



ONTAP Tools for VMware vSphereのドキュメント

ONTAP tools for VMware vSphere 10.1

NetApp
March 17, 2025

目次

ONTAP Tools for VMware vSphereのドキュメント	1
リリースノート	2
リリースノート	2
ONTAP Tools for VMware vSphere 10.1の新機能	2
ONTAP Tools for VMware vSphere 9とONTAP Tools for VMware vSphere 10の機能比較	4
概念	6
ONTAP Tools for VMware vSphereの概要	6
主要な概念と用語	6
ロールベースアクセス制御	8
ONTAP tools for VMware vSphereでのロールベースアクセス制御の概要	8
vCenter Serverアクセス許可のコンポーネント	10
vCenter Serverの権限の割り当てと変更	11
ONTAP Tools for VMware vSphereのタスクに必要な権限	12
ONTAP Tools for VMware vSphereで推奨されるONTAPロール	13
ONTAP tools for VMware vSphereの高可用性	14
AutoSupport	14
ONTAP Tools for VMware vSphereの導入	15
ONTAP Tools for VMware vSphereを導入するための前提条件	15
ストレージとアプリケーションの最小要件	15
導入に関するその他の考慮事項	15
ONTAP Tools for VMware vSphereのダウンロード	16
コンテンツライブラリ	16
ONTAP tools for VMware vSphereを導入するための構成の制限	17
ONTAP Tools for VMware vSphere - Storage Replication Adapter (SRA)	17
ONTAP Tools for VMware vSphereの導入準備	18
導入の準備	18
非HAシングルノード構成の導入	19
HA構成を導入する	22
ONTAP Tools for VMware vSphereセットアップのリカバリ	27
導入エラーコード	28
ONTAPツールの設定	32
ONTAP tools Managerユーザインターフェイス	32
vCenter Serverインスタンスの追加と管理	32
vCenter Serverインスタンスを追加する	32
ONTAP Tools for VMware vSphereプラグインをvCenter Serverインスタンスに登録	33
ONTAP Tools for VMware vSphereプラグインの登録解除	33
VASA ProviderをvCenter Serverインスタンスに登録する	33
登録されたVASAプロバイダを確認	34
NFS VAAIプラグインをインストールする	34

ホストデータの更新	35
ESXiホストの設定	36
ESXiサーバのマルチパスとタイムアウトの設定	36
ESXiホストの値の設定	36
ストレージシステムとホストの検出	38
ストレージバックエンドを追加します	39
ONTAP tools Managerを使用したストレージバックエンドの追加	39
vSphere Client UIを使用してストレージバックエンドを追加します。	39
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	40
ネットワークアクセスの設定	40
ONTAPユーザのロールと権限の設定	41
SVMアグリゲートのマッピングの要件	42
ONTAPのユーザとロールを手動で作成する	42
管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト	43
NetApp ONTAP Tools for VMware vSphereプラグインのダッシュボードの概要	44
データストアを作成	46
vVolデータストアを作成する	47
NFSデータストアを作成する	47
VMFSデータストアの作成	48
データストアと仮想マシンの保護	49
SRAを有効にしてデータストアを保護する	49
ディザスタリカバリ用のストレージシステムの設定	49
SAN環境およびNAS環境向けのSRAの設定	49
大規模な環境向けのSRAの設定	50
SRMアプライアンスでSRAを設定する	51
SRAクレデンシャルの更新	52
保護対象サイトとリカバリサイトの設定	53
保護グループの設定	53
保護対象サイトとリカバリサイトをペアリング	53
保護サイトとリカバリサイトのリソースを設定	54
レプリケートされたストレージシステムの確認	58
ONTAPツールの管理	60
データストアの管理	60
NFSデータストアとVMFSデータストアのマウント	60
vVolデータストアのマウント	60
NFSデータストアとVMFSデータストアのサイズ変更	60
vVolデータストアの拡張	61
vVolデータストアの縮小	61
データストアの削除	62
データストアのONTAPストレージビュー	62
仮想マシンストレージビュー	63

ストレージのしきい値の管理	64
ストレージバックエンドを管理	64
ストレージの検出	64
ストレージバックエンドの変更	64
ストレージバックエンドの削除	65
ストレージバックエンドのドリルダウンビュー	65
vCenter Serverインスタンスを管理します。	66
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または関連付け解除する	66
vCenter Serverインスタンスの変更	66
vCenter Serverインスタンスの削除	67
証明書の管理	67
igroupとエクスポートポリシーを管理します。	68
ONTAP Tools for VMware vSphereメンテナンスコンソールへのアクセス	68
ONTAP Tools for VMware vSphereメンテナンスコンソールの概要	69
リモート診断アクセスの設定	70
他のノードでSSHを開始する	71
vCenter ServerとONTAPのクレデンシャルを更新する	71
ONTAP Toolレポート	71
ログファイルを収集する	72
仮想マシンの管理	73
仮想マシンの移行またはクローニングに関する考慮事項	73
NFSおよびVMFSデータストアを使用する仮想マシンをvVolデータストアに移行する	74
VASAのクリーンアップ	74
ONTAPツールを使用したESXiホストの設定の変更	74
パスワードを管理します	75
ONTAP tools Managerのパスワードの変更	75
ONTAP tools Managerのパスワードのリセット	75
アプリケーションユーザパスワードのリセット	76
メンテナンスコンソールのユーザパスワードのリセット	76
ボリュームをクリーンアップ	77