認します。前のポイントがすべて正しければ、再起動してください。それ以外の場合は再デプロイします。
060	オペレータの展開に失敗しました	再起動
061	サービスの展開に失敗しました	詳細とエラー ログ (<code>/var/log/ansible-perl-errors.log</code> および <code>/var/log/ansible-run.log</code>) を確認するには、 <code>ntv-system</code> 名前空間で <code>get pods</code> 、 <code>get rs</code> 、 <code>get svc</code> などの基本的な Kubernetes デバッグを実行し、再デプロイします。
062	ONTAPツールサービスの導入に失敗しました	詳細および再デプロイについては、 <code>/var/log/ansible-perl-errors.log</code> のエラー ログを参照してください。
065	Swagger ページの URL にアクセスできません	再導入
066	ゲートウェイ証明書の展開後の手順が失敗しました	アップグレードを回復/完了するには、次の手順を実行します。* 診断シェルを有効にします。* ' <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy</code> ' コマンドを実行します。* <code>/var/log/post-deploy-upgrade.log</code> のログを確認します。
088	journald のログローテーションの設定に失敗しました	VM がホストされているホストと互換性のある VM ネットワーク設定を確認します。別のホストに移行して VM を再起動してみてください。

089	サマリーログローテーション設定 ファイルの所有権の変更に失敗し ました	プライマリ VM を再起動します。
096	動的ストレージプロビジョナーを インストールする	-
108	シードスクリプトが失敗しました	-

再起動エラーコード	ワークフロー	解決
067	rke2-server の待機がタイムアウト しました。	-
101	Maint/Console ユーザー パスワー ドのリセットに失敗しました。	-
102	Maint/Console ユーザー パスワー ドのリセット中にパスワード ファ イルを削除できませんでした。	-
103	ボールド内の新しい Maint/Console ユーザー パスワードの更新に失敗 しました。	-
088	journald のログローテーションの構 成に失敗しました。	VM がホストされているホストと互 換性のある VM ネットワーク設定 を確認します。別のホストに移行 して VM を再起動してみてください。
089	サマリー ログ ローテーション構成 ファイルの所有権の変更に失敗し ました。	VM を再起動します。

ONTAP Tools for VMware vSphereの設定

vCenter Serverインスタンスを追加する

ONTAP tools for VMware vSphereに vCenter Server インスタンスを追加して、vCenter Server 環境内の仮想データストアを構成、管理、保護します。複数の vCenter Server インスタンスを追加する場合、ONTAPツールと各 vCenter Server 間の安全な通信にはカスタム CA 証明書が必要です。

このタスクについて

ONTAPツールを vCenter と統合すると、プロビジョニング、スナップショット、データ保護などのストレージ タスクを vSphere クライアントから直接実行できるようになり、別のストレージ管理コンソールに切り替える必要がなくなります。

手順

1. Web ブラウザを開き、次の URL に移動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. **vCenter** > **追加** を選択して、vCenter Server インスタンスをオンボードします。vCenter の IP アドレスまたはホスト名、ユーザー名、パスワード、ポートの詳細を入力します。



ONTAPツールに vCenter インスタンスを追加するには、管理者アカウントは必要ありません。管理者アカウントなしで、権限が制限されたカスタム ロールを作成できます。参照["ONTAP tools for VMware vSphereで vCenter Server RBAC を使用する"](#)詳細については。

ONTAPツールに vCenter Server インスタンスを追加すると、次のアクションが自動的にトリガーされます。

- vCenter クライアント プラグインはリモート プラグインとして登録されます。
- プラグインと API のカスタム権限が vCenter Server インスタンスに適用されます。
- ユーザーを管理するためにカスタム ロールが作成されます。
- プラグインは、vSphere ユーザー インターフェイスにショートカットとして表示されます。

VASA プロバイダを vCenter Server インスタンスに登録する

ONTAP tools for VMware vSphereを使用して、VASA プロバイダーを vCenter Server インスタンスに登録できます。VASA プロバイダ設定セクションには、選択した vCenter Server の VASA プロバイダ登録ステータスが表示されます。マルチ vCenter 展開では、各 vCenter Server インスタンスにカスタム CA 証明書があることを確認します。

手順

1. vSphere クライアントにログインします。
2. プラグイン セクションで、[ショートカット] > [* NetApp ONTAPツール*] を選択します。

3. 設定 > *VASA プロバイダー設定*を選択します。VASA プロバイダーの登録ステータスは未登録として表示されます。
4. *登録*ボタンを選択して、VASA プロバイダーを登録します。
5. VASA プロバイダーの名前と資格情報を入力します。ユーザー名には文字、数字、アンダースコアのみを含めることができます。パスワードの長さは 8 ～ 256 文字にする必要があります。
6. *登録*を選択します。
7. 登録が正常に完了し、ページが更新されると、登録された VASA プロバイダーのステータス、名前、バージョンが表示されます。登録後、登録解除アクションがアクティブになります。

次の手順

オンボードされた VASA プロバイダーが vCenter クライアントの VASA プロバイダーの下にリストされていることを確認します。

手順

1. vCenter Server インスタンスに移動します。
2. 管理者の資格情報を使用してログインします。
3. ストレージ プロバイダー > 構成 を選択します。オンボードされた VASA プロバイダーが正しくリストされていることを確認します。

NFS VAAIプラグインのインストール

NFS vStorage API for Array Integration (NFS VAAI) プラグインは、VMware vSphere と NFS ストレージ アレイを統合するソフトウェア コンポーネントです。ONTAP tools for VMware vSphereを使用して NFS VAAI プラグインをインストールし、NFS ストレージ アレイの高度な機能を活用して、特定のストレージ関連の操作を ESXi ホストからストレージ アレイ自体にオフロードします。

開始する前に

- ダウンロード ["NetApp NFS Plug-in for VMware VAAI"](#) インストール パッケージ。
- ESXi ホストと vSphere 7.0U3 の最新パッチ以降のバージョン、およびONTAP 9.14.1 以降のバージョンがインストールされていることを確認してください。
- NFS データストアをマウントします。

手順

1. vSphere クライアントにログインします。
2. プラグイン セクションで、[ショートカット] > [* NetApp ONTAPツール*] を選択します。
3. 設定 > **NFS VAAI ツール** を選択します。
4. VAAI プラグインが vCenter Server にアップロードされたら、[既存のバージョン] セクションで [変更] を選択します。VAAI プラグインが vCenter Server にアップロードされていない場合は、[アップロード] ボタンを選択します。
5. 参照して選択 `vib` ファイルを選択し、[アップロード] を選択して、ファイルをONTAPツールにアップロードします。
6. **ESXi** ホストにインストール を選択し、NFS VAAI プラグインをインストールする ESXi ホストを選択し

て、インストール を選択します。

プラグインのインストールに適した ESXi ホストのみが表示されます。vSphere Web Client の最近のタスク セクションでインストールの進行状況を監視できます。

7. インストール後に ESXi ホストを手動で再起動します。

VMware 管理者が ESXi ホストを再起動すると、ONTAP tools for VMware vSphereはNFS VAAI プラグインを自動的に検出し、有効にします。

次の手順

NFS VAAI プラグインをインストールし、ESXi ホストを再起動した後、VAAI コピー オフロード用の正しい NFS エクスポート ポリシーを構成する必要があります。NFS 環境で VAAI を構成する場合は、次の要件を考慮してエクスポート ポリシー ルールを構成します。

- 関連するONTAPボリュームは NFSv4 呼び出しを許可する必要があります。
- ルート ユーザーはルートのままにし、すべてのジャンクション 親ボリュームで NFSv4 を許可する必要があります。
- 関連する NFS サーバーで VAAI サポートのオプションを設定する必要があります。

手順の詳細については、"[VAAIコピーオフロード用の適切なNFSエクスポートポリシーを構成する](#)" KB 記事。

関連情報

["VMware vStorage over NFSのサポート"](#)

["NFSv4.0の有効化または無効化"](#)

["ONTAPでのNFSv4.2のサポート"](#)

ESXiホスト設定を構成する

ESXi サーバーのマルチパスとタイムアウト設定を構成すると、プライマリ パスに障害が発生した場合にバックアップ ストレージ パスにシームレスに切り替えることができるため、高可用性とデータの整合性が確保されます。

ESXi サーバーのマルチパスとタイムアウト設定を構成する

ONTAP Tools for VMware vSphereは、NetAppストレージ システムに最適なESXiホストのマルチパス設定とHBAタイムアウト設定を確認して設定します。

このタスクについて

構成とシステム負荷によっては、このプロセスに長い時間がかかる場合があります。タスクの進捗状況は[Recent Tasks]パネルに表示されます。

手順

1. VMware vSphere Web クライアントのホームページから、*ホストとクラスタ*を選択します。
2. ホストを右クリックし、* NetApp ONTAPツール* > ホスト データの更新 を選択します。

3. VMware vSphere Web クライアントのショートカット ページで、プラグイン セクションの * NetApp ONTAPツール* を選択します。
4. ONTAP tools for VMware vSphereプラグインの概要 (ダッシュボード) にある **ESXi** ホスト コンプライアンス カードに移動します。
5. *推奨設定を適用*リンクを選択します。
6. 推奨ホスト設定の適用 ウィンドウで、NetApp の推奨設定に準拠するように更新するホストを選択し、次へを選択します。



ESXi ホストを展開して現在の値を確認できます。

7. 設定ページで、必要に応じて推奨値を選択します。
8. 概要ペインで値を確認し、[完了] を選択します。最近のタスク パネルで進行状況を追跡できます。

ESXiホストの値を設定する

ONTAP tools for VMware vSphereを使用して、ESXi ホスト上でタイムアウトやその他の値を設定することで、最高のパフォーマンスとフェイルオーバーの成功を確保できます。ONTAP tools for VMware vSphereが設定する値は、NetApp の内部テストに基づいています。

次に示すESXiホストの値を設定できます。

HBA / CNA アダプタ設定

次のパラメータをデフォルト値に設定します。

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBAタイムアウト
- QLogic FC HBAタイムアウト

MPIO 設定

MPIO 設定は、NetAppストレージ システムの優先パスを定義します。利用可能なパスのうちどれが最適化されているか (相互接続ケーブルを通過する最適化されていないパスとは対照的) を決定し、優先パスをそれらのパスの 1 つに設定します。

高パフォーマンス環境の場合、または単一の LUN データストアでパフォーマンスをテストしている場合は、ラウンドロビン (VMW_PSP_RR) パス選択ポリシー (PSP) の負荷分散設定を、デフォルトの IOPS 設定の 1000 から値 1 に変更することを検討してください。



MPIO 設定は、NVMe、NVMe/FC、および NVMe/TCP プロトコルには適用されません。

NFS設定

パラメータ	この値を次のように設定します...
Net.TcpipHeapSize	32

Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128以上
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

ONTAPユーザーの役割と権限を構成する

ONTAP tools for VMware vSphereおよびONTAP System Manager 用の ONTAP ツールに付属の 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ー ロールと権限を設定できます。

開始する前に

- https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip を使用して、ONTAP tools for VMware vSphereからONTAP権限ファイルをダウンロードしておく必要があります。
- ONTAPツールからONTAPPrivilegesファイルをダウンロードしておく必要があります。
https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip。



ユーザーは、クラスターで作成することも、ストレージ仮想マシン (SVM) レベルで直接作成することもできます。user_roles.json ファイルを使用せずにユーザーを作成することもできますが、その場合は SVM レベルで最小限の権限セットが必要です。

- 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://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip ファイルを解凍します。
2. クラスターのクラスタ管理 IP アドレスを使用してONTAP System Manager にアクセスします。
3. 管理者権限でクラスターにログインします。ユーザーを構成するには、次の手順を実行します。
 - a. クラスタONTAPツール ユーザーを構成するには、[クラスタ] > [設定] > [ユーザーとロール] ペインを選択します。
 - b. SVM ONTAPツール ユーザーを構成するには、[ストレージ **SVM**] > [設定] > [ユーザーとロール] ペインを選択します。
 - c. [ユーザー]の下の[追加]を選択します。
 - d. 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。
 - e. *参照*して、ONTAPPrivilegesJSON ファイルを選択してアップロードします。

製品フィールドは自動的に入力されます。

- f. ドロップダウンから製品機能として*VSC、VASA プロバイダー、および SRA*を選択します。

役割 フィールドは、選択した製品の機能に基づいて自動的に入力されます。

- g. 必要なユーザ名とパスワードを入力します。
- h. ユーザーに必要な権限 (検出、ストレージの作成、ストレージの変更、ストレージの破棄、NAS/SAN ロール) を選択し、[追加] を選択します。

新しいロールとユーザーが追加され、設定したロールの詳細な権限を確認できます。

SVM集約マッピング要件

データストアのプロビジョニングに SVM ユーザー認証情報を使用するために、ONTAP tools for VMware vSphereは内部的に、データストア POST API で指定されたアグリゲート上にボリュームを作成します。ONTAP、SVM ユーザー認証情報を使用して、SVM 上のマッピングされていないアグリゲート上にボリュームを作成することはできません。これを解決するには、ここで説明するように、ONTAP REST API または CLI を使用して SVM をアグリゲートに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ユーザーとロールを手動で作成する

JSON ファイルを使用せずにユーザーとロールを手動で作成するには、このセクションの指示に従います。

1. クラスタのクラスタ管理 IP アドレスを使用してONTAP System Manager にアクセスします。
2. 管理者権限でクラスターにログインします。
 - a. クラスタONTAPツールのロールを設定するには、クラスタ > 設定 > ユーザーとロール ペインを選択します。
 - b. クラスタSVM ONTAPツールのロールを設定するには、ストレージ**SVM** > 設定 > *ユーザーとロール* ペインを選択します。
3. ロールの作成:
 - a. *ロール*テーブルの下に*追加*を選択します。
 - b. *ロール名*と*ロール属性*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。

4. ユーザーの作成:

- a. *ユーザー*テーブルの下で*追加*を選択します。
- b. *ユーザーの追加*ダイアログボックスで、*システムマネージャ*を選択します。
- c. *ユーザー名*を入力します。
- d. 上記の*ロールの作成*手順で作成したオプションから*ロール*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。必要なアプリケーションは ONTAPI と HTTP で、認証タイプは パスワード です。
- f. *ユーザーのパスワード*を設定し、ユーザーを*保存*します。

管理者以外のグローバル スコープのクラスタ ユーザーに必要な最小限の権限のリスト

このセクションでは、ユーザー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スコープのクラスタユーザーに必要な最小限の権限について説明します。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ーを作成することをお勧めします。これは、ONTAP tools for VMware vSphereでは、ONTAPでのプロビジョニングに読み取り権限以上の権限が必要になるためです。

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/ライセンス/ライセンス	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/cluster/nodes	読み取り専用	プラットフォームタイプの検出
/api/セキュリティ/アカウント	読み取り専用	特権の発見
/api/セキュリティ/ロール	読み取り専用	特権の発見
/api/ストレージ/集約	読み取り専用	データストア/ボリュームのプロビジョニング中の合計スペースチェック
/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効率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たディスクを取得するには
/api/storage/qos/ポリシー	読み取り/作成/変更	QoSとVMポリシー管理
/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 構成を取得します。
/api/ネットワーク/ip/インターフェース	読み取り専用	ストレージバックエンドの追加 - 管理LIFスコープがクラスタ/SVMであることを確認する
/api/storage/可用性ゾーン	読み取り専用	SAZディスクバリエーション。ONTAP 9.16.1 リリース以降およびASA r2 システムに適用されます。

VMware vSphere ONTAP API ベースのクラスター スコープ ユーザー ONTAP tools for VMware vSphereを作成する



データストアで障害が発生した場合に PATCH 操作と自動ロールバックを実行するには、検出、作成、変更、および破棄のPrivilegesが必要です。これらすべての権限が不足すると、ワークフローの中断やクリーンアップの問題が発生します。

検出、ストレージの作成、ストレージの変更、ストレージの破棄の権限を持つ ONTAP tools for VMware vSphere ONTAP API ベースのユーザー用の ONTAP ツールを作成すると、検出を開始し、ONTAP ツール ワークフローを管理できるようになります。

上記のすべての権限を持つクラスター スコープ ユーザーを作成するには、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
```

```

-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

```

```

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

```

```
security login rest-role create -role <role-name> -api /api/svm/peers  
-access readonly  
  
security login rest-role create -role <role-name> -api /api/svm/svms  
-access readonly
```

さらに、ONTAPバージョン 9.16.0 以降の場合は、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/storage/storage-units -access all
```

ONTAPバージョン 9.16.1 以降のASAr2 システムの場合は、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/storage/availability-zones -access readonly
```

VMware vSphere ONTAP API ベースの SVM スコープ ユーザーONTAP tools for VMware vSphereを作成する

すべての権限を持つ SVM スコープ ユーザーを作成するには、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/application/consistency-groups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/private/cli/snapmirror -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/igroups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/lun-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api
```

```

/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

```

```

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>

```

さらに、ONTAPバージョン 9.16.0 以降の場合は、次のコマンドを実行します。

```
security login rest-role create -role <role-name> -api  
/api/storage/storage-units -access all -vserver <vserver-name>
```

上記で作成した API ベースのロールを使用して新しい API ベースのユーザーを作成するには、次のコマンドを実行します。

```
security login create -user-or-group-name <user-name> -application http  
-authentication-method password -role <role-name> -vserver <cluster-or-  
vserver-name>
```

例：

```
security login create -user-or-group-name testvpsraall -application http  
-authentication-method password -role  
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_stil60-cluster_
```

アカウントのロックを解除し、管理インターフェースへのアクセスを有効にするには、次のコマンドを実行します。

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

例：

```
security login unlock -username testvpsraall -vserver C1_stil60-cluster
```

ONTAP tools for VMware vSphereを10.3 ユーザーにアップグレードする

JSON ファイルを使用して作成されたクラスター スコープのユーザーを持つONTAP tools for VMware vSphere の場合は、ユーザー管理者権限で次のONTAP CLI コマンドを使用して 10.3 リリースにアップグレードします。

製品の機能について：

- VSC
- VSCおよびVASAプロバイダー
- VSCおよびSRA
- VSC、VASA プロバイダー、および SRA。

クラスター権限：

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map remove" -access all

json ファイルを使用して作成された SVM スコープ ユーザーを持つ ONTAP tools for VMware vSphere の場合は、管理者ユーザー権限で ONTAP CLI コマンドを使用して 10.3 リリースにアップグレードします。

SVM 権限:

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <既存のロール名> -cmddirname "vserver nvme namespace delete" -access all

`-vserver <vserver-name>`

`security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem delete" -access all
-vserver <vserver-name>`

`security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem host remove"
-access all -vserver <vserver-name>`

`security login role create -role <既存のロール名> -cmddirname "vserver nvme subsystem map remove"
-access all -vserver <vserver-name>`

既存のロールにコマンド `vserver nvme namespace show` と `vserver nvme subsystem show` を追加すると、次のコマンドが追加されます。

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

ONTAP tools for VMware vSphereを10.4 ユーザー向けにアップグレードする

ONTAP 9.16.1 以降では、ONTAP tools for VMware vSphereを10.4 ユーザーにアップグレードします。

JSON ファイルとONTAPバージョン 9.16.1 以上を使用して作成されたクラスター スコープ ユーザーを持つONTAP tools for VMware vSphereの場合は、管理者ユーザー権限でONTAP CLI コマンドを使用して 10.4 リリースにアップグレードします。

製品の機能について:

- VSC
- VSCおよびVASAプロバイダー
- VSCおよびSRA
- VSC、VASA プロバイダー、および SRA。

クラスター権限:

```
security login role create -role <existing-role-name> -cmddirname "storage  
availability-zone show" -access all
```

ストレージバックエンドを追加する

ストレージ バックエンドを追加すると、ONTAPクラスターをオンボードできるようになります。

このタスクについて

vCenter が関連付けられた SVM を持つテナントとして機能するマルチテナント設定の場合は、ONTAP ツール マネージャを使用してクラスタを追加します。ストレージ バックエンドを vCenter Server に関連付けて、オンボードされた vCenter Server インスタンスにグローバルにマップします。vCenter テナントは、必要なストレージ仮想マシン (SVM) をオンボードする必要があります。これにより、SVM ユーザーは vVols データストアをプロビジョニングできるようになります。SVM を使用して vCenter にストレージを追加できます。

ONTAP ツールのユーザー インターフェイスを使用して、クラスタまたは SVM 認証情報を持つローカル ストレージ バックエンドを追加します。これらのストレージ バックエンドは、単一の vCenter に制限されます。クラスタ認証情報をローカルで使用する場合、関連付けられた SVM は自動的に vCenter にマッピングされ、vVols または VMFS を管理します。SRA を含む VMFS 管理の場合、ONTAP ツールはグローバル クラスタを必要とせずに SVM 認証情報をサポートします。

ONTAPツールマネージャの使用



マルチテナント設定では、ストレージ バックエンド クラスターをグローバルに追加し、SVM をローカルに追加して、SVM ユーザー資格情報を使用できます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから*ストレージ バックエンド*を選択します。
4. ストレージ バックエンドを追加し、サーバーの IP アドレスまたは FQDN、ユーザー名、およびパスワードの詳細を指定します。



IPv4 および IPv6 アドレス管理 LIF がサポートされています。

vSphere クライアント ユーザー インターフェイスの使用



vSphere クライアント ユーザー インターフェイスを通じてストレージ バックエンドを構成する場合、vVolsデータストアでは SVM ユーザーの直接追加がサポートされていないことに注意することが重要です。

1. vSphere クライアントにログインします。
2. ショートカット ページで、プラグイン セクションの *NetApp ONTAPツール* を選択します。
3. サイドバーから*ストレージ バックエンド*を選択します。
4. ストレージ バックエンドを追加し、サーバーの IP アドレス、ユーザー名、パスワード、ポートの詳細を指定します。



SVM ユーザーを直接追加するには、クラスターベースの認証情報と IPv4 および IPv6 アドレス管理 LIF を追加するか、SVM 管理 LIF を使用して SVM ベースの認証情報を提供します。

次は何？

リストが更新され、新しく追加されたストレージ バックエンドがリストに表示されます。

ストレージ バックエンドを vCenter Server インスタンスに関連付ける

ストレージ バックエンドを vCenter Server に関連付けて、ストレージ バックエンドとオンボードされた vCenter Server インスタンス間のマッピングをグローバルに作成します。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。

https://<ONTAPtoolsIP>:8443/virtualization/ui/

2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから vCenter を選択します。
4. ストレージ バックエンドに関連付ける vCenter Server インスタンスに対して縦の省略記号を選択します。
5. ドロップダウンからストレージ バックエンドを選択し、vCenter Server インスタンスに必要なストレージ バックエンドに関連付けます。

ネットワークアクセスを構成する

ネットワーク アクセスを構成していない場合は、ESXi ホストから検出されたすべての IP アドレスがデフォルトでエクスポート ポリシーに追加されます。特定の IP アドレスをいくつかエクスポート ポリシーに追加し、残りを除外するように構成できます。ただし、除外された ESXi ホストでマウント操作を実行すると、操作は失敗します。

手順

1. vSphere クライアントにログインします。
2. プラグイン セクションのショートカット ページで * NetApp ONTAPツール* を選択します。
3. ONTAPツールの左側のペインで、設定 > ネットワーク アクセスの管理 > 編集 に移動します。

複数の IP アドレスを追加するには、リストをコンマ、範囲、クラスレス ドメイン間ルーティング (CIDR)、またはこれら 3 つすべての組み合わせで区切ります。

4. *保存*を選択します。

データストアを作成する

ホスト クラスター レベルでデータストアを作成すると、データストアは宛先のすべてのホストに作成されてマウントされ、現在のユーザーに実行権限がある場合にのみアクションが有効になります。

vCenter Server および**ONTAP**ツールで管理されるデータストアを備えたネイティブ データストア間の相互運用性

ONTAP tools for VMware vSphereは、データストアに固有の親 igroup とホストにマップされた子 igroup を持つ、データストアのネストされた igroup を作成します。ONTAPシステム マネージャからフラット igroup を作成し、それを使用してONTAPツールを使用せずに VMFS データストアを作成できます。参照 ["SANイニシエータとigroupを管理する"](#)詳細についてはこちらをご覧ください。

ストレージがONTAPツールにオンボードされ、データストア検出が実行されると、フラット igroup と VMFS データストアはONTAPツールによって管理され、ネストされた igroup に変換されます。以前のフラット igroup を使用して新しいデータストアを作成することはできません。ネストされた igroup を再利用するには、ONTAPツールのユーザ インターフェイスまたは REST API を使用する必要があります。

vVolsデータストアを作成する

ONTAP tools for VMware vSphere以降では、スペース効率の高い thin.vVol としてASA r2 システム上にvVolsデータストアを作成できます。VASA プロバイダーは、vVol データストアを作成するときに、コンテナと必要なプロトコル エンドポイントを作成します。このコンテナにはバックアップボリュームはありません。

開始する前に

- ルート アグリゲートが SVM にマップされていないことを確認します。
- 選択した vCenter に VASA プロバイダーが登録されていることを確認します。
- ASA r2 ストレージ システムでは、SVM を SVM ユーザーのアグリゲートにマッピングする必要があります。

手順

1. vSphere クライアントにログインします。
2. ホスト システム、ホスト クラスター、またはデータ センターを右クリックし、* NetApp ONTAP ツール* > データストアの作成 を選択します。
3. vVols *データストア タイプ*を選択します。
4. *データストア名*と*プロトコル*情報を入力します。



ASA r2 システムは、vVolsの iSCSI および FC プロトコルをサポートしています。

5. データストアを作成するストレージ VM を選択します。
6. 詳細オプション:
 - カスタム エクスポート ポリシー を選択した場合は、すべてのオブジェクトに対して vCenter で検出を実行するようにしてください。このオプションは使用しないことをお勧めします。
 - iSCSI および FC プロトコルに対して カスタム イニシエーター グループ 名を選択できます。



ASA r2 ストレージ システム タイプ SVM では、データストアは論理コンテナにすぎないため、ストレージ ユニット (LUN/名前空間) は作成されません。

7. ストレージ属性 ペインでは、新しいボリュームを作成したり、既存のボリュームを使用したりできます。ただし、これら 2 種類のボリュームを組み合わせるとvVolsデータストアを作成することはできません。

新しいボリュームを作成するときに、データストアで QoS を有効にできます。デフォルトでは、LUN 作成要求ごとに 1 つのボリュームが作成されます。この手順は、ASA r2 ストレージ システムを使用するvVolsデータストアには適用されません。

8. 概要 ペインで選択内容を確認し、完了 を選択します。

NFSデータストアを作成する

VMware ネットワーク ファイル システム (NFS) データストアは、NFS プロトコルを使用して、ESXi ホストをネットワーク経由で共有ストレージ デバイスに接続します。NFS データストアは VMware vSphere 環境で一般的に使用されており、シンプルさや柔軟性など、いくつかの利点があります。

手順

1. vSphere クライアントにログインします。
2. ホスト システム、ホスト クラスター、またはデータ センターを右クリックし、* NetApp ONTAP ツール* > * データストアの作成* を選択します。
3. データストア タイプ フィールドで NFS を選択します。
4. 名前とプロトコル ペインにデータストアの名前、サイズ、プロトコル情報を入力します。詳細オプションで*データストア クラスター*と*Kerberos 認証*を選択します。



Kerberos 認証は、NFS 4.1 プロトコルが選択されている場合にのみ使用できます。

5. ストレージ ペインで プラットフォーム と ストレージ **VM** を選択します。
6. 詳細オプションで カスタム エクスポート ポリシー を選択した場合は、vCenter ですべてのオブジェクトの検出を実行します。このオプションは使用しないことをお勧めします。



SVM のデフォルト/ルート ボリューム ポリシーを使用して NFS データストアを作成することはできません。

- 詳細オプションでは、プラットフォーム ドロップダウンでパフォーマンスまたは容量が選択されている場合にのみ、非対称 トグル ボタンが表示されます。
 - プラットフォーム ドロップダウンで 任意 オプションを選択すると、プラットフォームや非対称フラグに関係なく、vCenter の一部である SVM が表示されます。
7. ストレージ属性 ペインでボリューム作成用のアグリゲートを選択します。詳細オプションで、必要に応じて スペース予約 と **QoS** の有効化 を選択します。
 8. 概要 ペインで選択内容を確認し、完了 を選択します。

NFS データストアが作成され、すべてのホストにマウントされます。

VMFS データストアを作成する

仮想マシン ファイル システム (VMFS) は、VMware vSphere 環境で仮想マシン ファイルを保存するクラスター化されたファイル システムです。VMFS を使用すると、複数の ESXi ホストが同じ仮想マシン ファイルに同時にアクセスできるようになり、vMotion や高可用性などの機能が有効になります。

保護されたクラスターの場合:

- VMFS データストアのみを作成できます。保護されたクラスターに VMFS データストアを追加すると、データストアは自動的に保護されます。
- 1 つ以上の保護されたホスト クラスターを持つデータセンターにデータストアを作成することはできません。
- 親ホスト クラスターが「自動フェイルオーバー デュプレックス ポリシー」タイプ (均一/非均一構成) の関係で保護されている場合、ESXi ホストにデータストアを作成することはできません。
- VMFS データストアは、非同期関係によって保護された ESXi ホスト上にのみ作成できます。「自動フェイルオーバー デュプレックス」ポリシーによって保護されているホスト クラスターの一部である ESXi ホスト上にデータストアを作成してマウントすることはできません。

開始する前に

- ONTAPストレージ側で各プロトコルのサービスと LIF を有効にします。

- ASA r2 ストレージ システム内の SVM ユーザーのアグリゲートに SVM をマップします。
- NVMe/TCP プロトコルを使用している場合は、ESXi ホストを構成します。
 - a. レビュー ["VMware 互換性ガイド"](#)



VMware vSphere 7.0 U3 以降のバージョンでは、NVMe/TCP プロトコルがサポートされています。ただし、VMware vSphere 8.0 以降のバージョンが推奨されます。

- b. ネットワーク インターフェイス カード (NIC) ベンダーが NVMe/TCP プロトコルを使用した ESXi NIC をサポートしているかどうかを検証します。
 - c. NIC ベンダーの仕様に従って、ESXi NIC を NVMe/TCP 用に構成します。
 - d. VMware vSphere 7リリースを使用する場合は、VMwareサイトの指示に従ってください。["NVMe over TCP アダプタの VMkernel バインディングを構成する"](#) NVMe/TCP ポート バインディングを構成します。VMware vSphere 8リリースを使用する場合は、["ESXi での NVMe over TCP の構成"](#)、NVMe/TCP ポート バインディングを構成します。
 - e. VMware vSphere 7リリースの場合は、次のページの手順に従ってください。["NVMe over RDMA または NVMe over TCP ソフトウェア アダプターを有効にする"](#) NVMe/TCP ソフトウェア アダプターを構成します。VMware vSphere 8リリースについては、["ソフトウェア NVMe over RDMA または NVMe over TCP アダプターを追加する"](#) NVMe/TCP ソフトウェア アダプターを構成します。
 - f. 走る["ストレージ システムとホストの検出"](#)ESXi ホストでのアクション。["vSphere 8.0 Update 1 およびONTAP 9.13.1 を使用して VMFS データストアに NVMe/TCP を構成する方法"](#)。
- NVMe/FC プロトコルを使用している場合は、次の手順を実行して ESXi ホストを構成します。
 - a. まだ有効になっていない場合は、ESXi ホストで NVMe over Fabrics (NVMe-oF) を有効にします。
 - b. SCSI ゾーニングを完了します。
 - c. ESXi ホストとONTAPシステムが物理層と論理層で接続されていることを確認します。

ONTAP SVMをFCプロトコル用に設定するには、["FC用のSVMの設定"](#)。

VMware vSphere 8.0でNVMe/FCプロトコルを使用する方法の詳細については、以下を参照してください。["ONTAPを使用した ESXi 8.x 向け NVMe-oF ホスト構成"](#)。

VMware vSphere 7.0でNVMe/FCを使用する方法の詳細については、以下を参照してください。["ONTAP NVMe/FC ホスト構成ガイド"](#)そして ["TR-4684"](#)。

手順

1. vSphere クライアントにログインします。
2. ホスト システム、ホスト クラスター、またはデータ センターを右クリックし、* NetApp ONTAP ツール* > データストアの作成 を選択します。
3. VMFS データストア タイプを選択します。
4. 名前とプロトコル ペインにデータストアの名前、サイズ、プロトコル情報を入力します。新しいデータストアを既存の VMFS データストア クラスターに追加する場合は、[詳細オプション] の下にあるデータストア クラスター セレクタを選択します。
5. ストレージ ペインでストレージ VM を選択します。必要に応じて、[詳細オプション] セクションに

カスタム イニシエーター グループ名 を入力します。データストアに既存の igroup を選択するか、カスタム名で新しい igroup を作成することができます。

NVMe/FC または NVMe/TCP プロトコルを選択すると、新しい名前空間サブシステムが作成され、名前空間マッピングに使用されます。名前空間サブシステムは、データストア名を含む自動生成された名前を使用して作成されます。ストレージ ペインの詳細オプションの カスタム名前空間サブシステム名 フィールドで、名前空間サブシステムの名前を変更できます。

6. ストレージ属性 ペインから:

- a. ドロップダウン オプションから **Aggregate** を選択します。



ASA r2ストレージシステムの場合、ASA r2ストレージは分散ストレージであるため、「アグリゲート」オプションは表示されません。ASAASAストレージシステムタイプのSVMを選択すると、ストレージ属性ページにQoSを有効にするためのオプションが表示されます。

- b. 選択したプロトコルに従って、thin タイプのスペース予約を持つストレージ ユニット (LUN/名前空間) が作成されます。



ONTAP 9.16.1 以降、ASA r2 ストレージ システムはクラスタごとに最大 12 個のノードをサポートします。

- c. 異機種クラスタである 12 ノード SVM を備えたASA r2 ストレージ システムの パフォーマンス サービス レベル を選択します。選択した SVM が同種クラスタであるか、SVM ユーザーを使用している場合、このオプションは使用できません。

「Any」はデフォルトのパフォーマンス サービス レベル (PSL) 値です。この設定では、ONTAP バランス配置アルゴリズムを使用してストレージ ユニットが作成されます。ただし、必要に応じてパフォーマンス オプションまたはエクストリーム オプションを選択できます。

- d. 必要に応じて、「既存のボリュームを使用する」および「QoS を有効にする」オプションを選択し、詳細を入力します。



ASA r2 ストレージ タイプでは、ボリュームの作成または選択はストレージ ユニットの作成 (LUN/名前空間) には適用されません。したがって、これらのオプションは表示されません。



既存のボリュームを使用して NVMe/FC または NVMe/TCP プロトコルで VMFS データストアを作成することはできません。新しいボリュームを作成する必要があります。

7. 概要 ペインでデータストアの詳細を確認し、完了 を選択します。



保護されたクラスタ上にデータストアを作成すると、「データストアは保護されたクラスタにマウントされています。」という読み取り専用メッセージが表示されます。

結果

VMFS データストアが作成され、すべてのホストにマウントされます。

データストアと仮想マシンの保護

ホストクラスタ保護を使用して保護する

ONTAP tools for VMware vSphereは、ホスト クラスターの保護を管理します。選択した SVM に属し、クラスタの 1 つ以上のホストにマウントされているすべてのデータストアは、ホスト クラスタの下で保護されます。

開始する前に

次の前提条件が満たされていることを確認してください。

- ホスト クラスタには、1 つの SVM のデータストアのみが含まれます。
- ホスト クラスタにマウントされたデータストアは、クラスタ外部のホストにマウントしないでください。
- ホスト クラスタにマウントされるすべてのデータストアは、iSCSI/FC プロトコルを使用した VMFS データストアである必要があります。NVMe/FC および NVMe/TCP プロトコルを使用したvVols、NFS、または VMFS データストアはサポートされていません。
- ホスト クラスタにマウントされたデータストアを形成するFlexVol/LUN は、既存の整合性グループ (CG) の一部であってはなりません。
- ホスト クラスタにマウントされたFlexVol/LUN 形成データストアは、既存のSnapMirror関係の一部であってはなりません。
- ホスト クラスタには少なくとも 1 つのデータストアが必要です。

手順

1. vSphere クライアントにログインします。
2. ホスト クラスタを右クリックし、* NetApp ONTAPツール* > クラスタの保護 を選択します。
3. 保護クラスタ ウィンドウでは、データストア タイプとソース ストレージ仮想マシン (VM) の詳細が自動的に入力されます。保護されたデータストアを表示するには、データストア リンクを選択します。
4. *整合性グループ名*を入力します。
5. *関係を追加*を選択します。
6. * SnapMirror関係の追加* ウィンドウで、ターゲット ストレージ **VM** と ポリシー タイプを選択します。

ポリシー タイプは、非同期または自動フェールオーバーデュプレックスにすることができます。

SnapMirror関係を AutomatedFailOverDuplex タイプのポリシーとして追加する場合は、ONTAP tools for VMware vSphereが展開されているのと同じ vCenter に、ターゲット ストレージ VM をストレージ バックエンドとして追加する必要があります。

AutomatedFailOverDuplex ポリシー タイプには、均一なホスト構成と非均一なホスト構成があります。* 均一ホスト構成*トグル ボタンを選択すると、ホスト イニシエーター グループ構成がターゲット サイトに暗黙的に複製されます。詳細については、["重要な概念と用語"](#)。

7. 非均一なホスト構成を選択する場合は、そのクラスタ内の各ホストのホスト アクセス (ソース/ターゲット) を選択します。

8. *追加*を選択します。
9. *クラスターの保護*ウィンドウでは、作成操作中に保護されたクラスターを編集することはできません。削除して再度保護を追加することができます。ホスト クラスター保護の変更操作中に、編集オプションが利用できます。省略記号メニュー オプションを使用して、関係を編集または削除できます。
10. *保護*ボタンを選択します。

ジョブ ID の詳細を含む vCenter タスクが作成され、その進行状況が最近のタスク パネルに表示されます。これは非同期タスクです。ユーザー インターフェイスにはリクエストの送信ステータスのみが表示され、タスクが完了するまで待機しません。
11. 保護されたホスト クラスターを表示するには、* NetApp ONTAP ツール* > 保護 > ホスト クラスター リレーションシップ に移動します。

SRA保護を使用して保護する

データストアを保護するために**SRA**を構成する

ONTAP tools for VMware vSphereには、SRA 機能を有効にして災害復旧を構成するオプションが用意されています。

開始する前に

- vCenter Server インスタンスをセットアップし、ESXi ホストを構成しておく必要があります。
- ONTAP tools for VMware vSphereを導入しておく必要があります。
- SRAアダプターをダウンロードしておく必要があります。`.tar.gz`ファイルから ["NetAppサポート サイト"](#)。
- SRA ワークフローを実行する前に、ソースと宛先のONTAPクラスターに同じカスタムSnapMirrorスケジュールが作成されている必要があります。
- ["ONTAP tools for VMware vSphereを有効にする"](#) SRA 機能を有効にします。

手順

1. 次の URL を使用して VMware Live Site Recovery アプライアンス管理インターフェイスにログインします。`https://<srm\_ip>:5480`をクリックし、VMware VMware Live Site Recovery アプライアンス管理インターフェイスのストレージ レプリケーション アダプタに移動します。
2. *新しいアダプター*を選択します。
3. SRA プラグインの `.tar.gz` インストーラーを VMware Live Site Recovery にアップロードします。
4. アダプタを再スキャンして、VMware Live Site Recovery のストレージ レプリケーション アダプタ ページで詳細が更新されていることを確認します。

SANおよびNAS環境向けにSRAを構成する

VMware Live Site Recovery のストレージ レプリケーション アダプタ (SRA) を実行する前に、ストレージ システムをセットアップする必要があります。

SAN環境向けにSRAを構成する

開始する前に

保護されたサイトと回復サイトに次のプログラムがインストールされている必要があります。

- VMware ライブサイトリカバリ

VMware Live Site Recovery のインストールに関するドキュメントは、VMware サイトにあります。

["VMware Live Site Recoveryについて"](#)

- SRA

アダプタは VMware Live Site Recovery にインストールされます。

手順

1. 保護対象サイトで、プライマリESXiホストがプライマリ ストレージ システムのLUNに接続されていることを確認します。
2. LUNが次のigroupにあることを確認します。`ostype`プライマリ ストレージ システムでオプションが *VMware* に設定されています。
3. リカバリ サイトの ESXi ホストがストレージ仮想マシン (SVM) に適切に iSCSI 接続できることを確認します。セカンダリ サイトの ESXi ホストはセカンダリ サイトのストレージにアクセスできる必要があります、プライマリ サイトの ESXi ホストはプライマリ サイトのストレージにアクセスできる必要があります。

これは、ESXiホストにSVMに接続されたローカルLUNがあることを確認するか、`iscsi show initiators SVM` に対するコマンド。ESXi ホスト内のマップされた LUN の LUN アクセスをチェックして、iSCSI 接続を確認します。

NAS環境向けにSRAを構成する

開始する前に

保護されたサイトと回復サイトに次のプログラムがインストールされている必要があります。

- VMware ライブサイトリカバリ

VMware Live Site Recovery のインストールに関するドキュメントは、VMware サイトにあります。

["VMware Live Site Recoveryについて"](#)

- SRA

アダプタは、VMware Live Site Recovery および SRA サーバーにインストールされます。

手順

1. 保護対象サイトのデータストアに、vCenter Serverに登録された仮想マシンがあることを確認します。
2. 保護されたサイトの ESXi ホストがストレージ仮想マシン (SVM) から NFS エクスポート ボリュームをマウントしていることを確認します。
3. アレイマネージャウィザードを使用してVMware Live Site Recoveryにアレイを追加する際は、*NFSアド

レス*フィールドにNFSエクスポートが存在するIPアドレスやFQDNなどの有効なアドレスが指定されていることを確認してください。*NFSアドレス*フィールドにはNFSホスト名を使用しないでください。

4. 使用 `ping` リカバリ サイトの各 ESXi ホストでコマンドを実行して、SVM からの NFS エクスポートを提供するために使用される IP アドレスにアクセスできる VMkernel ポートがホストにあることを確認します。

大規模環境向けに **SRA** を構成する

大規模環境でストレージ レプリケーション アダプタ (SRA) が最適に機能するには、推奨設定に従ってストレージ タイムアウト間隔を構成する必要があります。

ストレージ プロバイダの設定

拡張環境の場合、VMware Live Site Recovery で次のタイムアウト値を設定する必要があります。

詳細設定	タイムアウト値
<code>StorageProvider.resignatureTimeout</code>	値を900秒から12000秒に引き上げます。
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	高い値を設定します (例: 99999)

また、`StorageProvider.autoResignatureMode` オプション。

参照 ["Change Storage Provider Settings"](#) ストレージ プロバイダー設定の変更の詳細については、こちらをご覧ください。

ストレージ設定

タイムアウトになったら、`storage.commandTimeout` そして `storage.maxConcurrentCommandCnt` より高い価値へ。



このタイムアウト間隔は最大値です。最大タイムアウトに達することはありません。ほとんどのコマンドは、設定された最大タイムアウト間隔以内に終了します。

参照 ["Change Storage Settings"](#) SAN プロバイダーの設定を変更するため。

VMware Live Site Recovery アプライアンスで **SRA** を構成する

VMware Live Site Recovery アプライアンスを展開した後、ストレージ レプリケーション アダプタ (SRA) を構成して、災害復旧管理を有効にします。

VMware Live Site Recovery アプライアンスで SRA を構成すると、ONTAP tools for VMware vSphere がアプライアンス内に保存され、VMware Live Site Recovery と SRA 間の通信が可能になります。

開始する前に

- `_tar.gz` ファイルを ["NetAppサポート サイト"](#)。
- ONTAP ツール マネージャーで SRA サービスを有効にします。詳細については、["サービスを有効にする"](#) セクション。
- VMware vSphere アプライアンスの ONTAP ツールに vCenter Server を追加します。詳細については、["vCenter Server を追加する"](#) セクション。
- ONTAP tools for VMware vSphere にストレージ バックエンドを追加します。詳細については、["ストレージバックエンドを追加する"](#) セクション。

手順

1. VMware Live Site Recovery アプライアンス画面で、ストレージ レプリケーション アダプタ > 新しいアダプタ を選択します。
2. `.tar.gz` ファイルを VMware Live Site Recovery にアップロードします。
3. PuTTY などの SSH クライアントを介して管理者アカウントを使用して VMware Live Site Recovery アプライアンスにログインします。
4. 次のコマンドを使用して、root ユーザーに切り替えます。 `su root`
5. コマンドを実行する ``cd /var/log/vmware/srm`` ログディレクトリに移動します。
6. ログの場所で、SRA で使用される docker ID を取得するコマンドを入力します。 `docker ps -l`
7. コンテナ ID にログインするには、次のコマンドを入力します。 `docker exec -it -u srm <container id> sh`
8. 次のコマンドを使用して、ONTAP tools for VMware vSphere IP アドレスとパスワードで VMware Live Site Recovery を構成します。 `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - パスワードを一重引用符で囲んで指定すると、Perl スクリプトは特殊文字を区切り文字としてではなく、パスワードの一部として扱います。
 - アプリケーション (VASA Provider/SRA) のユーザー名とパスワードは、これらのサービスを初めて有効にする際に、ONTAP Tools Manager で設定できます。これらの資格情報を使用して、SRA を VMware Live Site Recovery に登録します。
 - vCenter GUID を見つけるには、vCenter インスタンスを追加した後、ONTAP ツール マネージャの vCenter Server ページに移動します。参照 ["vCenter Server を追加する"](#) セクション。
9. アダプタを再スキャンして、更新された詳細が VMware Live Site Recovery のストレージ レプリケーション アダプタ ページに表示されることを確認します。

結果

ストレージ資格情報が保存されたことを示す確認メッセージが表示されます。これで、SRA は指定された IP アドレス、ポート、および資格情報を使用して SRA サーバーと通信できるようになりました。

SRA クレデンシャルの更新

VMware Live Site Recovery が SRA と通信するには、資格情報を変更した場合に VMware Live Site Recovery サーバー上の SRA 資格情報を更新する必要があります。

開始する前に

トピックに記載されている手順を実行する必要があります"VMware Live Site Recovery アプライアンスでの SRA の構成"。

手順

1. 次のコマンドを実行して、VMware Live Site Recovery マシン フォルダーのキャッシュされたONTAPツールのユーザー名とパスワードを削除します。

- a. `sudo su <enter root password>`
- b. `docker ps`
- c. `docker exec -it <container_id> sh`
- d. `cd conf/`
- e. `rm -rf *`

2. Perl コマンドを実行して、新しい資格情報を使用して SRA を構成します。

- a. `cd ..`
- b. ``perl command.pl -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>``パスワード値を一重引用符で囲む必要があります。

ストレージ クレデンシャルが保存されたことを示すメッセージが表示されます。以降SRAは、指定されたIPアドレス、ポート、およびクレデンシャルを使用してSRAサーバと通信できます。

保護対象サイトとリカバリ サイトの設定

保護されたサイト上の仮想マシンのグループを保護するには、保護グループを作成する必要があります。

新しいデータストアを追加する際は、既存のデータストアグループに含めるか、新しいデータストアを追加して保護用の新しいボリュームまたはコンシステンシーグループを作成することができます。保護対象のコンシステンシーグループまたはボリュームに新しいデータストアを追加したら、SnapMirrorを更新し、保護対象サイトとリカバリサイトの両方でストレージ検出を実行します。新しいデータストアを確実に検出・保護するために、検出手動で実行することも、スケジュールに従って実行することもできます。

保護対象サイトとリカバリ サイトのペアリング

ストレージ レプリケーション アダプタ (SRA) がストレージ システムを検出できるようにするには、vSphere Client を使用して作成された保護サイトとリカバリ サイトをペアリングする必要があります。



ストレージ レプリケーション アダプタ (SRA) は、整合性グループ上の自動フェイルオーバー デュプレックス タイプの 1 つの同期関係と非同期関係SnapMirrorによるファンアウトをサポートします。ただし、整合性グループ上の 2 つの非同期SnapMirrorを使用したファンアウト、またはボリューム上のファンアウト SnapMirror はサポートされていません。

開始する前に

- 保護サイトとリカバリ サイトに VMware Live Site Recovery がインストールされている必要があります。
- 保護サイトとリカバリ サイトに SRA をインストールする必要があります。

手順

1. vSphere Client ホームページで **Site Recovery** をダブルクリックし、**Sites** を選択します。
2. オブジェクト > アクション > *サイトのペア*を選択します。
3. **Site Recovery Manager** サーバーのペアリング ダイアログ ボックスで、保護されたサイトの Platform Services Controller のアドレスを入力し、次へ を選択します。
4. [Select vCenter Server]セクションで、次の手順を実行します。
 - a. 保護対象サイトのvCenter Serverが対応するペア候補として表示されていることを確認します。
 - b. SSO 管理者の資格情報を入力し、[完了] を選択します。
5. プロンプトが表示されたら、「はい」を選択してセキュリティ証明書を受け入れます。

結果

保護されたサイトと回復サイトの両方が [オブジェクト] ダイアログ ボックスに表示されます。

保護グループの設定

開始する前に

ソース サイトとターゲット サイトの両方で以下が設定されていることを確認する必要があります。

- 同じバージョンの VMware Live Site Recovery がインストールされている
- 仮想マシン
- 保護対象サイトとリカバリ サイトがペアリングされている
- ソースとデスティネーションのデータストアがそれぞれのサイトにマウントされている

手順

1. vCenter Server にログインし、**Site Recovery > Protection Groups** を選択します。
2. 保護グループ ペインで、新規 を選択します。
3. 保護グループの名前と説明、方向を指定して、[次へ] を選択します。
4. *タイプ*フィールドで、*タイプフィールドオプション...*として、NFSおよびVMFSデータストアのデータストアグループ（アレイベースレプリケーション）を選択します。フォールト ドメインは、実際には、レプリケーションが有効になっているSVMです。ピアリングのみが実装されており、問題のないSVMが表示されます。
5. [レプリケーション グループ] タブで、有効なアレイ ペアまたは構成した仮想マシンが含まれるレプリケーション グループのいずれかを選択し、[次へ] を選択します。

レプリケーション グループ上のすべての仮想マシンが保護グループに追加されます。

6. 既存のリカバリ プランを選択するか、[新しいリカバリ プランに追加] を選択して新しいリカバリ プランを作成することもできます。
7. [準備完了] タブで、作成した保護グループの詳細を確認し、[完了] を選択します。

保護対象サイトとリカバリ サイトのリソースの設定

ネットワーク マッピングの設定

保護されたサイトの各リソースをリカバリ サイトの適切なリソースにマッピングできるようにするには、両方のサイトで VM ネットワーク、ESXi ホスト、フォルダーなどのリソース マッピングを構成する必要があります。

次のリソース構成を完了する必要があります。

- ネットワーク マッピング
- フォルダ マッピング
- リソース マッピング
- プレースホルダ データストア

開始する前に

保護されたサイトと回復サイトを接続する必要があります。

手順

1. vCenter Server にログインし、**Site Recovery > Sites** を選択します。
2. 保護されたサイトを選択し、[管理] を選択します。
3. 新しいネットワーク マッピングを作成するには、管理タブで [ネットワーク マッピング] > [新規] を選択します。
4. ネットワーク マッピングの作成ウィザードで、次の操作を行います。
 - a. *一致する名前を持つネットワークのマッピングを自動的に準備する*を選択し、*次へ*を選択します。
 - b. 保護サイトとリカバリ サイトに必要なデータ センター オブジェクトを選択し、[マッピングの追加] を選択します。
 - c. マッピングが正常に作成されたら、[次へ] を選択します。
 - d. 先ほど逆マッピングを作成するために使用したオブジェクトを選択し、[完了] を選択します。

結果

[Network Mappings] ページに、保護対象サイトのリソースとリカバリ サイトのリソースが表示されます。環境内の他のネットワークについても同じ手順を実行します。

フォルダ マッピングの設定

保護されたサイトと回復サイト間の通信を可能にするには、それらの間でフォルダーをマップする必要があります。

開始する前に

保護されたサイトと回復サイトを接続する必要があります。

手順

1. vCenter Server にログインし、**Site Recovery > Sites** を選択します。
2. 保護されたサイトを選択し、[管理] を選択します。

3. 新しいフォルダー マッピングを作成するには、[管理] タブで [フォルダー マッピング] > [フォルダー] アイコンを選択します。
4. Create Folder Mappingウィザードで、次の手順を実行します。
 - a. *名前が一致するフォルダーのマッピングを自動的に準備する*を選択し、*次へ*を選択します。
 - b. 保護サイトとリカバリ サイトに必要なデータ センター オブジェクトを選択し、[マッピングの追加] を選択します。
 - c. マッピングが正常に作成されたら、[次へ] を選択します。
 - d. 先ほど逆マッピングを作成するために使用したオブジェクトを選択し、[完了] を選択します。

結果

[Folder Mappings]ページに、保護対象サイトのリソースとリカバリ サイトのリソースが表示されます。環境内の他のネットワークについても同じ手順を実行します。

リソース マッピングの設定

仮想マシンがいずれかのホスト グループにフェールオーバーするように構成されるように、保護サイトとリカバリ サイトでリソースをマップする必要があります。

開始する前に

保護されたサイトと回復サイトを接続する必要があります。



VMware Live Site Recovery では、リソースはリソース プール、ESXi ホスト、または vSphere クラスターになります。

手順

1. vCenter Server にログインし、**Site Recovery > Sites** を選択します。
2. 保護されたサイトを選択し、[管理] を選択します。
3. 新しいリソース マッピングを作成するには、管理タブで リソース マッピング > 新規 を選択します。
4. Create Resource Mappingウィザードで、次の手順を実行します。
 - a. *一致する名前を持つリソースのマッピングを自動的に準備する*を選択し、*次へ*を選択します。
 - b. 保護サイトとリカバリ サイトに必要なデータ センター オブジェクトを選択し、[マッピングの追加] を選択します。
 - c. マッピングが正常に作成されたら、[次へ] を選択します。
 - d. 先ほど逆マッピングを作成するために使用したオブジェクトを選択し、[完了] を選択します。

結果

[Resource Mappings]ページに、保護対象サイトのリソースとリカバリ サイトのリソースが表示されます。環境内の他のネットワークについても同じ手順を実行します。

プレースホルダ データストアの設定

保護対象の仮想マシン (VM) 用の場所をリカバリサイトのvCenterインベントリに確保するために、プレースホルダデータストアを設定する必要があります。プレースホル

ダVMは数百キロバイト以下しか使用しないため、プレースホルダデータストアはそれほど大きくする必要はありません。

開始する前に

- 保護されたサイトと回復サイトを接続する必要があります。
- リソース マッピングを構成する必要があります。

手順

1. vCenter Server にログインし、**Site Recovery > Sites** を選択します。
2. 保護されたサイトを選択し、[管理] を選択します。
3. 管理タブで プレースホルダー データストア > 新規 を選択して、新しいプレースホルダー データストアを作成します。
4. 適切なデータストアを選択し、「OK」を選択します。



プレースホルダ データストアはローカルまたはリモートに作成し、レプリケートはしないでください。

5. 手順 3 ~ 5 を繰り返して、リカバリ サイトのプレースホルダー データストアを構成します。

アレイ マネージャを使用した**SRA**の設定

VMware Live Site Recovery のアレイ マネージャ ウィザードを使用してストレージ レプリケーション アダプタ (SRA) を構成し、VMware Live Site Recovery とストレージ仮想マシン (SVM) 間の対話を有効にすることができます。

開始する前に

- VMware Live Site Recovery で保護サイトとリカバリ サイトをペアリングしておく必要があります。
- アレイ マネージャを構成する前に、オンボード ストレージを構成しておく必要があります。
- 保護されたサイトとリカバリ サイト間のSnapMirror関係を構成して複製しておく必要があります。
- マルチテナントを有効にするには、SVM 管理 LIF を有効にする必要があります。

SRAでは、クラスタレベルの管理とSVMレベルの管理がサポートされます。クラスター レベルでストレージを追加すると、クラスター内のすべての SVM を検出して操作を実行できます。SVMレベルでストレージを追加する場合は、特定のSVMだけを管理できます。

手順

1. VMware Live Site Recovery で、アレイ マネージャ > アレイ マネージャの追加 を選択します。
2. VMware Live Site Recovery でアレイを説明するには、次の情報を入力します。
 - a. 表示名 フィールドにアレイ マネージャを識別するための名前を入力します。
 - b. **SRA** タイプ フィールドで、* NetApp Storage Replication Adapter for ONTAP* を選択します。
 - c. クラスタまたはSVMへの接続情報を入力します。
 - クラスタに接続する場合は、クラスタ管理LIFを入力する必要があります。

- SVM に直接接続する場合は、SVM 管理 LIF の IP アドレスを入力する必要があります。



アレイ マネージャを構成するときは、ONTAP tools for VMware vSphereでストレージシステムをオンボードするために使用したのと同じ接続 (IP アドレス) をストレージシステムに使用する必要があります。たとえば、アレイ マネージャ構成が SVM 範囲である場合、ONTAP tools for VMware vSphereの下ストレージを SVM レベルで追加する必要があります。

- d. クラスターに接続する場合は、**SVM** 名 フィールドに SVM 名を指定するか、クラスター内のすべての SVM を管理するには空白のままにします。
- e. ボリューム包含リスト フィールドに検出するボリュームを入力します。

保護対象サイト側のソース ボリューム、およびリカバリ サイト側のレプリケートされたデスティネーション ボリュームを入力できます。

たとえば、ボリューム `dst_vol1` と SnapMirror関係にあるボリューム `src_vol1` を検出する場合は、保護サイト フィールドに `src_vol1` を指定し、リカバリ サイト フィールドに `dst_vol1` を指定する必要があります。

- f. (オプション) 「ボリューム除外リスト」 フィールドに、検出から除外するボリュームを入力します。

保護対象サイト側のソース ボリューム、およびリカバリ サイト側のレプリケートされたデスティネーション ボリュームを入力できます。

たとえば、ボリューム `dst_vol1` と SnapMirror関係にあるボリューム `src_vol1` を除外する場合は、保護サイト フィールドに `src_vol1` を指定し、リカバリ サイト フィールドに `dst_vol1` を指定する必要があります。

- 3. *次へ*を選択します。
- 4. アレイが検出され、「アレイ マネージャの追加」ウィンドウの下部に表示されていることを確認し、「完了」を選択します。

該当するSVMの管理IPアドレスとクレデンシャルを使用して、リカバリ サイトでも同じ手順を実行します。Add Array Managerウィザードの[Enable Array Pairs]画面で、正しいアレイ ペアが選択されていて、有効化できる状態になっていることを確認します。

レプリケートされたストレージ システムの検証

ストレージ レプリケーション アダプタ (SRA) を構成した後、保護されたサイトとリカバリ サイトが正常にペアリングされていることを確認する必要があります。複製されたストレージ システムは、保護されたサイトとリカバリ サイトの両方で検出可能である必要があります。

開始する前に

- ストレージ システムを構成する必要があります。
- VMware Live Site Recovery アレイ マネージャを使用して、保護サイトとリカバリ サイトをペアリングしておく必要があります。
- SRA のテスト フェイルオーバー操作とフェイルオーバー操作を実行する前に、FlexCloneライセンスとSnapMirrorライセンスを有効にしておく必要があります。

- ソース サイトと宛先サイトで同じSnapMirrorポリシーとスケジュールを設定する必要があります。

手順

1. vCenter Serverにログインします。
2. サイト回復 > アレイ ベースのレプリケーション に移動します。
3. 必要なアレイ ペアを選択し、対応する詳細を確認します。

保護サイトとリカバリサイトでストレージ システムが検出され、ステータスが「有効」になっている必要があります。

ファンアウト保護

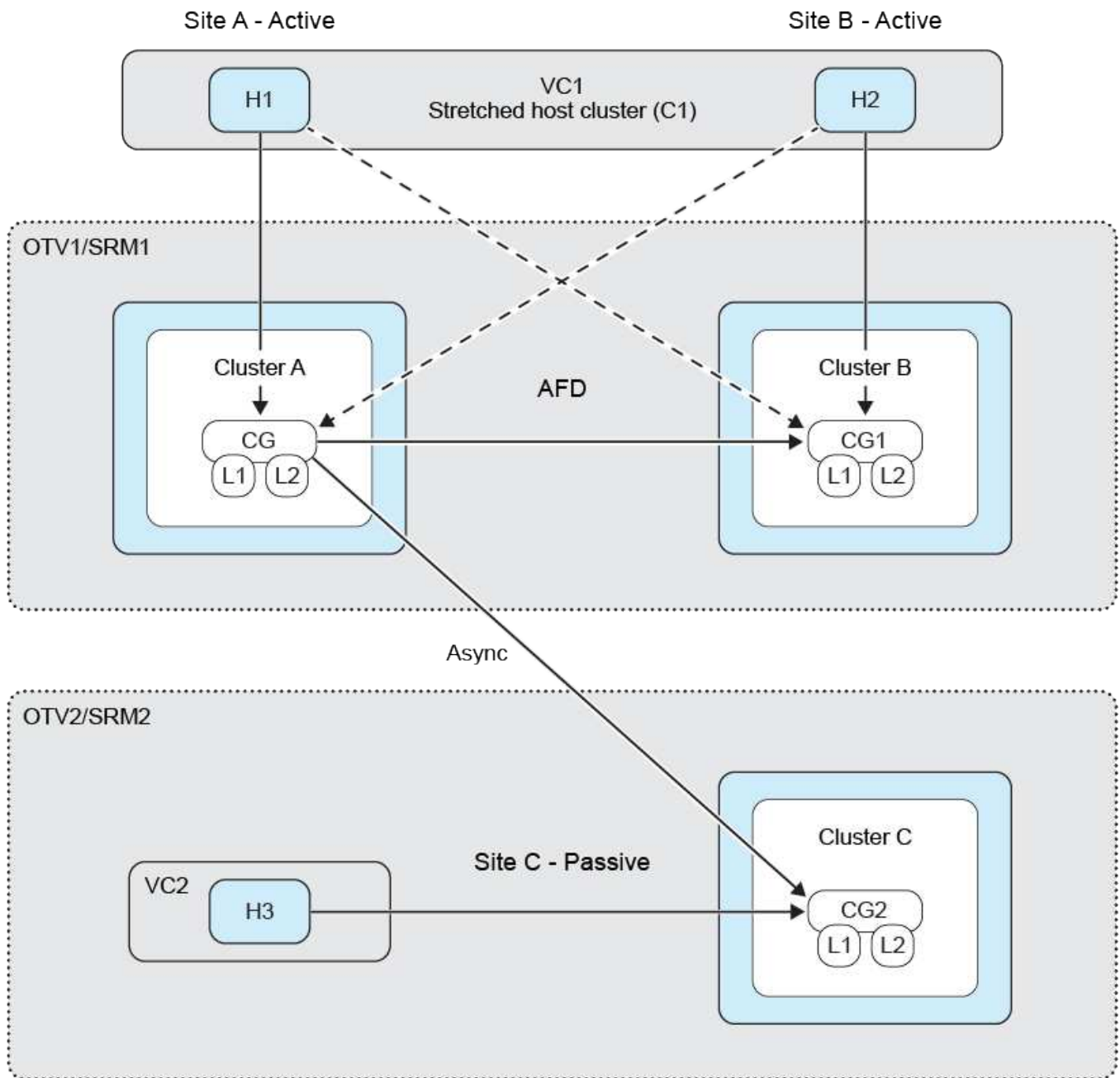
ファンアウト保護では、コンシステンシ グループは、最初の宛先ONTAPクラスタ上の同期関係と、2 番目の宛先ONTAPクラスタ上の非同期関係によって二重に保護されます。SnapMirrorアクティブ同期保護の作成、編集、および削除ワークフローにより、同期保護が維持されます。SRM フェイルオーバーおよび再保護ワークフローは非同期保護を維持します。

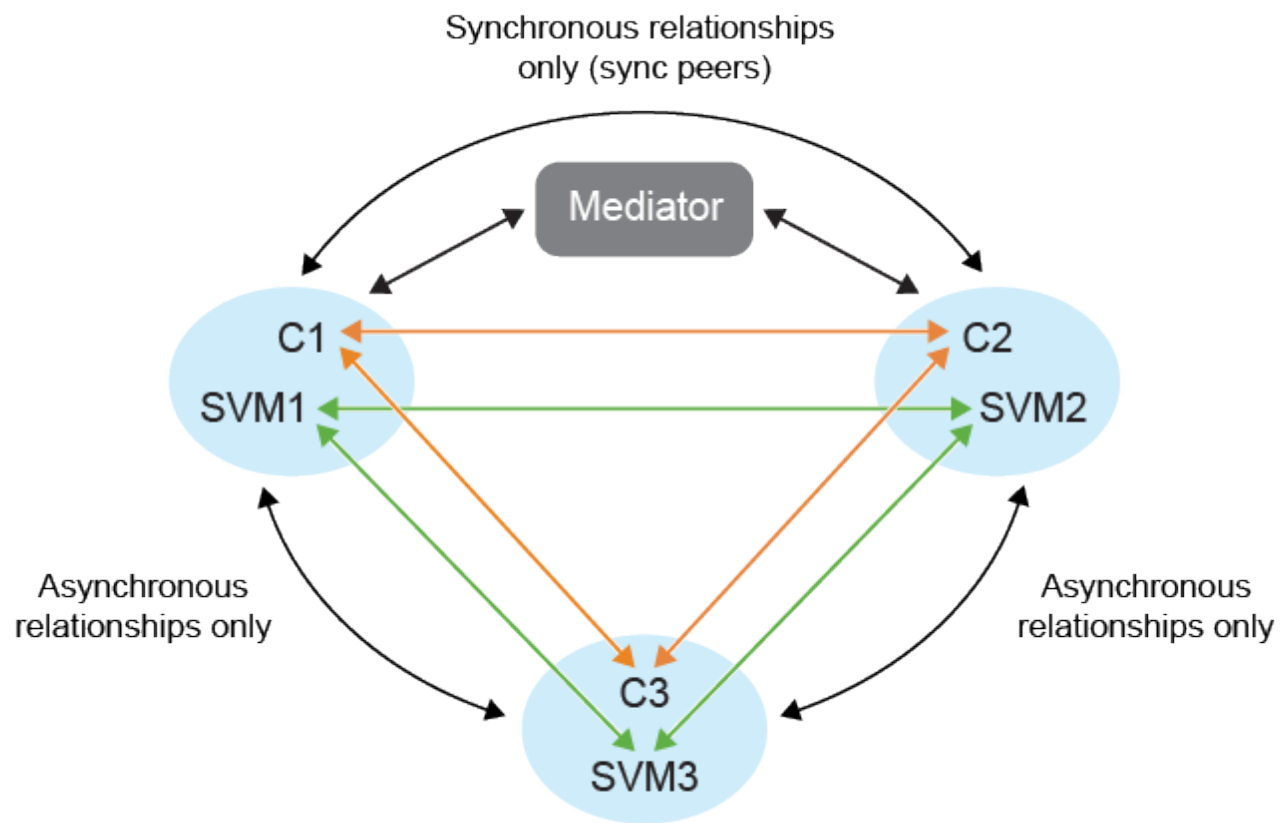
ファンアウト保護を確立するには、3 つのサイト クラスタと SVM をピアリングする必要があります。

例：

実行している場合、	それから
• ソース整合性グループはクラスタ c1 と SVM svm1 にあります • 最初の宛先コンシステンシグループはクラスタc2 とSVM svm2にあり、 • 2番目の宛先コンシステンシグループはクラスタc3とSVM svm3にあります	• ソースONTAPクラスタ上のクラスタ ピアリングは (C1、C2) と (C1、C3) になります。 • 最初の宛先ONTAPクラスタのクラスタピアリングは (C2、C1) と (C2、C3) となり、 • 2 番目の宛先ONTAPクラスタ上のクラスタ ピアリングは (C3、C1) と (C3、C2) になります。 • ソース SVM 上の SVM ピアリングは (svm1、svm2) と (svm1、svm3) になります。 • 最初の宛先SVMのSVMピアリングは(svm2、svm1)と(svm2、svm3)となり、 • 2 番目の宛先 SVM 上の SVM ピアリングは (svm3、svm1) と (svm3、svm2) になります。

次の図はファンアウト保護の構成を示しています。





手順

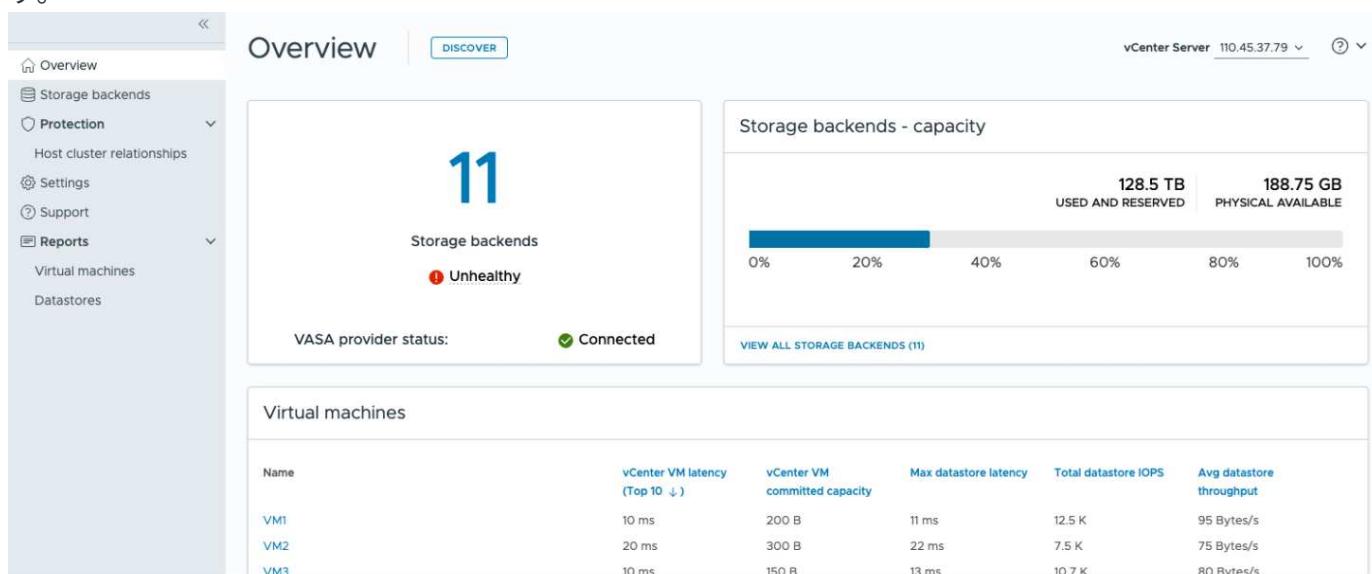
1. 新しいブレースホルダー データストアを作成します。参照する ["ブレースホルダー データストアを選択"](#)
2. ホストクラス保護にデータストアを追加する ["保護されたホスト クラスターを変更する"](#)。非同期ポリシー タイプと同期ポリシー タイプの両方を追加する必要があります。

ONTAP tools for VMware vSphereを管理する

ONTAP tools for VMware vSphereの概要

vCenter クライアントのショートカット セクションでONTAP tools for VMware vSphere プラグイン アイコンを選択すると、ユーザー インターフェイスが概要ページに移動します。このページは、ONTAP tools for VMware vSphereの概要を提供するダッシュボードのように機能します。

拡張リンク モード セットアップ (ELM) の場合、vCenter Server 選択ドロップダウンが表示され、目的の vCenter Server を選択して関連するデータを表示できます。このドロップダウンは、プラグインの他のすべてのリストビューで使用できます。1 つのページで行われた vCenter Server の選択は、プラグインのタブ全体で保持されます。



概要ページから、*検出*アクションを実行できます。検出アクションは、vCenter レベルで検出を実行し、新しく追加または更新されたストレージ バックエンド、ホスト、データストア、および保護ステータス/関係を検出します。スケジュールされた検出を待たずに、エンティティのオンデマンド検出を実行できます。



アクション ボタンは、検出アクションを実行する権限がある場合にのみ有効になります。

検出要求が送信された後、最近のタスク パネルでアクションの進行状況を追跡できます。

ダッシュボードには、システムのさまざまな要素を表示する複数のカードがあります。次の表は、さまざまなカードとそれらが表す内容を示しています。

カード	説明
-----	----

ステータス	ステータス カードには、ストレージ バックエンドの数と、ストレージ バックエンドおよび VASA プロバイダーの全体的なヘルス ステータスが表示されます。ストレージ バックエンドのステータスは、すべてのストレージ バックエンドのステータスが正常な場合は 正常 と表示され、いずれかのストレージ バックエンドに問題がある場合 (不明/到達不能/劣化ステータス) は 異常 と表示されます。ツールチップを選択すると、ストレージ バックエンドのステータスの詳細が開きます。詳細については、任意のストレージ バックエンドを選択できます。その他の VASA プロバイダの状態 リンクには、vCenter Server に登録されている VASA プロバイダの現在の状態が表示されます。
ストレージバックエンド - 容量	このカードには、選択したvCenter Serverインスタンスのすべてのストレージバックエンドの使用済み容量と使用可能容量の合計が表示されます。ASAASAストレージシステムの場合は、非集約型システムであるため、容量データは表示されません。
仮想マシン	このカードには、パフォーマンス メトリック別にソートされた上位 10 個の VM が表示されます。ヘッダーを選択すると、選択したメトリックの上位 10 個の VM が昇順または降順で並べ替えられます。カードで行われた並べ替えとフィルタリングの変更は、ブラウザのキャッシュを変更またはクリアするまで保持されます。
データストア	このカードには、パフォーマンス メトリック別にソートされた上位 10 件のデータストアが表示されます。ヘッダーを選択すると、選択したメトリックの上位 10 個のデータストアが昇順または降順で並べ替えられます。カードで行われた並べ替えとフィルタリングの変更は、ブラウザのキャッシュを変更またはクリアするまで保持されます。データストアのタイプ (NFS、VMFS、またはvVols) を選択するためのデータストア タイプ ドロップダウンがあります。
ESXi ホストコンプライアンスカード	このカードには、設定グループ/カテゴリ別に、推奨されるNetAppホスト設定に関するすべての ESXi ホスト (選択した vCenter 用) 設定の全体的なコンプライアンス ステータスが表示されます。推奨設定を適用するには、「推奨設定を適用」リンクを選択できます。ホストの準拠ステータスを選択して、ホストのリストを表示できます。

ONTAP ツール マネージャのユーザーインターフェース

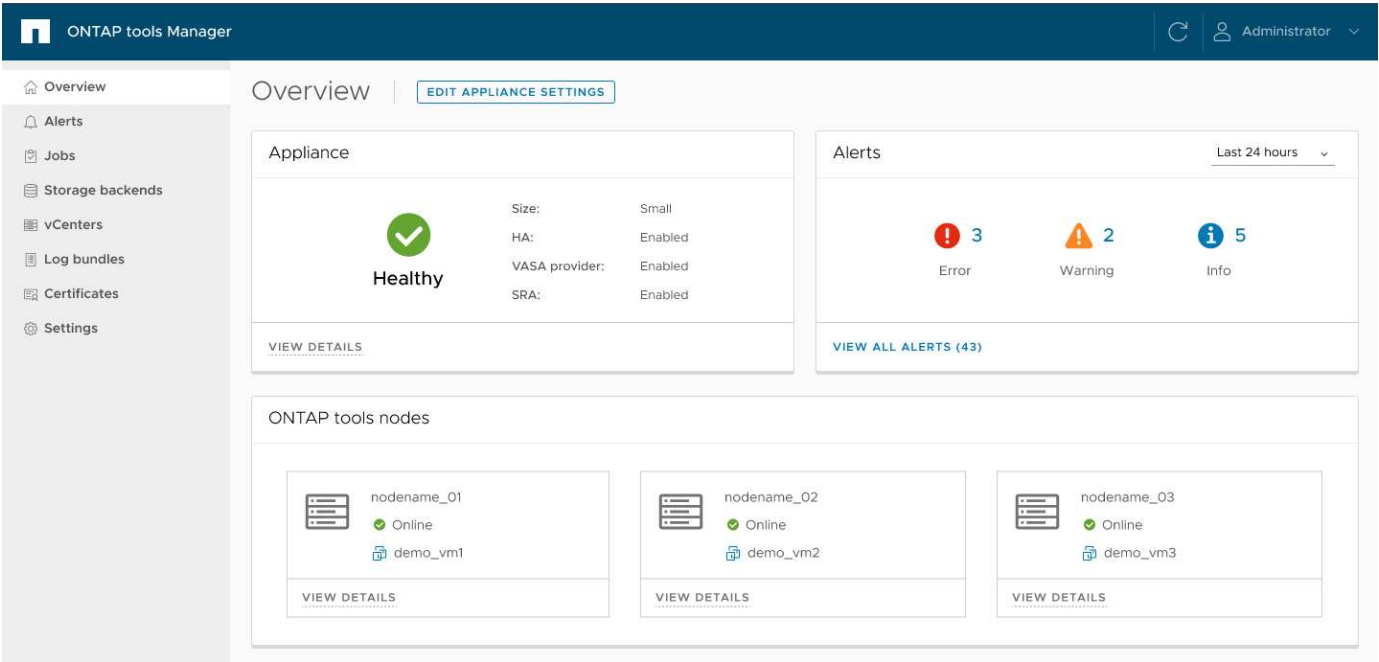
ONTAP tools for VMware vSphereは、複数の vCenter Server インスタンスを管理できるマルチテナント システムです。ONTAP ツール マネージャは、管理対象 vCenter Server インスタンスとオンボード ストレージ バックエンドに対するONTAP tools for VMware vSphere管理者のより詳細な制御機能を提供します。

ONTAPツール マネージャーは次のことに役立ちます。

- vCenter Server インスタンス管理 - ONTAPツールに vCenter Server インスタンスを追加および管理します。
- ストレージ バックエンド管理 - ONTAPストレージ クラスターをONTAP tools for VMware vSphereに追加して管理し、オンボードされた vCenter Server インスタンスにグローバルにマッピングします。
- ログ バンドルのダウンロード - ONTAP tools for VMware vSphereのログ ファイルを収集します。
- 証明書管理 - 自己署名証明書をカスタム CA 証明書に変更し、VASA プロバイダーおよびONTAPツールのすべての証明書を更新またはリフレッシュします。
- パスワード管理 - ユーザーの OVA アプリケーション パスワードをリセットします。

ONTAPツールマネージャにアクセスするには、`https://<ONTAPtoolsIP>:8443/virtualization/ui/` ブラウザから、導入時に指定したONTAP tools for VMware vSphere管理者の認証情報を使用してログインします。

ONTAPツール マネージャの概要セクションは、サービス管理、ノード サイズの拡大、高可用性 (HA) の有効化などのアプライアンス構成の管理に役立ちます。また、健全性、ネットワークの詳細、アラートなど、ノードに関連するONTAPツールの全体的な情報を監視することもできます。



カード	説明
家電カード	アプライアンス カードは、 ONTAPツール アプライアンスの全体的なステータスを提供します。アプライアンスの構成の詳細と有効なサービスのステータスが表示されます。 ONTAPツール アプライアンスの追加情報については、[詳細を表示] リンクを選択してください。アプライアンス設定アクション ジョブの編集が進行中の場合、アプライアンス ポートレットにジョブのステータスと詳細が表示されます。

カード	説明
アラートカード	アラート カードには、HA ノード レベルのアラートを含む、ONTAPツールのアラートがタイプ別にリストされます。カウントテキスト (ハイパーリンク) を選択すると、アラートのリストを表示できます。リンクをクリックすると、選択したタイプでフィルタリングされたアラート表示ページに移動します。
vCenter	vCenter カードには、システム内の vCenter の健全性状態が表示されます。
ストレージバックエンド	ストレージ バックエンド カードには、システム内のストレージ バックエンドの正常性状態が表示されます。
ONTAPツールノードカード	ONTAPツール ノード カードには、ノード名、ノード VM 名、ステータス、およびすべてのネットワーク関連データを含むノードのリストが表示されます。*詳細を表示*を選択すると、選択したノードに関連する追加の詳細を表示できます。[注意] 非 HA セットアップでは、1つのノードのみが表示されます。HA セットアップでは、3つのノードが表示されます。

ONTAP tools for VMware vSphereにおける igroup とエクスポート ポリシーを理解する

イニシエータ グループ (igroup) は、FC プロトコル ホストのワールド ワイド ポート名 (WWPN) または iSCSI ホスト修飾ノード名のテーブルです。igroupを定義してLUNにマッピングし、どのイニシエータがLUNにアクセスできるかを制御できます。

ONTAP tools for VMware vSphereでは、igroup はフラットな構造で作成および管理され、vCenter 内の各データストアは単一の igroup に関連付けられていました。このモデルでは、複数のデータストアにわたる igroup の柔軟性と再利用が制限されてきました。ONTAP tools for VMware vSphereでは、ネストされた igroup が導入されています。ネストされた igroup では、vCenter 内の各データストアが親 igroup に関連付けられ、各ホストはその親の下の子 igroup にリンクされます。複数のデータストア間で再利用できるように、ユーザー定義の名前を持つカスタムの親 igroup を定義して、より柔軟で相互接続された igroup の管理を実現できます。igroup ワークフローを理解することは、ONTAP tools for VMware vSphereで LUN とデータストアを効果的に管理するために不可欠です。次の例に示すように、ワークフローによって異なる igroup 構成が生成されます。



記載されている名前は説明のみを目的としており、実際の igroup 名を指すものではありません。ONTAPツールで管理される igroup は、プレフィックス「otv_」を使用します。カスタム igroup には任意の名前を付けることができます。

期間	説明
DS<番号>	データストア
iqn<番号>	イニシエーターIQN
ホスト<番号>	ホストMoRef
lun<数値>	LUN ID

<DSName>igroup<番号>	デフォルト（ONTAPツール管理）の親igroup
<Host-Moref>igroup<番号>	子igroup
Customigroup<番号>	ユーザー定義のカスタム親 igroup
Classicigroup<番号>	ONTAPツール 9.x バージョンで使用される igroup。

例1：

1つのイニシエータを持つ単一のホスト上にデータストアを作成する

ワークフロー: [作成] DS1 (lun1): host1 (iqn1)

結果：

- DS1igroup :
 - ホスト1igroup → (iqn1: lun1)

DS1 のONTAPシステム上に親 igroup DS1igroup が作成され、子 igroup host1igroup が lun1 にマッピングされます。LUN は常に子 igroup にマップされます。

例2：

既存のデータストアを追加ホストにマウントする

ワークフロー: [マウント] DS1 (lun1): host2 (iqn2)

結果：

- DS1igroup :
 - ホスト1igroup → (iqn1: lun1)
 - ホスト2igroup → (iqn2: lun1)

子 igroup host2igroup が作成され、既存の親 igroup DS1igroup に追加されます。

例3：

ホストからデータストアをアンマウントする

ワークフロー: [アンマウント] DS1 (lun1): host1 (iqn1)

結果：

- DS1igroup :
 - ホスト2igroup → (iqn2: lun1)

host1igroup は階層から削除されます。子 igroup は明示的に削除されません。削除は次の 2 つの条件下で発生します。

- LUN がマップされていない場合、ONTAPシステムは子 igroup を削除します。
- スケジュールされたクリーンアップジョブにより、LUN マッピングのない、ぶら下がっている子 igroup が削除されます。これらのシナリオは、ONTAPツールで管理される igroup にのみ適用され、カスタム作

成された igroup には適用されません。

例4：

データストアを削除

ワークフロー: [削除] DS1 (lun1): host2 (iqn2)

結果：

- DS1lgroup :
 - ホスト2lグループ → (iqn2: lun1)

別のデータストアが親 igroup を再利用しない場合、親 igroup と子 igroup は削除されます。子igroupは明示的に削除されることはありません

例5：

カスタム親igroupの下に複数のデータストアを作成する

ワークフロー:

- [作成] DS2 (lun2): ホスト1 (iqn1)、ホスト2 (iqn2)
- [作成] DS3 (lun3): host1 (iqn1)、host3 (iqn3)

結果：

- Customlgroup1 :
 - host1lgroup → (iqn1: lun2、lun3)
 - ホスト2lグループ → (iqn2: lun2)
 - ホスト3lグループ → (iqn3: lun3)

Customlgroup1 は DS2 用に作成され、DS3 に再利用されます。子 igroup は共有親の下に作成または更新され、各子 igroup は関連する LUN にマッピングされます。

例6：

カスタム親 igroup の下にある 1 つのデータストアを削除します。

ワークフロー: [削除] DS2 (lun2): host1 (iqn1)、host2 (iqn2)

結果：

- Customlgroup1 :
 - ホスト1lグループ → (iqn1: lun3)
 - ホスト3lグループ → (iqn3: lun3)
- Customlgroup1 は再利用されませんが、削除されません。
- LUN がマップされていない場合、ONTAPシステムは host2lgroup を削除します。
- host1lgroupはDS3のlun3にマッピングされているため削除されません。カスタムigroupは、再利用ステータスに関わらず削除されることはありません。

例7：

vVolsデータストアの拡張（ボリュームの追加）

ワークフロー：

拡張前：

[展開] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

拡張後：

[展開] DS4 (lun4、lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4、lun5)

新しい LUN が作成され、既存の子 igroup host4Igroup にマップされます。

例8：

vVolsデータストアの縮小（ボリュームの削除）

ワークフロー：

収縮前：

[縮小] DS4 (lun4、lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4、lun5)

縮小後：

[縮小] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

指定された LUN (lun5) は子 igroup からマッピング解除されています。igroup は、少なくとも 1 つの LUN がマップされている限りアクティブなままです。

例9：

ONTAPツール9から10への移行（igroupの正規化）

ワークフロー

VMware vSphere 9.x バージョン用のONTAPツールは、階層型 igroup をサポートしていません。10.3 以降のバージョンへの移行中は、igroup を階層構造に正規化する必要があります。

移行前：

[移行] DS6 (lun6、lun7): host6 (iqn6)、host7 (iqn7) → ClassicIgroup1 (iqn6 & iqn7: lun6、lun7)

ONTAPツール 9.x ロジックでは、1 対 1 のホスト マッピングを強制することなく、igroup ごとに複数のイニ

シエータが許可されます。

移行後:

[移行] DS6 (lun6、lun7): host6 (iqn6)、host7 (iqn7) → Classiclgroup1: otv_Classiclgroup1 (iqn6 & iqn7: lun6、lun7)

移行中:

- 新しい親 igroup (Classiclgroup1) が作成されます。
- 元の igroup の名前は otv_ プレフィックス付きで変更され、子 igroup になります。

これにより、階層モデルへの準拠が保証されます。

関連トピック

["igroupについて"](#)

エクスポート ポリシー

エクスポート ポリシーは、ONTAP tools for VMware vSphere内の NFS データストアへのアクセスを制御します。これらは、どのクライアントがデータストアにアクセスでき、どのような権限を持つかを定義します。エクスポート ポリシーはONTAPシステムで作成および管理され、NFS データストアに関連付けてアクセス制御を適用できます。各エクスポート ポリシーは、アクセスが許可されるクライアント (IP アドレスまたはサブネット) と付与される権限 (読み取り専用または読み取り/書き込み) を指定するルールで構成されます。

ONTAP tools for VMware vSphereで NFS データストアを作成するときに、既存のエクスポート ポリシーを選択するか、新しいエクスポート ポリシーを作成できます。次に、エクスポート ポリシーがデータストアに適用され、承認されたクライアントのみがデータストアにアクセスできるようになります。

新しい ESXi ホストに NFS データストアをマウントすると、ONTAP tools for VMware vSphere、データストアに関連付けられている既存のエクスポート ポリシーにホストの IP アドレスが追加されます。これにより、新しいエクスポート ポリシーを作成しなくても、新しいホストがデータストアにアクセスできるようになります。

ESXi ホストから NFS データストアを削除またはアンマウントすると、ONTAP tools for VMware vSphere、エクスポート ポリシーからホストの IP アドレスが削除されます。他のホストがそのエクスポート ポリシーを使用していない場合は、そのエクスポート ポリシーは削除されます。NFS データストアを削除すると、そのデータストアに関連付けられているエクスポート ポリシーが他のデータストアで再利用されていない場合、ONTAP tools for VMware vSphereそのデータストアが削除されます。エクスポート ポリシーが再利用される場合、ホスト IP アドレスは保持され、変更されません。データストアを削除すると、エクスポート ポリシーによってホスト IP アドレスの割り当てが解除され、デフォルトのエクスポート ポリシーが割り当てられるため、必要に応じてONTAPシステムがデータストアにアクセスできるようになります。

エクスポートポリシーを異なるデータストア間で再利用する場合、割り当て方法が異なります。エクスポートポリシーを再利用する際は、新しいホストIPアドレスをポリシーに追加できます。共有エクスポートポリシーを使用しているデータストアを削除またはアンマウントしても、ポリシーは削除されません。ポリシーは変更されず、ホストIPアドレスも削除されません。これは、他のデータストアと共有されているためです。エクスポートポリシーの再利用は、アクセスやレイテンシの問題につながる可能性があるため、推奨されません。

関連トピック

["エクスポート ポリシーの作成"](#)

ONTAPツールで管理されるigroupを理解する

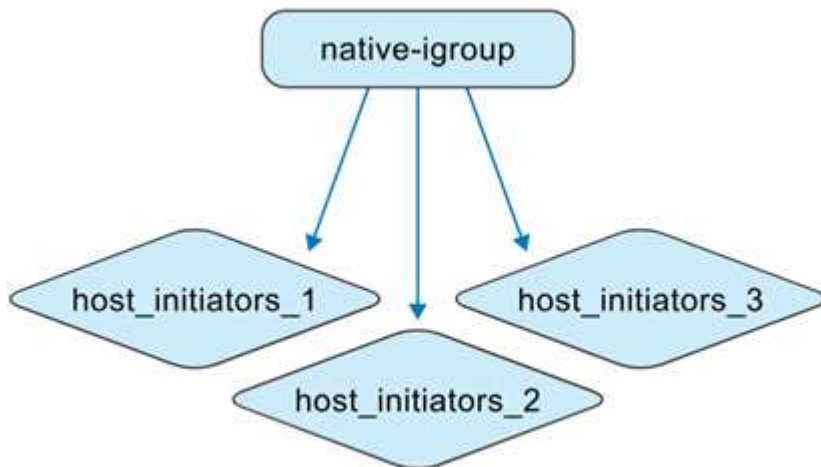
ONTAPツール VM とONTAPストレージ システムの両方を管理する場合、特にデータストアを非ONTAPツール環境からONTAPツール管理に移行する場合は、igroup の動作を理解することが重要です。このセクションでは、この移行中に igroup がどのように更新されるかについて説明します。

ONTAP tools for VMware vSphereは、VMware データセンター環境内でのONTAPおよび vCenter オブジェクトの作成とメンテナンスを自動化することで、データストアの管理を簡素化します。

ONTAP tools for VMware vSphereは、igroup を 2 つの異なるコンテキストで解釈します。

ONTAPツール以外で管理されるigroup

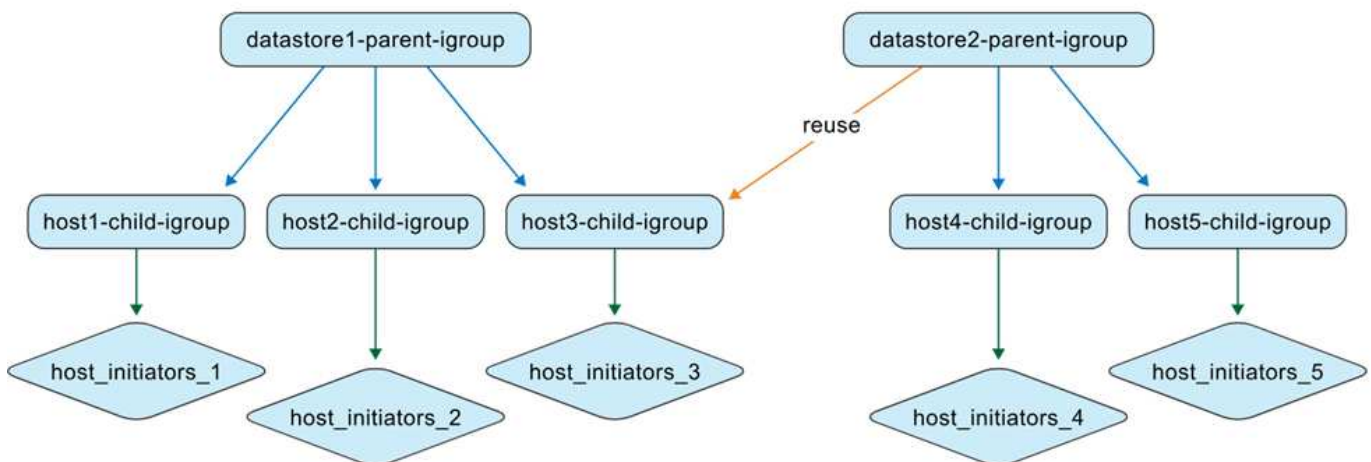
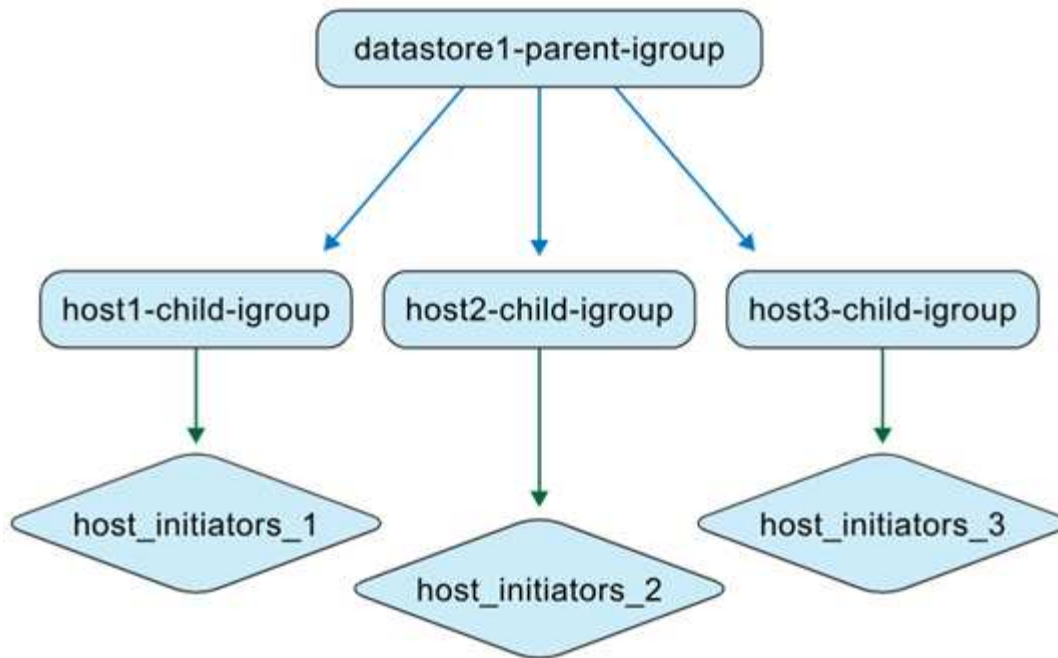
ストレージ管理者は、ONTAPシステム上にフラット構造またはネスト構造の igroup を作成できます。この図は、ONTAPシステムで作成されたフラット igroup を示しています。



ONTAPツールが管理するigroup

データストアを作成すると、ONTAP tools for VMware vSphereは、LUN マッピングを容易にするためにネストされた構造を使用して igroup を自動的に作成します。

たとえば、データストア 1 がホスト 1、2、3 に作成されてマウントされ、新しいデータストア (データストア 2) がホスト 3、4、5 に作成されてマウントされると、ONTAPツールは効率的な管理のためにホスト レベルの igroup を再利用します。



ここでは、ONTAP tools for VMware vSphereのいくつかの事例を示します。

デフォルトの**igroup**設定でデータストアを作成する場合

データストアを作成し、igroup フィールドを空白のままにすると（デフォルト設定）、ONTAPツールによってそのデータストアのネストされた igroup 構造が自動的に生成されます。データストア レベルの親 igroup は、otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name> というパターンを使用して名前が付けられます。各ホスト レベルの子 igroup は、otv_<hostMoref>_<vcguid> というパターンに従います。ONTAP ストレージ インターフェイスの 親イニシエータ グループ セクションで、親（データストア レベル）と子（ホスト レベル）igroup 間の関連付けを表示できます。

ネストされた igroup アプローチでは、LUN は子 igroup にのみマッピングされます。その後、vCenter Server インベントリに新しいデータストアが表示されます。

カスタム**igroup**名でデータストアを作成する場合

ONTAPツールでデータストアを作成するときに、ドロップダウンから選択する代わりに、カスタム igroup 名

を入力できます。次に、ONTAPツールは指定された名前を使用してデータストアレベルで親 igroup を作成します。複数のデータストアに同じホストが使用される場合、既存のホストレベル (子) igroup が再利用されます。その結果、新しいデータストアの LUN はこの既存の子 igroup にマップされ、複数の親 igroup (データストアごとに 1 つ) に関連付けられる可能性があります。vCenter Server ユーザー インターフェイスのデータストア リストで、カスタム igroup 名を持つ新しいデータストアが正常に作成されたことが確認されます。

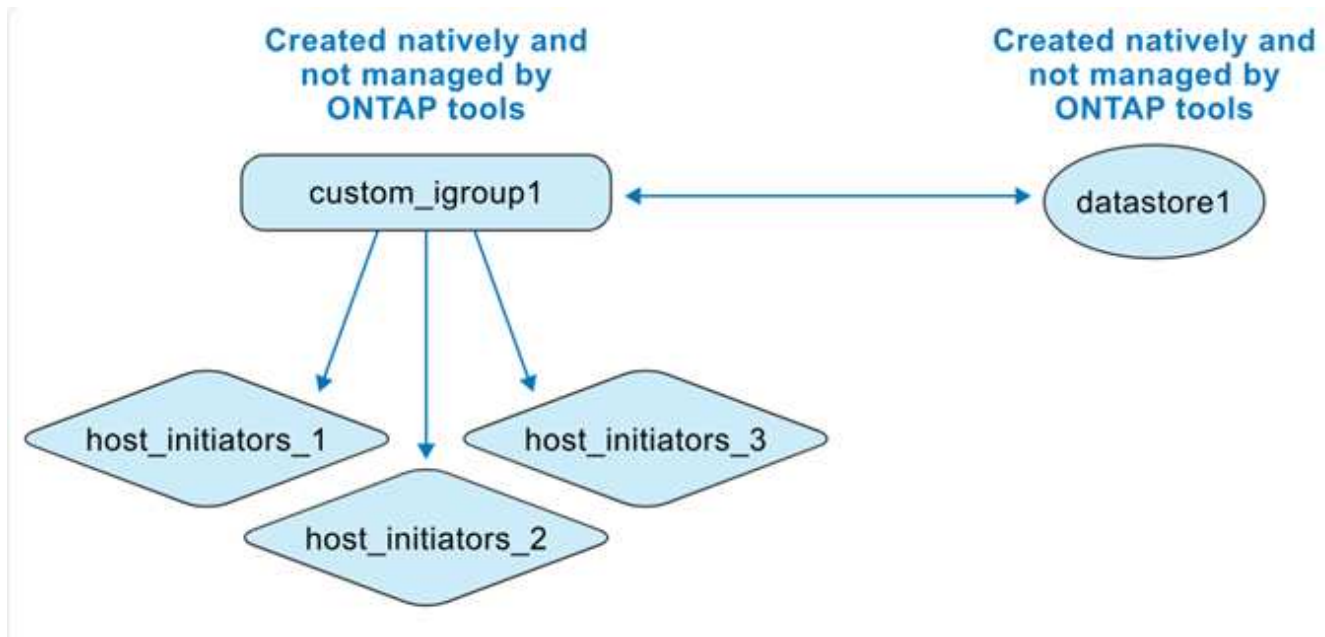
データストアの作成時に **igroup** 名を再利用する場合

ONTAPツールのユーザー インターフェイスを使用してデータストアを作成するときに、ドロップダウン リストから既存のカスタム親 igroup を選択できます。親 igroup を再利用して別のデータストアを作成すると、ONTAPシステムのユーザー インターフェイスにこの関連付けが表示されます。新しいデータストアは vCenter Server ユーザー インターフェイスにも表示されます。

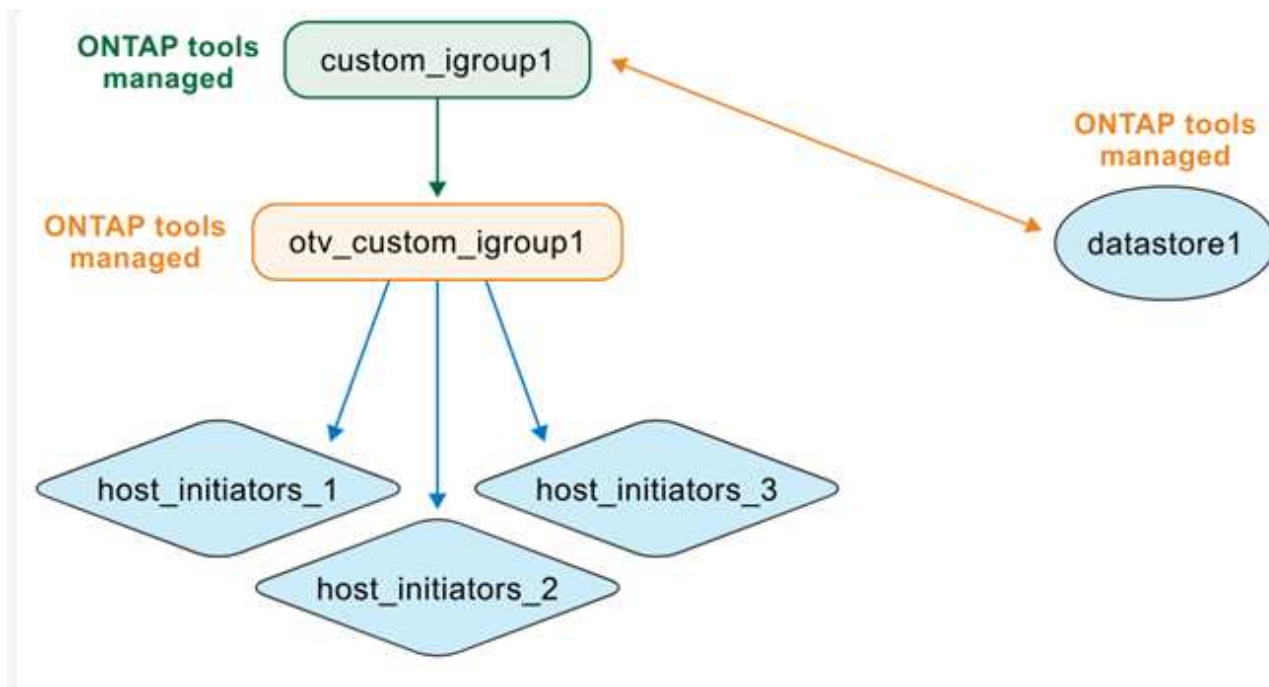
この操作は API を使用して実行することもできます。データストアの作成中に既存の igroup を再利用するには、API リクエスト ペイロードで igroup UUID を指定します。

- ONTAPとvCenterからネイティブにデータストアとigroupを作成する場合*

ONTAPシステムおよび VMware 環境で igroup およびデータストアを直接作成する場合、最初はONTAPツールはこれらのオブジェクトを管理しません。これにより、フラットな igroup 構造が作成されます。



ONTAPツールを使用して既存のデータストアと igroup を管理するには、データストアの検出を実行する必要があります。ONTAPツールは、データストアと igroup を識別して登録し、データベース内のネストされた構造に変換します。カスタム名を使用して新しい親 igroup が作成され、既存の igroup は「otv_」プレフィックスを使用して名前が変更され、子 igroup になります。イニシエーター マッピングは変更されません。検出中に、データストアにマップされた igroup のみが変換されます。この後、igroup 構造は次の図のようになります。



vCenter Server でデータストアを直接作成し、後でONTAPツールの管理下に置くことができます。まず、ONTAPシステムにフラット igroup を作成し、それに LUN をマップします。ONTAPツールでデータストア検出を実行すると、フラット igroup はネストされた構造に変換されます。その後、ONTAPツールは igroup を管理し、その名前を「otv_」プレフィックスに変更します。このプロセス全体を通じて、LUN は同じ igroup にマップされたままになります。

- ONTAPツールがネイティブに作成された igroup を再利用する方法*

ONTAPで管理した後、その igroup を使用してONTAPツールでデータストアをプロビジョニングできます。これらの igroup は、カスタム イニシエータ グループ名のドロップダウン リストに表示されます。次に、データストアの新しい LUN が、対応する正規化された子 igroup (「otv_Nativegroup1」など) にマップされます。

ONTAP tools for VMware vSphereは、ONTAPツールによって管理されていない、またはデータストアにリンクされていないONTAPシステムで作成された igroup を検出または使用しません。

ONTAP tools for VMware vSphereを有効にする

ONTAPツール マネージャを使用して管理者パスワードを変更し、ONTAPツール マネージャを使用して VASA プロバイダ、vVols構成のインポート、ディザスタ リカバリ (SRA) などのサービスを有効にすることができます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. 概要セクションで*アプライアンス設定の編集*を選択します。
4. サービス セクションでは、要件に応じて、VASA プロバイダー、vVols構成のインポート、災害復旧 (SRA) などのオプション サービスを有効にできます。

サービスを初めて有効にする場合は、VASA プロバイダーと SRA の資格情報を作成する必要があります。これらは、vCenter Server で VASA プロバイダーおよび SRA サービスを登録または有効化するために使用されます。ユーザー名には文字、数字、アンダースコアのみを含めることができます。パスワードの長さは 8 ～ 256 文字にする必要があります。



オプションのサービスを無効にする前に、ONTAP ツールによって管理される vCenter Server がそれらのサービスを使用していないことを確認してください。

- vVols 構成のインポートを許可する* オプションは、VASA プロバイダー サービスが有効になっている場合にのみ表示されます。このオプションにより、ONTAP ツール 9.xx から ONTAP ツール 10.4 への vVols データの移行が可能になります。

ONTAP tools for VMware vSphere を変更する

ONTAP ツール マネージャーを使用して、ONTAP tools for VMware vSphere をスケールアップし、展開内のノードの数を増やしたり、構成を高可用性 (HA) セットアップに変更したりします。ONTAP tools for VMware vSphere は、最初は単一ノードの非 HA 構成で導入されます。



非 HA バックアップが有効になっているときに HA に移行するには、まずバックアップを無効にし、移行後に再度有効にします。

開始する前に

- OVA テンプレートの OVA バージョンがノード 1 と同じであることを確認します。ノード 1 は、ONTAP tools for VMware vSphere が最初に導入されるデフォルト ノードです。
- 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。
- vCenter Server で、Disaster Recovery Service (DRS) の自動化レベルを部分的に自動化に設定します。HA を展開した後、完全に自動化された状態に戻します。
- HA セットアップ内のノード ホスト名は小文字にする必要があります。

手順

1. Web ブラウザから ONTAP ツール マネージャーを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定した ONTAP tools for VMware vSphere 管理者認証情報を使用してログインします。
3. 概要セクションで*アプライアンス設定の編集*を選択します。
4. *構成*セクションでは、スケールアップしてノード サイズを増やし、要件に応じて HA 構成を有効にすることができます。変更を行うには、vCenter Server の認証情報が必要です。

ONTAP ツールが HA 構成の場合、コンテンツ ライブラリの詳細を変更できます。新しい編集を送信するには、パスワードを再度入力する必要があります。



ONTAP tools for VMware vSphere では、ノード サイズを増やすことしかできず、ノード サイズを縮小することはできません。HA 以外のセットアップでは、中規模の構成のみがサポートされます。HA セットアップでは、中規模および大規模の構成がサポートされます。

5. HA トグル ボタンを使用して HA 構成を有効にします。 **HA 設定** ページで、次の点を確認します。

- コンテンツライブラリは、ONTAPツールノードVMが実行されるvCenter Serverと同じvCenter Serverに属します。vCenter Serverの認証情報は、アプライアンスの変更に必要なOVAテンプレートの検証とダウンロードに使用されます。
- ONTAPツールをホストする仮想マシンは、ESXi ホストに直接展開されません。VM はクラスターまたはリソース プールにデプロイする必要があります。



HA 構成を有効にした後は、非 HA 単一ノード構成に戻すことはできません。

6. アプライアンス設定の編集 ウィンドウの **HA 設定** セクションで、ノード 2 と 3 の詳細を入力できます。ONTAP tools for VMware vSphereは、HA セットアップで 3 つのノードをサポートします。



ワークフローを容易にするために、ほとんどの入力オプションにはノード 1 ネットワークの詳細が事前に入力されています。ただし、ウィザードの最終ページに進む前に入力データを編集することはできます。最初のノードで IPv6 アドレスが有効になっている場合にのみ、他の 2 つのノードの IPv6 アドレスの詳細を入力できます。

ESXi ホストにONTAPツール VM が 1 つだけ含まれていることを確認します。次のウィンドウに移動するたびに入力が検証されます。

7. 概要 セクションの詳細を確認し、変更を 保存 します。

次の手順

概要 ページには、デプロイメントのステータスが表示されます。ジョブ ID を使用すると、ジョブ ビューからアプライアンス設定編集ジョブのステータスを追跡することもできます。

HA の展開が失敗し、新しいノードのステータスが「新規」と表示される場合は、HA の有効化操作を再試行する前に、vCenter で新しい VM を削除します。

左側のパネルの アラート タブには、ONTAP tools for VMware vSphereのアラートが一覧表示されます。

データストアの管理

NFSおよびVMFSデータストアをマウントする

追加のホストにデータストアをマウントすると、そ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。ホストをVMware環境に追加したあとで、そのホストにデータストアをマウントできます。

タスク概要

- vSphere クライアントのバージョンと選択したデータストアのタイプによっては、一部の右クリック アクションが無効になったり使用できなくなったりします。
 - vSphere クライアント 8.0 以降のバージョンを使用している場合、右クリック オプションの一部は非表示になります。
 - vSphere 7.0U3 から vSphere 8.0 バージョンでは、オプションは表示されますが、アクションは無効になります。

- ホスト クラスターが均一な構成で保護されている場合、データストアのマウント オプションは無効になります。

手順

1. vSphere Client のホームページから、[ホストとクラスター] を選択します。
2. 左側のナビゲーション ペインで、ホストが含まれているデータ センターを選択します。
3. NFS/VMFS データストアをホストまたはホスト クラスターにマウントするには、右クリックして * NetApp ONTAP ツール* > * データストアのマウント* を選択します。
4. マウントするデータストアを選択し、「マウント」を選択します。

次の手順

最近のタスク パネルで進行状況を追跡できます。

NFSおよびVMFSデータストアのマウント解除

データストアのアンマウント アクションは、ESXi ホストから NFS または VMFS データストアをアンマウントします。データストアのアンマウント アクションは、ONTAP tools for VMware vSphereによって検出または管理される NFS および VMFS データストアに対して有効になります。

手順

1. vSphere クライアントにログインします。
2. NFS または VMFS データストア オブジェクトを右クリックし、データストアのマウント解除 を選択します。

ダイアログ ボックスが開き、データストアがマウントされている ESXi ホストが一覧表示されます。保護されたデータストアに対して操作を実行すると、画面に警告メッセージが表示されます。

3. データストアをアンマウントする 1 つ以上の ESXi ホストを選択します。

すべてのホストからデータストアをアンマウントすることはできません。ユーザー インターフェイスでは、代わりにデータストアの削除操作を使用することが提案されます。

4. *アンマウント*ボタンを選択します。

データストアが保護されたホスト クラスターの一部である場合は、警告メッセージが表示されます。



。"保護されたホスト クラスターを変更する"完全な保護を可能にします。

次の手順

最近のタスク パネルで進行状況を追跡できます。

vVolデータストアのマウント

VMware Virtual Volumes (vVols) データストアを 1 つ以上の追加ホストにマウントして、追加ホストへのストレージ アクセスを提供できます。vVolsデータストアのマウント解

除は API 経由でのみ行えます。

手順

1. vSphere Client のホームページから、[ホストとクラスタ] を選択します。
2. ナビゲーション ペインで、データストアが含まれているデータ センターを選択します。
3. データストアを右クリックし、* NetApp ONTAP ツール* > * データストアのマウント* を選択します。
4. ホストにデータストアをマウント ダイアログ ボックスで、データストアをマウントするホストを選択し、マウント を選択します。

最近のタスク パネルで進行状況を追跡できます。

NFS および VMFS データストアのサイズ変更

データストアのサイズを変更すると、仮想マシン ファイル用のストレージを増やすことができます。インフラストラクチャの要件の変化に応じて、データストアのサイズを変更できます。

このタスクについて

NFS および VMFS データストアのサイズのみを増やすことができます。NFS および VMFS データストアの一部である FlexVol volume は、既存のサイズより小さくすることはできませんが、最大 120% まで拡張できます。

手順

1. vSphere Client のホームページから、[ホストとクラスタ] を選択します。
2. ナビゲーション ペインで、データストアが含まれているデータ センターを選択します。
3. NFS または VMFS データストアを右クリックし、* NetApp ONTAP ツール* > * データストアのサイズ変更* を選択します。
4. [サイズ変更] ダイアログ ボックスで、データストアの新しいサイズを指定し、[OK] を選択します。

vVols データストアを拡張する

vCenter オブジェクト ビューでデータストア オブジェクトを右クリックすると、プラグイン セクションの下に、ONTAP tools for VMware vSphere でサポートされているアクションが表示されます。データストアの種類と現在のユーザー権限に応じて、特定のアクションが有効になります。



vVols データストアの拡張操作は、ASA r2 システムベースの vVols データストアには適用されません。

手順

1. vSphere Client のホームページから、[ホストとクラスタ] を選択します。
2. ナビゲーション ペインで、データストアが含まれているデータ センターを選択します。
3. データストアを右クリックし、* NetApp ONTAP ツール* > * データストアにストレージを追加* を選択します。

4. *ボリュームの作成または選択*ウィンドウでは、新しいボリュームを作成するか、既存のボリュームから選択することができます。ユーザー インターフェースは説明不要です。選択に応じて指示に従ってください。
5. *概要*ウィンドウで選択内容を確認し、*展開*を選択します。最近のタスク パネルで進行状況を追跡できます。

vVols データストアを縮小する

データストアの削除アクションは、選択したデータストアにvVolsがない場合にデータストアを削除します。



ASA r2 システムベースのvVolsデータストアでは、vVolsデータストアの縮小操作はサポートされていません。

手順

1. vSphere Client のホームページから、[ホストとクラスタ] を選択します。
2. ナビゲーション ペインで、データストアが含まれているデータ センターを選択します。
3. vVol データストアを右クリックし、* NetApp ONTAP ツール* > * データストアからストレージを削除* を選択します。
4. vVolsがないボリュームを選択し、[削除] を選択します。



vVolsが存在するボリュームを選択するオプションは無効になっています。

5. ストレージの削除*ポップアップで、ONTAP クラスターからボリュームを削除*チェックボックスを選択して、データストアとONTAPストレージからボリュームを削除し、*削除*を選択します。

データストアを削除する

データストアからストレージを削除するアクションは、vCenter Server 内の VMware vSphere によって検出または管理されているvVolsデータストアのONTAP tools for VMware vSphereでサポートされています。このアクションにより、vVolsデータストアからボリュームを削除できます。

特定のボリュームにvVolsが存在する場合、削除オプションは無効になります。データストアからボリュームを削除するだけでなく、ONTAPストレージ上の選択したボリュームを削除することもできます。

vCenter Server のONTAP tools for VMware vSphereからデータストアを削除するタスクは、次の操作を実行します。

- vVol コンテナをアンマウントする。
- igroup をクリーンアップします。igroupが使用されていない場合は、iqnをigroupから削除する。
- vVol コンテナを削除する。
- FlexVolはストレージ アレイに残す。

vCenter Server のONTAPツールから NFS、VMFS、または vVOL データストアを削除するには、次の手順に従います。

手順

1. vSphere クライアントにログインします。
2. ホスト システム、ホスト クラスタ、またはデータ センターを右クリックし、* NetApp ONTAPツール* > * データストアの削除* を選択します。



そのデータストアを使用している仮想マシンがある場合、そのデータストアを削除することはできません。データストアを削除する前に、仮想マシンを別のデータストアに移動する必要があります。データストアが保護されたホスト クラスターに属している場合は、ボリューム削除チェックボックスを選択できません。

- a. NFS または VMFS データストアの場合、データストアを使用している VM のリストを含むダイアログボックスが表示されます。
 - b. VMFS データストアがASA r2 システム上に作成され、保護の一部である場合は、削除する前にデータストアの保護を解除する必要があります。
 - c. vVolsデータストアの場合、データストアの削除アクションでは、それに関連付けられたvVolsがない場合にのみデータストアが削除されます。データストアの削除ダイアログ ボックスには、ONTAPクラスタからボリュームを削除するオプションがあります。
 - d. ASA r2 システム ベースのvVolsデータストアの場合、バックアップ ボリュームを削除するチェックボックスは適用されません。
3. ONTAPストレージ上のバックアップ ボリュームを削除するには、* ONTAPクラスター上のボリュームの削除* を選択します。



保護されたホスト クラスターの一部である VMFS データストアのONTAPクラスタ上のボリュームを削除することはできません。

データストアのONTAPストレージビュー

ONTAP tools for VMware vSphereは、構成タブにデータストアとそのボリュームのONTAPストレージ側のビューを表示します。

手順

1. vSphere クライアントからデータストアに移動します。
2. 右側のペインで*構成*タブを選択します。
3. * NetApp ONTAPツール* > * ONTAPストレージ* を選択します。データストアの種類に応じて、ビューは変わります。詳細については、以下の表を参照してください。

データストアの種類	情報あり
NFSデータストア	ストレージの詳細 ページには、ストレージ バックエンド、アグリゲート、ボリュームの情報が含まれています。 NFS 詳細 ページには、NFS データストアに関連するデータが含まれています。

VMFSデータストア	ストレージの詳細 ページには、ストレージ バックエンド、アグリゲート、ボリューム、およびストレージ 可用性ゾーン (SAZ) の詳細が表示されます。ストレージ ユニットの詳細 ページには、ストレージ ユニットの詳細が表示されます。
vVolsデータストア	すべてのボリュームを一覧表示します。ONTAPストレージ ペインからストレージを拡張または削除できます。このビューは、ASA r2 システムベースのvVolsデータストアではサポートされていません。

仮想マシンのストレージビュー

ストレージ ビューには、仮想マシンによって作成されたvVolsのリストが表示されます。



このビューは、ONTAP tools for VMware vSphere管理対象vVolsデータストア関連ディスク用のONTAP ツールが少なくとも1つマウントされているVMに適用されます。

手順

1. vSphere Client から仮想マシンに移動します。
2. 右側のペインで*モニター*タブを選択します。
3. *NetApp ONTAPツール* > ストレージ を選択します。*ストレージ*の詳細が右側のペインに表示されます。VM上に存在するvVolsのリストを表示できます。

「列の管理」オプションを使用して、さまざまな列を非表示または表示できます。

ストレージしきい値を管理する

ボリュームと合計容量が特定のレベルに達したときに vCenter Server で通知を受信するためのしきい値を設定できます。

手順：

1. vSphere クライアントにログインします。
2. ショートカット ページで、プラグイン セクションの *NetApp ONTAPツール* を選択します。
3. ONTAPツールの左ペインで、設定 > しきい値設定 > 編集 に移動します。
4. *しきい値の編集*ウィンドウで、*ほぼ満杯*フィールドと*満杯*フィールドに必要な値を入力し、*保存*を選択します。数値を推奨値（ほぼ満タンの場合は 80、満タンの場合は 90）にリセットできます。

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、ESXi ホストがデータ ストレージに使用するシステムです。

ストレージを発見

スケジュールされた検出によってストレージの詳細が更新されるのを待たずに、ストレージ バックエンドの検出をオンデマンドで実行できます。

ストレージ バックエンドを検出するには、以下の手順に従います。

手順

1. vSphere クライアントにログインします。
2. ショートカット ページで、プラグイン セクションの * NetApp ONTAPツール* を選択します。
3. ONTAPツールの左側のペインで、ストレージ バックエンド に移動し、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選択し、「ストレージの検出」を選択します。

最近のタスク パネルで進行状況を追跡できます。

ストレージバックエンドを変更する

ストレージ バックエンドを変更するには、このセクションの手順に従います。

1. vSphere クライアントにログインします。
2. ショートカット ページで、プラグイン セクションの * NetApp ONTAPツール* を選択します。
3. ONTAPツールの左側のペインで、ストレージ バックエンド に移動し、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選択し、[変更] を選択して資格情報またはポート名を変更します。最近のタスク パネルで進行状況を追跡できます。

次の手順に従って、ONTAPツール マネージャを使用してグローバルONTAPクラスタの変更操作を実行できます。

1. Web ブラウザからONTAPツール マネージャを起動します。
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーからストレージ バックエンドを選択します。
4. 変更するストレージ バックエンドを選択します。
5. 縦の省略記号メニューを選択し、[変更] を選択します。
6. 資格情報またはポートを変更できます。ストレージ バックエンドを変更するには、ユーザー名 と パスワード を入力します。

ストレージバックエンドを削除する

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、以下の手順に従います。

1. vSphere クライアントにログインします。

2. ショートカット ページで、プラグイン セクションの * NetApp ONTAPツール* を選択します。
3. ONTAPツールの左側のペインで、ストレージ バックエンド に移動し、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選択し、[削除] を選択します。ストレージ バックエンドにデータストアが含まれていないことを確認します。最近のタスク パネルで進行状況を追跡できます。

ONTAPツール マネージャを使用して、グローバルONTAPクラスタの削除操作を実行できます。

1. Web ブラウザからONTAPツール マネージャを起動します。
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから*ストレージ バックエンド*を選択します。
4. 削除するストレージバックエンドを選択します
5. 縦の省略記号メニューを選択し、[削除] を選択します。

ストレージバックエンドのドリルダウンビュー

ストレージ バックエンド ページには、すべてのストレージ バックエンドが一覧表示されます。ストレージの検出、変更、および削除の操作は、クラスタの下の子 SVM ではなく、追加したストレージ バックエンドに対して実行できます。

ストレージ バックエンドの下の子クラスターまたは子クラスターのいずれかを選択すると、コンポーネントの全体的な概要が表示されます。親クラスターを選択すると、アクション ドロップダウンが表示され、そこからストレージの検出、変更、削除の操作を実行できます。

概要ページには次の詳細が表示されます。

- ストレージバックエンドのステータス
- 容量情報
- VMに関する基本情報
- ネットワークの IP アドレスやポートなどのネットワーク情報。子 SVM の場合、情報は親ストレージ バックエンドと同じになります。
- ストレージ バックエンドに対して許可および制限されるPrivileges。子 SVM の場合、情報は親ストレージ バックエンドと同じになります。Privilegesは、クラスターベースのストレージ バックエンドにのみ表示されます。SVM をストレージ バックエンドとして追加すると、権限情報は表示されません。
- SVM またはクラスタの分離プロパティが「true」に設定されている場合、ASA r2 システム クラスタのドリルダウン ビューにはローカル層タブが含まれません。
- ASA r2 SVM システムの場合、容量ポートレットは表示されません。容量ポータルは、SVM またはクラスターの disaggregated プロパティが「true」に設定されている場合にのみ必要です。
- ASA r2 SVM システムの場合、基本情報セクションにプラットフォーム タイプが表示されます。

インターフェース タブには、インターフェースに関する詳細情報が表示されます。

ローカル ティア タブには、集計リストに関する詳細情報が表示されます。

vCenter Serverインスタンスを管理する

vCenter Server インスタンスは、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集中管理プラットフォームです。

ストレージ バックエンドと **vCenter Server** インスタンスの関連付けを解除します。

vCenter Server リスト ページには、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 Server インスタンスには、ストレージ バックエンドとの関連付けまたは関連付け解除を行うオプションがあります。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから必要な vCenter Server インスタンスを選択します。
4. ストレージ バックエンドに関連付ける、または関連付けを解除する vCenter Server に対して縦の省略記号を選択します。
5. *ストレージ バックエンドの関連付けを解除*を選択します。

vCenter Serverインスタンスを変更する

vCenter Server インスタンスを変更するには、以下の手順に従います。

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから該当するvCenter Serverインスタンスを選択します。
4. 変更する vCenter Server の縦の省略記号を選択し、[変更] を選択します。
5. vCenter Server インスタンスの詳細を変更し、[変更] を選択します。

vCenter Serverインスタンスを削除する

vCenter Server を削除する前に、vCenter Server 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. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから該当するvCenter Serverインスタンスを選択します。
4. 削除する vCenter Server の縦の省略記号を選択し、[削除] を選択します。



vCenter Server インスタンスを削除すると、それらはアプリケーションによってメンテナンスされなくなります。

ONTAPツールで vCenter Server インスタンスを削除すると、次のアクションが自動的に実行されます。

- プラグインは登録されていません。
- プラグイン権限とプラグイン ロールは削除されます。

証明書の管理

導入時に、ONTAPツールおよび VASA プロバイダー用の自己署名証明書がデフォルトで生成されます。ONTAPツール マネージャ インターフェイスを使用して、証明書を更新したり、カスタム CA にアップグレードしたりできます。マルチ vCenter 展開ではカスタム CA 証明書が必須です。

開始する前に

- 証明書が発行されるドメイン名は、仮想 IP アドレスにマッピングする必要があります。
- ドメイン名に対して nslookup チェックを実行し、ドメインが意図した IP アドレスに解決されているかどうかを確認します。
- 証明書は、ドメイン名とONTAPツールの IP アドレスを使用して作成する必要があります。



ONTAPツールの IP アドレスは、完全修飾ドメイン名 (FQDN) にマッピングする必要があります。証明書には、サブジェクト名またはサブジェクト代替名に、ONTAPツールの IP アドレスにマッピングされた同じ FQDN が含まれている必要があります。



CA 署名証明書から自己署名証明書に切り替えることはできません。

ONTAPツール証明書のアップグレード

ONTAPツール タブには、証明書の種類 (自己署名/CA 署名) やドメイン名などの詳細が表示されます。展開中に、自己署名証明書がデフォルトで生成されます。証明書を更新したり、CA に証明書をアップグレードしたりできます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. 証明書を更新するには、[証明書] > [ONTAPツール] > [更新] を選択します。

証明書の有効期限が切れている場合、または有効期限が近づいている場合は、証明書を更新できません。更新オプションは、証明書の種類が CA 署名の場合に使用できます。ポップアップ ウィンドウで、サーバー証明書、秘密キー、ルート CA、中間証明書の詳細を入力します。



証明書が更新されるまでシステムはオフラインになり、ONTAP Tools Manager インターフェイスからログアウトされます。

4. 自己署名証明書をカスタム CA 証明書にアップグレードするには、[証明書] > [* ONTAPツール] > [CA にアップグレード] オプションを選択します。
 - a. ポップアップ ウィンドウで、サーバー証明書、サーバー証明書の秘密キー、ルート CA 証明書、および中間証明書ファイルをアップロードします。
 - b. この証明書を生成したドメイン名を入力し、証明書をアップグレードします。



アップグレードが完了するまでシステムはオフラインになり、ONTAP Tools Manager インターフェイスからログアウトされます。

VASAプロバイダー証明書のアップグレード

ONTAP tools for VMware vSphereは、VASA プロバイダーの自己署名証明書を使用して導入されます。これにより、vVolsデータストアに対して 1 つの vCenter Server インスタンスのみを管理できるようになります。複数の vCenter Server インスタンスを管理し、それらでvVols機能を有効にする場合は、自己署名証明書をカスタム CA 証明書に変更する必要があります。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. 証明書を更新するには、[証明書] > [VASA プロバイダー] または [ONTAPツール] > [更新] を選択します。
4. 自己署名証明書をカスタム CA 証明書にアップグレードするには、[証明書] > [VASA プロバイダー] または [ONTAPツール] > [CA にアップグレード] を選択します。
 - a. ポップアップ ウィンドウで、サーバー証明書、サーバー証明書の秘密キー、ルート CA 証明書、および中間証明書ファイルをアップロードします。
 - b. この証明書を生成したドメイン名を入力し、証明書をアップグレードします。



アップグレードが完了するまでシステムはオフラインになり、ONTAP Tools Manager インターフェイスからログアウトされます。

ONTAP tools for VMware vSphereにアクセスする

ONTAP tools for VMware vSphereの概要

ONTAP Tools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 パスワードを変更できるほか、サポート バンドルの生成、別のログ 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実行できます。

メンテナンス コンソールにアクセスするには、ONTAP tools for VMware vSphereを導入した後、VMware ツールをインストールする必要があります。使用すべき `maint` 導入時に設定したユーザー名とパスワードを使用して、ONTAPツールのメンテナンス コンソールにログインします。メンテナンスまたはルート 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。



パスワードを設定する必要があります `diag` リモート診断を有効にしながらユーザーを保護します。

メンテナンス コンソールにアクセスするには、ONTAP tools for VMware vSphereの 概要 タブを使用する必要があります。選択すると 、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
アプリケーション構成	1. サーバーステータスの概要を表示する 2. VASA プロバイダサービスと SRA サービスのログレベルを変更する
システム構成	1. Reboot virtual machine 2. Shutdown virtual machine 3. 「maint」ユーザーのパスワードを変更する 4. タイムゾーンを変更する 5. jailディスクサイズを増やす (/jail) 6. Upgrade 7. VMwareツールをインストールする

ネットワーク構成	1. IPアドレス設定を表示する 2. ドメイン名の検索設定を表示する 3. ドメイン名検索設定を変更する 4. 静的ルートを表示する 5. 静的ルートを変更する 6. Commit changes 7. Ping a host 8. デフォルト設定を復元する
Support and Diagnostics	1. 診断シェルにアクセスする 2. リモート診断アクセスを有効にする 3. バックアップ用のvCenter資格情報を提供する 4. バックアップを取る

リモート診断アクセスの設定

ONTAP tools for VMware vSphereを構成して、diag ユーザーの SSH アクセスを有効にすることができます。

開始する前に

VASA プロバイダ拡張機能は、vCenter Server インスタンスに対して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を使用した場合、同時に複数のdiagユーザ アカウントでログインできません。
- 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. メンテナンス ユーザとしてログインします。
3. 入力 `4` サポートと診断を選択します。
4. 入力 `2` リモート診断アクセスを有効にするを選択します。
5. 入力 `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を起動する

アップグレードする前に、他のノードで SSH を開始する必要があります。

開始する前に

VASA プロバイダ拡張機能は、vCenter Server インスタンスに対して有効にする必要があります。

このタスクについて

アップグレードする前に、各ノードでこの手順を実行します。

手順

1. vCenter Serverで、VASA Providerへのコンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. 入力 `4` サポートと診断を選択します。
4. 入力 `1` アクセス診断シェルを選択します。
5. 入力 `y` 続行します。
6. コマンド `sudo systemctl restart ssh` を実行します。

vCenter ServerとONTAPの認証情報を更新する

メンテナンス コンソールを使用して、vCenter Server インスタンスとONTAP認証情報を更新できます。

開始する前に

メンテナンス ユーザーのログイン資格情報が必要です。

このタスクについて

導入後に vCenter Server、ONTAP、または Data LIF の資格情報を変更した場合は、この手順を使用して資格情報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. メンテナンス ユーザとしてログインします。
3. 入力 `2` システム構成メニューを選択します。
4. 入力 `9` ONTAP認証情報を変更します。
5. 入力 `10` vCenter の資格情報を変更します。

ONTAPツールレポート

ONTAP tools for VMware vSphereは、仮想マシンとデータストアのレポートを提供しま

す。vCenter クライアントのショートカット セクションでONTAP tools for VMware vSphereのNetApp ONTAP ツール アイコンを選択すると、ユーザー インターフェイスは概要ページに移動します。仮想マシンとデータストアのレポートを表示するには、[レポート] タブを選択します。

仮想マシン レポートには、検出された仮想マシン (ONTAPストレージ ベースのデータストアからのディスクが少なくとも 1 つ必要) のリストとパフォーマンス メトリックが表示されます。VM レコードを展開すると、ディスク関連のデータストア情報がすべて表示されます。

データストア レポートには、パフォーマンス メトリックを含むすべてのタイプのONTAPストレージ バックエンドからプロビジョニングされたONTAP tools for VMware vSphereのリストが表示されます。

「列の管理」オプションを使用して、さまざまな列を非表示または表示できます。

ログ ファイルの収集

ONTAPツール マネージャ ユーザー インターフェイスで使用可能なオプションから、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。



ONTAPツール マネージャからログを生成すると、すべての vCenter Server インスタンスのすべてのログが含まれます。vCenter クライアント ユーザー インターフェイスから生成されるログの範囲は、選択した vCenter Server に限定されます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから*ログバンドル*を選択します。

この処理には数分かかることがあります。

4. ログ ファイルを生成するには、[生成] を選択します。
5. ログ バンドルのラベルを入力し、[生成] 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。

vCenter クライアント ユーザー インターフェイスを使用してログ バンドルを生成するには、次の手順に従います。

手順

1. vSphere クライアントにログインします。
2. vSphere Client のホームページから、サポート > ログ バンドル > 生成 に移動します。
3. ログバンドルのラベルを指定して、ログバンドルを生成します。ファイルが生成されると、ダウンロード オプションが表示されます。ダウンロードには時間がかかる場合があります。



生成されたログ バンドルは、過去 3 日間または 72 時間以内に生成されたログ バンドルに置き換えられます。

仮想マシンの管理

仮想マシンの移行またはクローン作成に関する考慮事項

データセンター内の既存の仮想マシンを移行する際には、いくつかの考慮事項に注意する必要があります。

保護されている仮想マシンの移行

保護されている仮想マシンは次の場所に移行できます。

- 別のESXiホストにある同じvVolデータストア
- 同じESXiホストにある、互換性のある別のvVolデータストア
- 別のESXiホストにある、互換性のある別のvVolデータストア

仮想マシンが別のFlexVol volumeに移行されると、それぞれのメタデータ ファイルも仮想マシン情報で更新されます。仮想マシンが同じストレージ内の別の ESXi ホストに移行された場合、基盤となるFlexVol volumeメタデータ ファイルは変更されません。

保護されている仮想マシンのクローニング

保護されている仮想マシンは、次の場所にクローニングできます。

- レプリケーション グループを使用する同じFlexVolの同じコンテナ

同じFlexVolのメタデータ ファイルが、クローニングされた仮想マシンの詳細で更新されます。

- レプリケーション グループを使用している別のFlexVolの同じコンテナ

クローニングされた仮想マシンが配置されているFlexVolのメタデータ ファイルが、クローニングされた仮想マシンの詳細で更新されます。

- 別のコンテナまたはvVolデータストア

クローニングされた仮想マシンが配置されているFlexVolのメタデータ ファイルが仮想マシンの詳細で更新されます。

VMware は現在、VM テンプレートにクローンされた仮想マシンをサポートしていません。

保護されている仮想マシンのクローンのクローニングはサポートされています。

参照 ["クローン用の仮想マシンの作成"](#) 詳細についてはこちらをご覧ください。

仮想マシンのSnapshot

現時点では、メモリなしの仮想マシンSnapshotのみがサポートされています。仮想マシンにメモリありのSnapshotが存在する場合、仮想マシンは保護対象とはみなされません。

また、メモリ スナップショットを持つ保護されていない仮想マシンを保護することもできません。このリリースでは、仮想マシンの保護を有効にする前に、メモリありのSnapshotを削除する必要があります。

ASA r2 ストレージ タイプを備えた Windows VM の場合、仮想マシンのスナップショットを作成すると、読み取り専用のスナップショットになります。VM の電源オン要求があると、VASA プロバイダーは読み取り専用スナップショットを使用して LUN を作成し、IOPS を有効にします。電源オフ要求時に、VASA プロバイダーは作成された LUN を削除し、IOPS を無効にします。

NFS および VMFS データストアを持つ仮想マシンをvVolsデータストアに移行する

NFS および VMFS データストアから仮想ボリューム (vVols) データストアに仮想マシンを移行して、ポリシーベースの VM 管理やその他のvVols機能を活用できます。vVols データvVolsを使用すると、増大するワークロード要件を満たすことができます。

開始する前に

移行を計画している仮想マシンのいずれでも VASA プロバイダーが実行されていないことを確認します。VASA Providerを実行している仮想マシンをvVolデータストアに移行すると、いっさいの管理操作を実行できなくなり、仮想マシンの電源をオンにすることもできなくなります。

このタスクについて

NFS および VMFS データストアからvVolsデータストアに移行する場合、vCenter Server は、NFS VMDK ファイルからではなく、VMFS データストアからデータを移動するときに vStorage APIs for Array Integration (VAAI) オフロードを使用します。VAAIのオフロードは、通常、ホスト サーバの負荷を軽減します。

手順

1. 移行する仮想マシンを右クリックし、[移行] を選択します。
2. *ストレージのみ変更*を選択し、*次へ*を選択します。
3. 移行するデータストアの機能に一致する仮想ディスク形式、VM ストレージ ポリシー、および vVol データストアを選択します。
4. 設定を確認し、[完了] を選択します。

VASAのクリーンアップ

VASAのクリーンアップを実行するには、このセクションの手順を使用します。



VASA クリーンアップを実行する前に、vVolsデータストアを削除することをお勧めします。

手順

1. プラグインの登録を解除するには、https://OTV_IP:8143/Register.htmlにアクセスしてください。
2. プラグインが vCenter Server で使用できなくなっていることを確認します。
3. ONTAP tools for VMware vSphereをシャットダウンします。

4. ONTAP tools for VMware vSphereを削除します。

仮想マシンからデータディスクを接続または切断する

仮想マシンにデータディスクを接続する

ストレージ容量を拡張するには、データ ディスクを仮想マシンに接続します。

手順

1. vSphere クライアントにログインします。
2. インベントリ内の仮想マシンを右クリックし、[設定の編集] を選択します。
3. *仮想ハードウェア*タブで、*既存のハードディスク*を選択します。
4. ディスクが存在する仮想マシンを選択します。
5. 接続するディスクを選択し、「OK」を選択します。

結果

ハードディスクが仮想ハードウェア デバイス リストに表示されます。

仮想マシンからデータディスクを切断する

仮想マシンに接続されているデータ ディスクは、不要になったときに切断できます。ディスクを仮想マシンからデタッチしても、ディスクは自動的に削除されず、ONTAPストレージ システムに残ります。

手順

1. vSphere クライアントにログインします。
2. インベントリ内の仮想マシンを右クリックし、[設定の編集] を選択します。
3. ポインタをディスクの上に移動し、「削除」を選択します。



ディスクは仮想マシンから削除されます。他の仮想マシンがディスクを共有している場合、ディスクファイルは削除されません。

関連情報

["仮想マシンに新しいハードディスクを追加する"](#)

["既存のハードディスクを仮想マシンに追加する"](#)

ストレージ システムとホストの検出

vSphere Client でONTAP tools for VMware vSphereを初めて実行すると、ONTAPツールはESXi ホスト、その LUN と NFS エクスポート、およびそれらの LUN とエクスポートを所有するNetAppストレージ システムを検出します。

開始する前に

- すべての ESXi ホストの電源がオンになって接続されている必要があります。

- 検出対象となるすべてのストレージ仮想マシン (SVM) が実行中であり、各クラスター ノードには使用中のストレージ プロトコル (NFS または iSCSI) 用に構成されたデータ LIF が少なくとも 1 つ必要です。

このタスクについて

新しいストレージ システムの検出や既存のストレージ システムの情報の更新はいつでも実行でき、容量や設定に関する最新の情報を確認することができます。また、ONTAP tools for VMware vSphereがストレージ システムにログインするために使用する資格情報を変更することもできます。

ストレージ システムを検出しながら、ONTAP tools for VMware vSphereは、vCenter Server インスタンスによって管理されている ESXi ホストから情報を収集します。

手順

1. vSphere Client のホームページから、[ホストとクラスター] を選択します。
2. 必要なデータセンターを右クリックし、* NetApp ONTAPツール* > ホスト データの更新 を選択します。

確認 ダイアログボックスで選択内容を確認します。

3. 検出されたストレージコントローラのうち、ステータスが Authentication Failureアクション > *変更*を選択します。
4. ストレージ システムの変更 ダイアログ ボックスに必要な情報を入力します。
5. すべてのストレージコントローラに対して手順4と5を繰り返します。`Authentication Failure`状態。

検出プロセスが完了したら、次のアクションを実行します。

- ONTAP tools for VMware vSphereを使用して、アダプタ設定列、MPIO 設定列、または NFS 設定列にアラート アイコンが表示されるホストの ESXi ホスト設定を構成します。
- ストレージ システムのクレデンシャルを入力します。

ONTAP Toolsを使用したESXiホストの設定の変更

ONTAP Tools for VMware vSphereのダッシュボードを使用して、ESXiホストの設定を編集できます。

開始する前に

ESXi ホスト設定に問題がある場合は、ダッシュボードの ESXi ホスト システム ポートレットに問題が表示されます。問題を選択すると、問題が発生している ESXi ホストのホスト名または IP アドレスを表示できます。

手順

1. vSphere クライアントにログインします。
2. ショートカット ページで、プラグイン セクションの * NetApp ONTAPツール* を選択します。
3. ONTAP tools for VMware vSphereプラグインの概要 (ダッシュボード) にある **ESXi** ホスト コンプライアンス ポートレットに移動します。
4. *推奨設定を適用*リンクを選択します。
5. 推奨ホスト設定の適用 ウィンドウで、NetApp推奨ホスト設定に準拠するホストを選択し、次へ を選択します。



ESXi ホストを展開して現在の値を確認できます。

6. 設定ページで、必要に応じて推奨値を選択します。
7. 概要ペインで値を確認し、[完了] を選択します。最近のタスク パネルで進行状況を追跡できます。

関連情報

["ESXiホスト設定を構成する"](#)

パスワードを管理する

ONTAP ツールマネージャのパスワードを変更する

ONTAP Tools Manager を使用して管理者パスワードを変更できます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. 画面の右上隅にある*管理者*アイコンを選択し、*パスワードの変更*を選択します。
4. パスワード変更ポップアップ ウィンドウで、古いパスワードと新しいパスワードの詳細を入力します。パスワード変更の制約はユーザーインターフェース画面に表示されます。
5. 変更を実装するには、[変更] を選択します。

ONTAP ツールマネージャのパスワードをリセットする

ONTAP ツール マネージャのパスワードを忘れた場合は、ONTAP tools for VMware vSphereによって生成されたトークンを使用して管理者の資格情報をリセットできます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. ログイン画面で、「パスワードのリセット」オプションを選択します。

Manager のパスワードをリセットするには、ONTAP tools for VMware vSphereを使用してリセット トークンを生成する必要があります。

- a. vCenter Serverからメンテナンスコンソールを開きます
 - b. システム構成オプションを選択するには「2」を入力してください
 - c. 「maint」 ユーザーパスワードを変更するには、「3」を入力します。
3. パスワード変更ポップアップ ウィンドウで、パスワード リセット トークン、ユーザー名、新しいパスワードの詳細を入力します。
 4. 変更を反映するには、[リセット] を選択します。パスワードのリセットが成功すると、新しいパスワード

を使用してログインできます。

アプリケーションユーザーのパスワードをリセットする

アプリケーション ユーザー パスワードは、vCenter Server への SRA および VASA プロバイダの登録に使用されます。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから*設定*を選択します。
4. **VASA/SRA** 資格情報 画面で、パスワードのリセット を選択します。
5. 新しいパスワードを入力し、新しいパスワードの入力を確認します。
6. 変更を反映するには、[リセット] を選択します。

メンテナンスコンソールのユーザーパスワードをリセットする

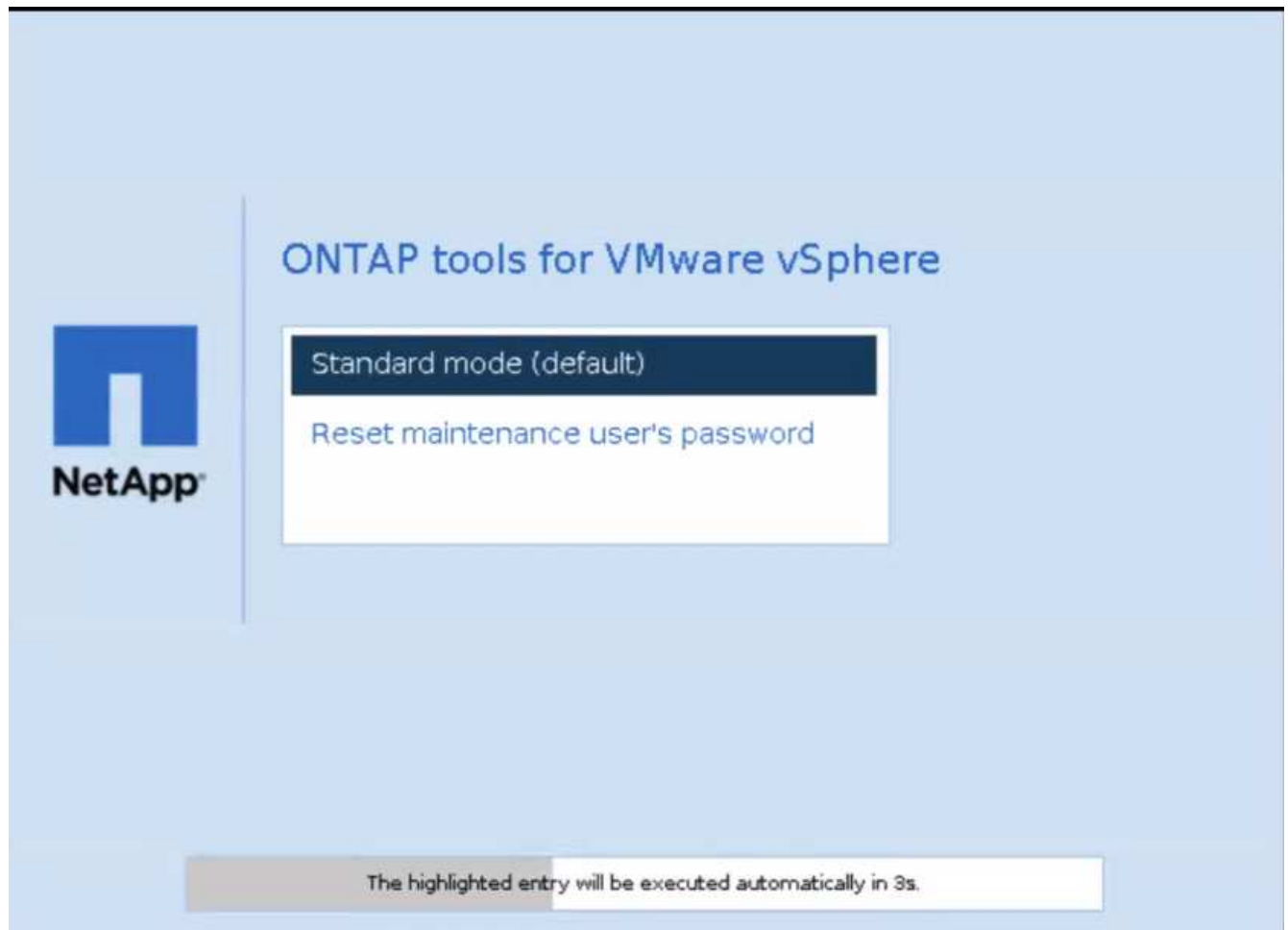
ゲストOSの再起動中に、GRUBメニューにメンテナンスコンソールのユーザーパスワードをリセットするオプションが表示されます。このオプションは、対応するVMのメンテナンスコンソールのユーザーパスワードを更新するために使用します。パスワードのリセットが完了すると、VMが再起動され、新しいパスワードが設定されます。HA展開シナリオでは、VMの再起動後、他の2つのVMのパスワードも自動的に更新されます。



ONTAP tools for VMware vSphereの場合、最初のノード (node1) のメンテナンス コンソール ユーザー パスワードを変更する必要があります。

手順

1. vCenter Serverにログインします
2. VM を右クリックし、[電源] > [ゲスト OS の再起動] を選択します。システムの再起動中に、次の画面が表示されます。



オプションを選択するのに 5 秒かかります。任意のキーを押すと進行が停止し、GRUB メニューがフリーズします。

3. メンテナンス ユーザーのパスワードをリセット オプションを選択します。メンテナンス コンソールが開きます。
4. コンソールで新しいパスワードの詳細を入力します。パスワードを正常にリセットするには、新しいパスワードと再入力した新しいパスワードの詳細が一致している必要があります。正しいパスワードを入力するチャンスは 3 回あります。新しいパスワードを正常に入力すると、システムが再起動します。
5. 続行するには Enter キーを押してください。VM 上でパスワードが更新されます。



VM の電源投入時にも同じ GRUB メニューが表示されます。ただし、パスワードのリセット オプションは、ゲスト OS の再起動 オプションとのみ併用する必要があります。

ホストクラスタ保護の管理

保護されたホスト クラスタを変更する

変更保護の一部として次のタスクを実行できます。すべての変更を同じワークフローで実行できます。

- 保護されたクラスタに新しいデータストアまたはホストを追加します。

- 保護設定に新しいSnapMirror関係を追加します。
- 保護設定から既存のSnapMirror関係を削除します。
- 既存のSnapMirror関係を変更します。

ホストクラスタ保護の監視

ホスト クラスタ保護の状態を監視するには、この手順を使用します。保護されているすべてのホスト クラスタを、その保護状態、 SnapMirror関係、データストア、および対応するSnapMirrorステータスとともに監視できます。

手順

1. vSphere クライアントにログインします。
2. * NetApp ONTAPツール* > 保護 > ホスト クラスタ リレーションシップ に移動します。

保護列の下アイコンは保護の状態を示します

3. アイコンの上にマウスを移動すると詳細が表示されます。

新しいデータストアまたはホストを追加する

新しく追加されたデータストアまたはホストを保護するには、この手順を使用します。 vCenter ネイティブ ユーザー インターフェイスを使用して、保護されたクラスタに新しいホストを追加したり、ホスト クラスタ上に新しいデータストアを作成したりできます。

手順

1. vSphere クライアントにログインします。
2. 保護されたクラスタのプロパティを編集するには、次のいずれかを実行します。
 - a. * NetApp ONTAPツール* > 保護 > *ホストクラスタ関係*に移動し、クラスタの省略記号メニューを選択して*編集*を選択するか、
 - b. ホスト クラスタを右クリックし、* NetApp ONTAPツール* > クラスタの保護 を選択します。
3. vCenter ネイティブ ユーザー インターフェイスでデータストアを作成した場合、そのデータストアは保護されていないものとして表示されます。ユーザー インターフェイスでは、クラスタ内のすべてのデータストアとその保護ステータスがダイアログ ボックスに表示されます。完全な保護を有効にするには、[保護] ボタンを選択します。
4. 新しい ESXi ホストを追加した場合、保護ステータスは部分的に保護されていると表示されます。SnapMirror設定の下の省略記号メニューを選択し、[編集] を選択して、新しく追加された ESXi ホストの近接性を設定します。



非同期タイプの関係の場合、第3サイトのターゲットSVMを同じONTAPツールインスタンスに追加できないため、編集操作はサポートされません。ただし、ターゲットSVMのシステムマネージャまたはCLIを使用して、関係の設定を変更することは可能です。

5. 必要な変更を行った後、[保存] を選択します。
6. **Protect Cluster** ウィンドウで変更を確認できます。

vCenter タスクが作成され、最近のタスク パネルで進行状況を追跡できます。

新しいSnapMirror関係を追加する

手順

1. vSphere クライアントにログインします。
2. 保護されたクラスタのプロパティを編集するには、次のいずれかを実行します。
 - a. * NetApp ONTAPツール* > 保護 > *ホストクラスタ関係*に移動し、クラスタの省略記号メニューを選択して*編集*を選択するか、
 - b. ホスト クラスタを右クリックし、* NetApp ONTAPツール* > クラスタの保護 を選択します。
3. *関係を追加*を選択します。
4. 新しい関係を **Asynchronous** または **AutomatedFailOverDuplex** ポリシー タイプとして追加します。
5. *保護*を選択します。

Protect Cluster ウィンドウで変更を確認できます。

vCenter タスクが作成され、最近のタスク パネルで進行状況を追跡できます。

既存のSnapMirror関係を削除する

非同期SnapMirror関係を削除するには、セカンダリ サイトの SVM またはクラスタを ONTAP tools for VMware vSphereのストレージ バックエンドとして追加する必要があります。すべてのSnapMirror関係を削除することはできません。関係を削除すると、ONTAPクラスタ上のそれぞれの関係も削除されます。AutomatedFailOverDuplex SnapMirror関係を削除すると、宛先のデータストアがマップ解除され、整合性グループ、LUN、ボリューム、および igroup が宛先ONTAPクラスタから削除されます。

関係を削除すると、セカンダリ サイトで再スキャンがトリガーされ、マップされていない LUN がホストからアクティブ パスとして削除されます。

手順

1. vSphere クライアントにログインします。
2. 保護されたクラスタのプロパティを編集するには、次のいずれかを実行します。
 - a. * NetApp ONTAPツール* > 保護 > *ホストクラスタ関係*に移動し、クラスタの省略記号メニューを選択して*編集*を選択するか、
 - b. ホスト クラスタを右クリックし、* NetApp ONTAPツール* > クラスタの保護 を選択します。
3. SnapMirror設定の下の省略記号メニューを選択し、[削除] を選択します。

vCenter タスクが作成され、最近のタスク パネルで進行状況を追跡できます。

既存のSnapMirror関係を変更する

非同期SnapMirror関係を変更するには、セカンダリ サイトの SVM またはクラスタを ONTAP tools for VMware vSphereのストレージ バックエンドとして追加する必要があります。AutomatedFailOverDuplex SnapMirror関係の場合、均一構成の場合はホストの近接性を、非均一構成の場合はホスト アクセスを変更できます。Asynchronous と AutomatedFailOverDuplex のポリシー タイプを交換することはできません。クラスタ上で新しく検出されたホストの近接性またはアクセスを設定できます。



既存の非同期SnapMirror関係を編集することはできません。

手順

1. vSphere クライアントにログインします。
2. 保護されたクラスタのプロパティを編集するには、次のいずれかを実行します。
 - a. * NetApp ONTAPツール* > 保護 > *ホストクラスタ関係*に移動し、クラスタの省略記号メニューを選択して*編集*を選択するか、
 - b. ホスト クラスターを右クリックし、* NetApp ONTAPツール* > クラスターの保護 を選択します。
3. AutomatedFailOverDuplex ポリシー タイプを選択した場合は、ホストの近接性またはホスト アクセスの詳細を追加します。
4. *保護*ボタンを選択します。

vCenter タスクが作成され、最近のタスク パネルで進行状況を追跡できます。

ホストクラスタ保護を削除する

ホスト クラスタの保護を削除すると、データストアは保護されなくなります。

手順

1. 保護されたホスト クラスターを表示するには、* NetApp ONTAPツール* > 保護 > ホスト クラスター リレーションシップ に移動します。

このページでは、保護されたホスト クラスタとその保護状態、 SnapMirror関係、および対応するSnapMirrorステータスを監視できます。

2. ホスト クラスター保護 ウィンドウで、クラスターに対する省略記号メニューを選択し、保護の削除 を選択します。

AutoSupportを無効にする

ストレージ システムを初めて構成する場合、AutoSupport はデフォルトで有効になります。有効になってから 24 時間以内にテクニカル サポートにメッセージが送信されます。AutoSupport を無効にすると、プロアクティブなサポートと監視は受けられなくなります。



AutoSupportを有効にしておくことをお勧めします。問題の検出と解決を迅速化するのに役立ちます。システムは、無効になっている場合でも、AutoSupport情報を収集し、ローカルに保存します。ただし、レポートはどのネットワークにも送信されません。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. 設定 > テレメトリ > 編集 オプションを選択します。
4. * AutoSupport* オプションの選択を解除し、変更を保存します。

AutoSupportプロキシ URL を更新する

ネットワーク アクセス制御やセキュリティ対策にプロキシ サーバーが使用されるシナリオでAutoSupport機能が適切に機能するように、 AutoSupportプロキシ URL を更新します。これにより、 AutoSupportデータを適切なプロキシ経由でルーティングできるようになり、安全な転送とコンプライアンスが実現します。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. サイドバーから*設定*を選択します。
4. 設定 > テレメトリ > 編集 オプションを選択します。
5. 有効な*プロキシ URL* を入力し、変更を保存します。

AutoSupportを無効にすると、プロキシ URL も無効になります。

NTPサーバーを追加する

ONTAPツール アプライアンスのタイム クロックを同期するには、NTP サーバーの詳細を入力します。

手順

1. Web ブラウザからONTAPツール マネージャを起動します。
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者認証情報を使用してログインします。
3. 設定 > **NTP** サーバー > 編集 オプションを選択します。
4. カンマ区切りの完全修飾ドメイン名 (FQDN)、IPv4、または IPv6 アドレスを入力します。

更新された値を確認するには画面を更新してください。

ONTAPツールのセットアップのバックアップを作成し、復元する

ONTAP tools for VMware vSphere以降、アプライアンスは動的ストレージ プロビジョナーを使用するため、ゼロ RPO を実現することはできません。ただし、RPO をほぼゼロにすることは可能です。ほぼゼロの RPO を実現するには、セットアップのバックアップを作成し、新しい仮想マシンに復元する必要があります。



非 HA バックアップが有効になっているときに HA に移行するには、まずバックアップを無効にし、移行後に再度有効にします。

バックアップを作成し、バックアップファイルをダウンロードする

手順

1. vCenter Server からメンテナンス コンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. 入力 4*サポートと診断*を選択します。
4. 入力 3*システムバックアップを有効にする*オプションを選択します。
5. HA 以外の場合は、ONTAPツール仮想マシンがデプロイされている vCenter の認証情報を入力します。
6. バックアップ頻度の値を 5 ～ 60 分の範囲で入力します。
7. Enterキーを押します

これにより、バックアップが作成され、定期的に仮想マシンのデータストアにバックアップがプッシュされます。

8. バックアップにアクセスするには、ストレージセクションに移動し、仮想マシンのデータストアを選択します。
9. *ファイル*セクションを選択します。

ファイルセクションではディレクトリを確認できます。ディレクトリの名前は、ドット (.) がアンダースコアに置き換えられ、末尾に *backup* が付けられたONTAPツールの IP アドレスになります。

10. バックアップの詳細については、[ファイル] > [ダウンロード] から *backup_info.txt* ファイルをダウンロードしてください。

リカバリ

セットアップを回復するには、既存の仮想マシンの電源をオフにし、最初の展開で使用された OVA を使用して新しい仮想マシンを展開します。

新しい仮想マシンには同じONTAPツール IP アドレスを使用する必要があり、有効なサービス、ノード サイズ、HA モードなどのシステム構成は初期展開と同じである必要があります。

バックアップ ファイルからセットアップを回復するには、次の手順を実行します。

1. vCenter Server からメンテナンス コンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. 入力 4*サポートと診断*を選択します。
4. 入力 2*リモート診断アクセスを有効にする*オプションを選択し、診断アクセス用の新しいパスワードを作成します。
5. ダウンロードしたディレクトリから任意のバックアップを 1 つ選択します。最新のバックアップ ファイル名は *backup_info.txt* ファイルに記録されます。
6. 以下のコマンドを実行してバックアップを新しい仮想マシンにコピーし、プロンプトが表示されたら診断パスワードを入力します。

```
scp <Backup_X.tar.enc> diag@<node_ip>:/home/diag/system_recovery.tar.enc
```



コマンドに記載されている宛先パスとファイル名 (/home/diag/system_recovery.tar.enc) を変更しないでください。

7. バックアップ ファイルがコピーされたら、診断シェルにログインして次のコマンドを実行します。

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

ログは /var/log/post-deploy-upgrade.log ファイルに記録されます。

8. リカバリが成功すると、サービスと vCenter オブジェクトが復元されます。

ONTAP tools for VMware vSphereをアンインストールする

ONTAP tools for VMware vSphereをアンインストールすると、ツール内のすべてのデータが削除されます。

手順

1. ONTAP tools for VMware vSphereからすべての仮想マシンを削除または移動します。
 - 仮想マシンを削除するには、"[VM と VM テンプレートの削除と再登録](#)"
 - 管理されていないデータストアに移動するには、"[Storage vMotion を使用して仮想マシンを移行する方法](#)"
2. "[データストアを削除する](#)"ONTAP tools for VMware vSphereで作成されました。
3. VASA プロバイダーを有効にしている場合は、ONTAPツールで **設定 > VASA プロバイダー設定 > 登録解除** を選択して、すべての vCenter サーバーから VASA プロバイダーを登録解除します。
4. すべてのストレージ バックエンドを vCenter Server インスタンスから関連付け解除します。。"[ストレージ バックエンドと vCenter Server インスタンスの関連付けを解除します。](#)"
5. すべてのストレージ バックエンドを削除します。。"[ストレージバックエンドの管理](#)"。
6. VMware Live Site Recovery から SRA アダプタを削除します。
 - a. ポート 5480 を使用して、VMware Live Site Recovery アプライアンス管理インターフェイスに管理者としてログインします。
 - b. *ストレージ レプリケーション アダプタ*を選択します。
 - c. 適切な SRA カードを選択し、ドロップダウン メニューから [削除] を選択します。
 - d. アダプタの削除結果を確認し、[削除] を選択します。
7. ONTAP tools for VMware vSphereにオンボードされた vCenter Server インスタンスを削除します。。"[vCenter Serverインスタンスを管理する](#)"。
8. vCenter Server からONTAP tools for VMware vSphereの電源をオフにし、VM を削除します。

次は何？

FlexVolボリュームを削除する

VMware 導入用のONTAPツール専用のONTAPクラスターを使用すると、未使用のFlexVolボリュームが多数作成されます。ONTAP tools for VMware vSphereを削除した後は、パフォーマンスへの影響を回避するためにFlexVolボリュームを削除する必要があります。

手順

1. 最初のノード VM からONTAP tools for VMware vSphereを決定します。

```
cat /opt/netapp/meta/ansible_vars.yaml | grep -i プロトコル
```

iSCSI 展開の場合は、igroup も削除する必要があります。

2. FlexVolボリュームのリストを取得します。

```
kubectl で永続ボリュームを記述 | grep で内部名を記述 | awk -F=' ' '{print $2}'
```

3. vCenter Server から仮想マシンを削除します。参照 ["VM と VM テンプレートの削除と再登録"](#)。
4. FlexVolボリュームを削除します。参照 ["FlexVolの削除"](#)。ボリュームを削除する CLI コマンドでは、FlexVolボリュームの正確な名前を指定します。
5. iSCSI 展開の場合は、ONTAPストレージシステムから SAN igroup を削除します。参照 ["SANのイニシエータとigroupの表示と管理"](#)。

ONTAP tools for VMware vSphereのアップグレード

ONTAP tools for VMware vSphereから 10.4 へのアップグレード

ONTAP tools for VMware vSphereから 10.4 にアップグレードできます。ただし、ONTAPツール 10.0 または 10.1 から 10.4 への直接アップグレードはサポートされていません。

注：

- ASA r2 システムでは、ストレージ可用性ゾーン (SAZ) を追加する前に、ONTAP 9.16.1 を搭載したONTAP tools for VMware vSphereにアップグレードする必要があります。
- ONTAP tools for VMware vSphereから 10.4 リリースへのアップグレードが失敗した場合、ロールバックはサポートされません。セットアップをリカバリするには、ONTAP tools for VMware vSphereの RPO と、ONTAP tools for VMware vSphereのほぼゼロ RPO またはスナップショット リカバリを使用します。

開始する前に

非 HA アップグレードの場合はONTAPツール VM の電源をオフにし、HA アップグレードの場合は最初のノードの電源をオフにしてから、仮想マシン (VM) 設定に次の変更を加えます。

ONTAP tools for VMware vSphereからアップグレードする場合は、アップグレードタスクを進める前に次の手順を完了する必要があります。* サービスデータは仮想マシンにローカルに保存されるため、各ノードに 100 GB のハードディスクを追加します。* パワーオフ状態の仮想マシンの CPU とメモリを、デプロイメントの種類に応じて変更します。CPUと RAM のホットプラグインを有効にします。

+

展開タイプ	ノードあたりのCPU (コア)	ノードあたりのメモリ(GB)	ノードあたりのディスク容量(GB)	合計CPU(コア)	メモリ(GB)	合計ディスク容量(GB)
非HA小	9	18	350	9	18	350
非HA培地	13	26	350	13	26	350
HAスモール	9	18	350	27	54	1050
HAミディアム	13	26	350	39	78	1050
HAラージ	17	34	350	51	102	1050

- 変更が完了したら、VM の電源をオンにし、サービスが実行状態になるまで待ちます。
- HA 展開の場合は、リソースを変更し、CPU と RAM のホット プラグインを有効にし、2 番目と 3 番目のノードにも 100 GB のハード ディスクを追加します。これらのノードを再起動する必要はありません。
- アプライアンスがONTAPツール 10.2 を使用してローカル パス (簡単な導入) として導入された場合は、アップグレードする前に静止スナップショットを取得する必要があります。

ONTAP tools for VMware vSphere 10.0から10.1にアップグレードする場合は、アップグレードタスクを続ける前に次の手順を完了する必要があります: 診断を有効にする

1. vCenter Server から、ONTAPツールへのコンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. **4** と入力して サポートと診断 を選択します。
4. **2** と入力して リモート診断アクセスを有効にする を選択します。
5. 希望するパスワードを設定するには、「**y**」と入力します。
6. ユーザー名を「diag」、パスワードを前の手順で設定した状態で、ターミナル/PuTTY から VM IP アドレスにログインします。

MongoDBのバックアップを取る

MongoDB のバックアップを取得するには、次のコマンドを実行します。

- `kn exec -it ntv-mongodb-0 sh - kn` は `kubectl -n ntv-system` のエイリアスです。
- ポッド内で `env | grep MONGODB_ROOT_PASSWORD` コマンドを実行します。
- ポッドから抜け出すには、`exit` コマンドを実行します。
- `kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip` コマンドを実行して、上記のコマンドで設定した `MONGO_ROOT_PASSWORD` を置き換えます。
- `kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz` コマンドを実行して、上記のコマンドを使用して作成された `mongodb` バックアップをポッドからホストにコピーします。

すべてのボリュームの準スナップショットを撮ります

- 「`kn get pvc`」 コマンドを実行し、コマンド出力を保存します。
- 次のいずれかの方法を使用して、すべてのボリュームのスナップショットを 1 つずつ作成します。
 - CLIから、`command _volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>` を実行します。
 - ONTAP System Manager ユーザー インターフェイスから、検索バーでボリュームを名前で検索し、名前を選択してそのボリュームを開きます。スナップショットに移動し、そのボリュームのスナップショットを追加します。

vCenter 内のONTAP tools for VMware vSphereのスナップショットを取得します (HA 展開の場合は 3 台の VM、非 HA 展開の場合は 1 台の VM)

- vSphere クライアント ユーザー インターフェイスで、VM を選択します。
- スナップショットタブに移動し、*スナップショットを撮る*ボタンを選択します。VM の静止スナップショットを取得します。参照 ["仮想マシンのスナップショットを作成する"](#) 詳細については。

アップグレードを実行する前に、プレフィックスが「`generate-support-bundle-job`」であるログ バンドルから完了したポッドを削除します。サポート バンドルの生成が進行中の場合は、完了するまで待ってからポッドを削除します。

どのようなタイプのアップグレードでも、100 GB のハード ディスク ドライブ (HDD) を追加する必要があります

ます。HDDを追加するには、次のタスクを実行します。

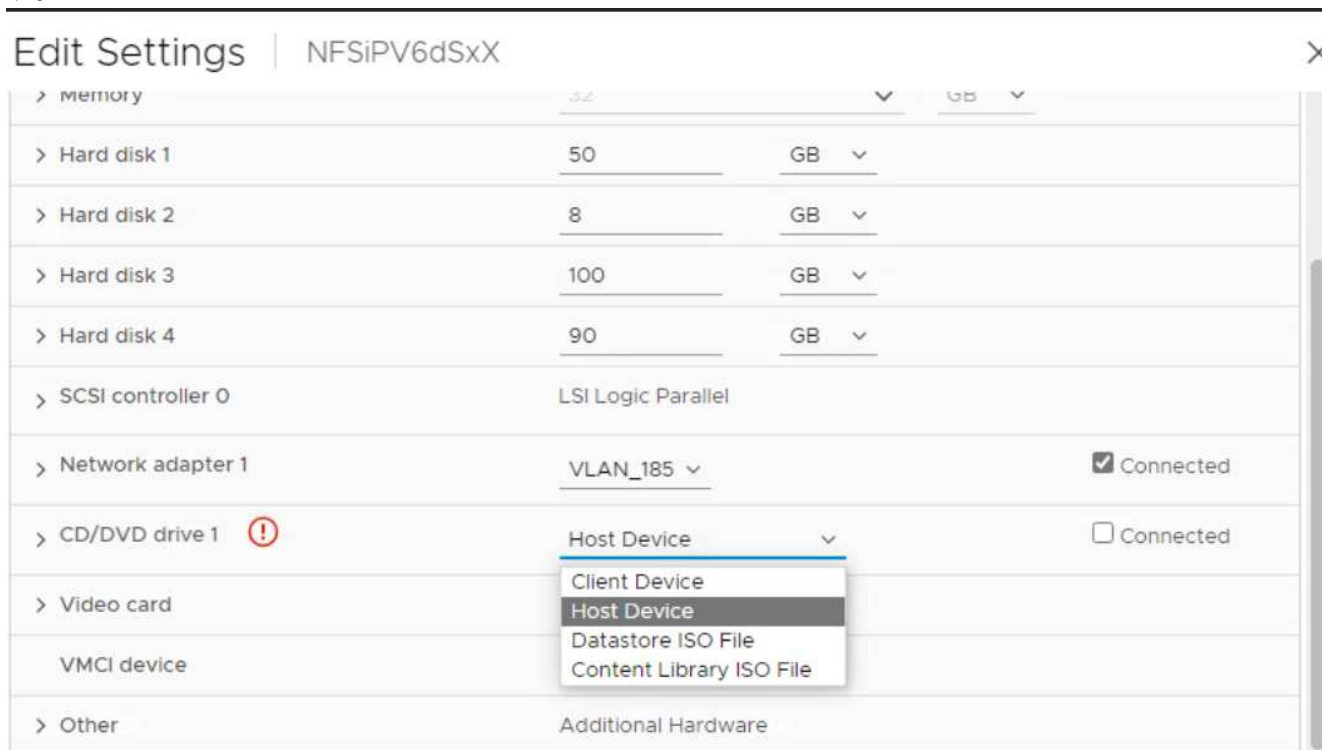
1. 単一ノード構成の VM を選択するか、HA 構成の 3 つの VM すべてを選択します。
2. VMを右クリックし、[新しいデバイスの追加]>[ハードディスク]を選択します。
3. 新しいハードディスク フィールドに 100 GB の HDD を追加します。
4. *適用*を選択

ハードディスクを追加した後、それぞれの構成に合わせて VM のリソースを更新し、プライマリ VM を再起動します。

新しいHDDが作成されます。動的ストレージ プロビジョナーは、この HDD を使用してボリュームを生成または複製します。

手順

1. ONTAP tools for VMware vSphereをコンテンツ ライブラリにアップロードします。
2. プライマリVMページで、アクション>*設定の編集*を選択します。
3. **CD/DVD** ドライブ フィールドの編集設定ウィンドウで、コンテンツ ライブラリの ISO ファイルを選択します。
4. ISO ファイルを選択し、[OK] を選択します。 **CD/DVD** ドライブ フィールドで接続されているチェックボックスを選択します。



5. vCenter Server から、ONTAPツールへのコンソールを開きます。
6. メンテナンス ユーザとしてログインします。
7. 3 と入力して、システム構成メニューを選択します。
8. アップグレード オプションを選択するには、「7」と入力します。

9. アップグレードすると、次のアクションが自動的に実行されます。

- a. 証明書のアップグレード
- b. リモートプラグインアップグレード

ONTAP tools for VMware vSphereにアップグレードすると、次のことが可能になります。

- マネージャーのユーザーインターフェースからサービスを無効にします
- 非HA設定からHA設定に移行する
- 非 HA の小規模構成を非 HA の中規模構成にスケールアップするか、または HA の中規模または大規模構成にスケールアップします。
- HA 以外のアップグレードの場合は、変更を反映するためにONTAPツール VM を再起動します。 HA アップグレードの場合は、最初のノードを再起動して、ノードの変更を反映します。

次の手順

ONTAP tools for VMware vSphereの以前のリリースから 10.4 にアップグレードした後、SRA アダプタを再スキャンして、VMware Live Site Recovery のストレージ レプリケーション アダプタ ページで詳細が更新されていることを確認します。

アップグレードが正常に完了したら、次の手順に従って、ONTAPからTridentボリュームを手動で削除します。



ONTAP tools for VMware vSphereが非 HA の小規模または中規模 (ローカル パス) 構成であった場合、これらの手順は必要ありません。

1. vCenter Server から、ONTAPツールへのコンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. 4 と入力して、サポートと診断 メニューを選択します。
4. 1 と入力して、診断シェルにアクセス オプションを選択します。
5. 次のコマンドを実行します

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. ONTAPのユーザー名とパスワードを入力してください

これにより、ONTAP tools for VMware vSphereで使用されるONTAP内のすべてのTridentボリュームが削除されます。

関連情報

["ONTAP tools for VMware vSphereから 10.4 に移行する"](#)

アップグレードエラーコード

ONTAP tools for VMware vSphereアップグレード操作中にエラー コードが発生する可能性があります。エラー コードは 5 桁で、最初の 2 桁は問題が発生したスクリプトを表

し、最後の 3 桁はそのスクリプト内の特定のワークフローを表します。

すべてのエラー ログは `ansible-perl-errors.log` ファイルに記録され、問題を簡単に追跡して解決できるようになります。このログ ファイルには、エラー コードと失敗した Ansible タスクが含まれています。



このページに記載されているエラー コードは参考用です。エラーが解決しない場合、または解決策が記載されていない場合は、サポート チームにお問い合わせください。

次の表に、エラー コードと対応するファイル名を示します。

エラーコード	スクリプト名
00	firstboot-network-config.pl、モードデプロイ
01	firstboot-network-config.pl、モードのアップグレード
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl、デプロイ、HA
04	firstboot-deploy-otv-ng.pl、デプロイ、非 HA
05	firstboot-deploy-otv-ng.pl、再起動
06	firstboot-deploy-otv-ng.pl、アップグレード、HA
07	firstboot-deploy-otv-ng.pl、アップグレード、非HA
08	firstboot-otv-recovery.pl
09	デプロイ後のアップグレード.pl

エラー コードの最後の 3 桁は、スクリプト内の特定のワークフロー エラーを示します。

アップグレードエラーコード	ワークフロー	解決
052	ISO は現在のバージョンと同じか、または現在のバージョンより 2 つ上のリリースである可能性があります。	現在のバージョンからアップグレードするには、互換性のある ISO バージョンを使用します。
068	Debian パッケージのロールバックに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
069	ファイルの復元に失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
070	バックアップの削除に失敗しました	-
071	Kubernetes クラスターが正常ではありませんでした	-
074	ISOマウントに失敗しました	<code>/var/log/upgrade-run.log</code> を確認し、アップグレードを再試行してください。

アップグレードエラーコード	ワークフロー	解決
075	アップグレードの事前チェックに失敗しました	アップグレードを再試行してください。
076	レジストリのアップグレードに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
077	レジストリのロールバックに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
078	オペレータのアップグレードに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
079	オペレータのロールバックに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
080	サービスのアップグレードに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
081	サービスのロールバックに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
082	コンテナから古いイメージを削除できませんでした	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
083	バックアップの削除に失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
084	JobManager を Production に戻すことができませんでした	アップグレードを回復/完了するには、以下の手順に従ってください。1.診断シェル 2 を有効にします。次のコマンドを実行します: <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade 3.</code> <code>/var/log/post-deploy-upgrade.log</code> のログを確認します。
087	アップグレード後の手順が失敗しました。	アップグレードを回復/完了するには、次の手順を実行します。1.診断シェル 2 を有効にします。 <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</code> コマンド 3 を実行します。 <code>/var/log/post-deploy-upgrade.log</code> のログを確認します。

アップグレードエラーコード	ワークフロー	解決
088	journald のログローテーションの設定に失敗しました	VM がホストされているホストと互換性のある VM ネットワーク設定を確認します。VM を別のホストに移行して再起動してみることができます。
089	サマリーログローテーション設定ファイルの所有権の変更に失敗しました	アップグレードを再試行してください。
095	OSのアップグレードに失敗しました	OSアップグレードの回復はありません。ONTAPツール サービスがアップグレードされ、新しいポッドが実行されます。
096	動的ストレージプロビジョナーをインストールする	アップグレード ログを確認し、アップグレードを再試行してください。
097	アップグレードのためのサービスのアンインストールに失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
098	ntv-system から動的ストレージ プロビジョナー名前空間への dockercred シークレットのコピーに失敗しました	アップグレード ログを確認し、アップグレードを再試行してください。
099	新しいHDDの追加を検証できませんでした	HA 展開の場合はすべてのノードに新しい HDD を追加し、非 HA 展開の場合は 1 つのノードに追加します。
108	シードスクリプトが失敗しました	-
109	永続ボリュームデータのバックアップに失敗しました	アップグレード ログを確認し、アップグレードを再試行してください。
110	永続ボリュームデータの復元に失敗しました	ゼロ RPO またはスナップショットベースのリカバリを使用して、アップグレードを再試行します。
111	RKE2 の etcd タイムアウトパラメータの更新に失敗しました	アップグレード ログを確認し、アップグレードを再試行してください。
112	ダイナミック ストレージ プロビジョナーのアンインストールに失敗しました	-
113	セカンダリノードのリソースの更新に失敗しました	アップグレード ログを確認し、アップグレードを再試行してください。
104	セカンダリノードの再起動に失敗しました	ノードを1つずつ手動で再起動します

アップグレードエラーコード	ワークフロー	解決
100	カーネルロールバックに失敗しました	-
051	動的ストレージプロビジョナーのアップグレードに失敗しました	アップグレード ログを確認し、アップグレードを再試行してください。
056	移行バックアップの削除に失敗しました	NA



ONTAP tools for VMware vSphere以降では、ゼロ RPO はサポートされません。

詳細はこちら ["バージョン 10.0 から 10.1 へのアップグレードに失敗した場合、ONTAP tools for VMware vSphereを復元する方法"](#)

ONTAP tools for VMware vSphereを10.4に移行する

ONTAP tools for VMware vSphereから 10.4 に移行する

ONTAP tools for VMware vSphereのNetApp ONTAP ツールをバージョン 9.xx から 10.x に移行する場合、バージョン間での製品の大幅な更新と機能強化のため、移行プロセスが必要になります。

ONTAP tools for VMware vSphereからONTAP tools for VMware vSphereに移行できます。

セットアップに NFS および VMFS データストアがあり、vVolsデータストアがない場合は、ONTAPツール 9.xx をアンインストールし、ONTAPツール 10.x を展開するだけです。ただし、セットアップにvVolsデータストアが含まれている場合は、VASA プロバイダーと SRA を移行するプロセスを実行する必要があります。

次の表は、これら 2 つの異なるシナリオにおける移行プロセスの概要を示しています。

セットアップにvVolsデータストアがある場合	セットアップにNFSとVMFSデータストアのみが含まれている場合
手順: 1." VASAプロバイダーの移行 " 2. " VMストレージポリシーを作成する "	手順: 1.環境からONTAPツール 9.xx を削除します。参照 " OTV 9.xx を環境から削除する方法 "NetAppナレッジベースの記事。2." ONTAP tools for VMware vSphereを導入および構成する " 3." SRAの更新 " 4. " VMストレージポリシーを作成する "



ONTAP tools for VMware vSphere 9.xx から 10.4 に移行すると、ONTAPツール 10.4 は VMFS データストアでのみ NVMe-oF プロトコルをサポートするため、NVMe/FC プロトコルを使用するvVolsデータストアは動作しなくなります。

VASA プロバイダーを移行し、SRA を更新する

VASAプロバイダーの移行手順

1. ONTAP tools for VMware vSphereで Derby PORT 1527 を有効にするには、root ユーザーを有効にし、SSH 経由で CLI にログインします。次に、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をデプロイします。
3. 移行する vCenter Server インスタンスを、ONTAP tools for VMware vSphereに追加します。参照"[vCenter Serverインスタンスを追加する](#)"詳細についてはこちらをご覧ください。
4. ONTAPツール プラグインの vCenter Server API からストレージ バックエンドをローカルにオンボードします。
5. 移行するには、Swagger または Postman から次の API を発行します。

カール -X POST

`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-jobs``

次の URL から Swagger にアクセスできます。 `https://$FQDN_IP_PORT/'`, for example:
``\https://10.67.25.33:8443。`

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTPメソッド	パス
POST	/api/v1

処理タイプ

非同期

カールの例

カール -X POST'`https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs'` \
--header 'x-auth: <auth_token>' \ --header 'Content-Type: application/json' \ --data '{ "otv_ip":
"xx.xx.xx.xx", "vasa_provider_credentials": { "username": "xxxxx", "password": "" },
"database_password": "" }'

他のリリース移行のリクエスト本文:

{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "ユーザー名": "xxxxx", "パスワード": "*" } }

JSON出力例

ジョブ オブジェクトが返されます。次のステップで使用するためにジョブ ID を保存する必要があります。

{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "実行中" }

6. ステータスを確認するには、Swagger で次の URI を使用します。

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

ジョブが完了したら、移行レポートを確認します。このレポートはジョブ データに含まれており、ジョブ 応答からアクセスできます。

7. ONTAP tools for VMware vSphereをvCenter Serverに追加し、**"VASAプロバイダーを登録する"** ONTAP tools for VMware vSphereを使用します。

8. "VASA Provider の有効化"ONTAP tools for VMware vSphereのサービス。
9. メンテナンス コンソールから、ONTAP tools for VMware vSphereを停止します。

VASA プロバイダーを削除しないでください。

古いVASAプロバイダが停止すると、vCenter ServerはONTAP tools for VMware vSphereにフェイルオーバーします。すべてのデータストアと仮想マシンはONTAP tools for VMware vSphereからアクセス可能になり、サービスが提供されます。

10. ONTAP tools for VMware vSphere 9.xxx から移行された NFS および VMFS データストアは、データストア検出ジョブがトリガーされた後にのみONTAP tools for VMware vSphere 10.4 に表示されます。このジョブが完了するまでに最大 30 分かかる場合があります。VMware vSphere プラグインのユーザー インターフェイス ページのONTAPツールの概要ページにデータストアが表示されていることを確認します。
11. Swagger または Postman で次の API を使用してパッチの移行を実行します。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTPメソッド	パス
PATCH	/api/v1

処理タイプ

非同期

カールの例

curl -X パッチ

```
https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43
```

JSON出力例

ジョブ オブジェクトが返されます。次のステップで使用するためにジョブ ID を保存する必要があります。

```
{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "実行中" }
```

パッチ操作のリクエスト本体は空です。



UUID は、移行後 API への応答として返される移行 UUID です。

パッチ移行 API を実行すると、すべての VM がストレージ ポリシーに準拠します。

次の手順

移行を完了し、ONTAPツール 10.4 を vCenter Server に登録したら、次の手順を実行します。

- 検出 が完了するまで待ちます。証明書はすべてのホストで自動的に更新されます。
- データストアおよび仮想マシンの操作を開始する前に、十分な時間を確保してください。必要な待機時間は、構成内のホスト、データストア、および仮想マシンの数によって異なります。待機しない場合、断続的な操作障害が発生する可能性があります。

アップグレード後、仮想マシンのコンプライアンス状態が古くなっている場合、次の手順に従ってストレージポリシーを再適用します。

1. データストアに移動し、概要 > **VM ストレージ ポリシー** を選択します。

VM ストレージ ポリシー コンプライアンス のコンプライアンス ステータスが 古い と表示されます。

2. ストレージVMポリシーと対応するVMを選択します
3. *適用*を選択

VM ストレージ ポリシー コンプライアンス のコンプライアンス ステータスが準拠として表示されるようになります。

関連情報

- ["ONTAP tools for VMware vSphereについて学ぶ"](#)
- ["ONTAP tools for VMware vSphereから 10.4 へのアップグレード"](#)

ストレージレプリケーションアダプタ(SRA)を更新する手順

開始する前に

リカバリプランにおいて、保護サイトとは仮想マシンが現在実行されている場所を指し、リカバリサイトとは仮想マシンがリカバリされる場所を指します。SRMインターフェースには、リカバリプランの状態と、保護サイトとリカバリサイトの詳細が表示されます。リカバリプランでは、「**CleanupP**」ボタンと「**Reprotect**」ボタンは無効になっていますが、「**TEST**」ボタンと「**RUN**」ボタンは有効なままです。これは、サイトがデータリカバリの準備ができていることを示します。SRAを移行する前に、一方のサイトが保護状態、もう一方のサイトがリカバリ状態であることを確認してください。



フェイルオーバーは完了しているが再保護が保留中の場合は、移行を開始しないでください。移行を続行する前に、再保護プロセスが完了していることを確認してください。テスト フェイルオーバーが進行中の場合は、テスト フェイルオーバーをクリーンアップして移行を開始します。

1. VMware Site Recovery で VMware vSphere 9.xx 用のONTAPツール SRA アダプタを削除するには、次の手順に従います。
 - a. VMware Live Site Recovery 構成管理ページに移動します
 - b. ストレージ レプリケーション アダプタ セクションに移動します。
 - c. 省略記号メニューから*構成のリセット*を選択します。
 - d. 省略記号メニューから*削除*を選択します。
2. 保護サイトと回復サイトの両方でこれらの手順を実行します。
 - a. ["ONTAP tools for VMware vSphereを有効にする"](#)
 - b. ONTAP tools for VMware vSphereを以下の手順でインストールします。 ["VMware Live Site Recovery](#)

アプライアンスでSRAを構成する"。

- c. VMware Live Site Recovery ユーザー インターフェイス ページで、アレイの検出 および デバイスの検出 操作を実行し、デバイスが移行前と同じように表示されていることを確認します。

REST APIを使用した自動化

ONTAP tools for VMware vSphere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。自動化プロセスの一部として使用できる強力な REST API が含まれています。

基盤としてのREST Webサービス

REST (Representational State Transfer) は、Web サービス API の設計を含む分散 Web アプリケーションを作成するためのスタイルです。サーバーベースのリソースを公開し、その状態を管理するための一連のテクノロジを確立します。

リソースと状態の表示

リソースは、REST Web サービス アプリケーションの基本コンポーネントです。REST API を設計する際には、次の 2 つの重要な初期タスクがあります。

- システムまたはサーバーベースのリソースを識別する
- リソースの状態と関連する状態遷移操作を定義する

クライアント アプリケーションは、明確に定義されたメッセージ フローを通じてリソースの状態を表示および変更できます。

HTTPメッセージ

ハイパーテキスト転送プロトコル (HTTP) は、Web サービスのクライアントとサーバーがリソースに関するメッセージを交換するために使用するプロトコルです。これは、作成、読み取り、更新、削除という一般的な操作に基づく CRUD モデルに従います。HTTP プロトコルには、要求ヘッダーと応答ヘッダー、および応答ステータス コードが含まれます。

JSONデータのフォーマット

利用できるメッセージ形式はいくつかありますが、最も一般的なオプションは JavaScript Object Notation (JSON) です。JSON は、単純なデータ構造をプレーンテキストで表現するための業界標準であり、リソースと必要なアクションを記述する状態情報を転送するために使用されます。

セキュリティ

セキュリティは REST API の重要な側面です。ネットワーク上の HTTP トラフィックを保護するために使用される Transport Layer Security (TLS) プロトコルに加えて、ONTAP tools for VMware vSphereは認証にアクセス トークンも使用します。アクセス トークンを取得し、後続の API 呼び出しで使用する必要があります。

非同期リクエストのサポート

ONTAP tools for VMware vSphereは、ほとんどの要求を同期的に実行し、操作が完了するとステータス コードを返します。また、完了までに長い時間を要するタスクの非同期処理もサポートしています。

ONTAPツールマネージャ環境

ONTAPツール マネージャ環境には、考慮すべきいくつかの側面があります。

仮想マシン

ONTAP tools for VMware vSphereは、vSphere リモート プラグイン アーキテクチャを使用して展開されます。REST API のサポートを含むソフトウェアは、別の仮想マシンで実行されます。

ONTAPツールのIPアドレス

ONTAP tools for VMware vSphereは、仮想マシンの機能へのゲートウェイを提供する単一の IP アドレスを公開します。初期構成時にアドレスを指定する必要があり、そのアドレスは内部ロード バランサー コンポーネントに割り当てられます。このアドレスは、ONTAPツール マネージャのユーザー インターフェイスで 사용되는ほか、Swagger ドキュメント ページや REST API に直接アクセスするために使用されます。

2つのREST API

ONTAP tools for VMware vSphereに加えて、ONTAPクラスターには独自の REST API があります。ONTAP ツール マネージャは、ONTAP REST API をクライアントとして使用して、ストレージ関連のタスクを実行します。これら 2 つの API は別個のものであり、異なるものであることを覚えておくことが重要です。

["ONTAP自動化"](#)。

ONTAP tools for VMware vSphereの実装の詳細

REST は共通のテクノロジーとベスト プラクティスのセットを確立しますが、各 API の正確な実装は設計の選択に応じて異なる場合があります。ONTAP tools for VMware vSphereを使用する前に、その設計方法を理解しておく必要があります。

REST API には、vCenter や Aggregates などのいくつかのリソース カテゴリが含まれています。レビュー ["APIリファレンス"](#) 詳細についてはこちらをご覧ください。

REST APIにアクセスする方法

ONTAP tools for VMware vSphereのONTAPツールにアクセスできます。完全な URL には、次のようないくつかの部分があります。

- ONTAPツールのIPアドレスとポート
- APIバージョン
- リソースカテゴリ
- 特定のリソース

初期セットアップ時に IP アドレスを設定する必要がありますが、ポートは 8443 に固定されています。URL の最初の部分は、ONTAP tools for VMware vSphereで一貫しており、エンドポイント間で変更されるのはリソース カテゴリと特定のリソースのみです。



以下の例の IP アドレスとポート値は説明のみを目的としています。環境に合わせてこれらの値を変更する必要があります。

認証サービスにアクセスする例

`https://10.61.25.34:8443/virtualization/api/v1/auth/login`

この URL は、POST メソッドを使用してアクセス トークンを要求するために使用できます。

vCenter Serverを一覧表示する例

`https://10.61.25.34:8443/virtualization/api/v1/vcenters`

この URL は、GET メソッドを使用して定義済みの vCenter Server インスタンスのリストを要求するために使用できます。

HTTP の詳細

ONTAP tools for VMware vSphereは、HTTP および関連パラメータを使用して、リソース インスタンスおよびコレクションを操作します。HTTP 実装の詳細は以下に記載されています。

HTTPメソッド

REST API でサポートされている HTTP メソッドまたは動詞を次の表に示します。

方法	CRUD	説明
GET	読み取り	リソース インスタンスまたはコレクションのオブジェクト プロパティを取得します。コレクションで使用する場合、これはリスト操作と見なされます。
POST	作成	入力パラメータに基づいて新しいリソース インスタンスを作成します。
PUT	更新	指定されたJSONリクエストボディを使用して、リソースインスタンス全体を更新します。ユーザーが変更できないキー値は保持されます。
PATCH	更新	リクエスト内の選択された変更のセットをリソース インスタンスに適用するよう要求します。
DELETE	削除	既存のリソース インスタンスを削除します。

リクエストヘッダーとレスポンスヘッダー

次の表は、REST API で使用される最も重要な HTTP ヘッダーをまとめたものです。

ヘッダー	タイプ	使用上の注意
受け入れる	要求	これは、クライアント アプリケーションが受け入れることができるコンテンツの種類です。有効な値は `*/` または `application/json`。
x-auth	要求	クライアント アプリケーションを通じてリクエストを発行するユーザーを識別するアクセス トークンが含まれます。
コンテンツタイプ	応答	サーバーによって返される `Accept` リクエスト ヘッダー。

HTTPステータスコード

REST API で使用される HTTP ステータス コードについて以下に説明します。

コード	説明	説明
200	OK	新しいリソース インスタンスを作成しない呼び出しが成功したことを示します。
201	作成	リソース インスタンスの一意の識別子を持つオブジェクトが正常に作成されました。

コード	説明	説明
202	承認済み	リクエストが承認され、リクエストを実行するためのバックグラウンド ジョブが作成されました。
204	コンテンツなし	コンテンツは返されませんでしたが、リクエストは成功しました。
400	Bad request	要求の入力が認識されないか不適切です。
401	Unauthorized	ユーザーは承認されていないため、認証する必要があります。
403	Forbidden	認証エラーのためアクセスが拒否されました。
404	Not found	要求で参照されているリソースが存在しません。
409	対立	オブジェクトがすでに存在するため、オブジェクトの作成に失敗しました。
500	内部エラー	サーバーで一般的な内部エラーが発生しました。

認証

REST API へのクライアントの認証は、アクセス トークンを使用して実行されます。トークンと認証プロセスの関連する特性は次のとおりです。

- クライアントは、ONTAPツール マネージャの管理者認証情報 (ユーザー名とパスワード) を使用してトークンを要求する必要があります。
- トークンは JSON Web Token (JWT) としてフォーマットされます。
- 各トークンは 60 分後に期限切れになります。
- クライアントからのAPIリクエストには、`x-auth`リクエスト ヘッダー。

参照["最初のREST API呼び出し"](#)アクセス トークンの要求と使用の例については、こちらをご覧ください。

同期リクエストと非同期リクエスト

ほとんどの REST API 呼び出しはすぐに完了するため、同期的に実行されます。つまり、リクエストが完了した後にステータス コード (200 など) を返します。完了までに時間のかかるリクエストは、バックグラウンド ジョブを使用して非同期的に実行されます。

非同期に実行される API 呼び出しを発行した後、サーバーは 202 HTTP ステータス コードを返します。これは、リクエストが受け入れられたがまだ完了していないことを示します。バックグラウンド ジョブをクエリして、成功や失敗などのステータスを確認できます。

非同期処理は、データストアや vVol 操作など、いくつかの種類の長時間実行操作に使用されます。詳細については、Swagger ページの REST API のジョブ マネージャー カテゴリを参照してください。

ONTAP tools for VMware vSphereの最初の

curl を使用して API 呼び出しを発行し、ONTAP tools for VMware vSphereを開始できます。

開始する前に

curl の例に必要な情報とパラメータを確認する必要があります。

必要な情報

次のものがが必要です:

- ONTAP tools for VMware vSphereのIP アドレスまたは FQDN とポート
- ONTAPツールマネージャ管理者の認証情報（ユーザー名とパスワード）

パラメータと変数

以下に示す curl の例には、Bash スタイルの変数が含まれています。これらの変数は Bash 環境で設定することも、コマンドを発行する前に手動で更新することもできます。変数を設定すると、シェルは各コマンドを実行する前にその値を置き換えます。変数については以下の表で説明します。

変数	説明
\$FQDN_IP_ポート	ONTAPツール マネージャの完全修飾ドメイン名または IP アドレスとポート番号。
\$MYUSER	ONTAPツール マネージャ アカунトのユーザー名。
\$MYパスワード	ONTAPツール マネージャのユーザー名に関連付けられたパスワード。
\$ACCESS_TOKEN	ONTAPツール マネージャによって発行されたアクセス トークン。

Linux CLI での次のコマンドと出力は、変数を設定および表示する方法を示しています。

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

ステップ1: アクセストークンを取得する

REST API を使用するには、アクセス トークンを取得する必要があります。アクセス トークンを要求する方法の例を以下に示します。ご使用の環境に応じて適切な値を代入する必要があります。

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login" \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d '{"username": "$MYUSER", "password": "$MYPASSWORD"}'
```

応答で提供されたアクセス トークンをコピーして保存します。

ステップ2: REST API呼び出しを発行する

アクセス トークンを取得したら、curl を使用して REST API 呼び出しを発行できます。最初のステップで取

得したアクセス トークンを含めます。

Curlの例

```
curl --request GET \  
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \  
--header "Accept: */*" \  
--header "x-auth: $ACCESS_TOKEN"
```

JSON 応答には、ONTAPツール マネージャーに設定されている VMware vCenter インスタンスのリストが含まれます。

ONTAP tools for VMware vSphereの API リファレンス

ONTAP tools for VMware vSphereには、すべての API 呼び出しに関する詳細が記載されています。このリファレンスは、自動化アプリケーションを開発するときに役立ちます。

Swagger ユーザー インターフェイスを通じて、ONTAP tools for VMware vSphereにオンラインでアクセスできます。ONTAP tools for VMware vSphereの IP アドレスまたは FQDN とポートが必要です。

手順

1. 変数に適切な IP アドレスとポートの組み合わせを代入してブラウザに次の URL を入力し、**Enter** キーを押します。

```
https://$FQDN_IP_PORT/
```

例

```
https://10.61.25.33:8443/
```

2. 個々のAPI呼び出しの例として、*vCenters*カテゴリまでスクロールし、エンドポイントの横にある*GET*を選択します。 /virtualization/api/v1/vcenters

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

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

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲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。

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

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

<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、NetAppソフトウェアで使用す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提供されます。

["ONTAP tools for VMware vSphereに関するお知らせ"](#)

著作権に関する情報

Copyright © 2025 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。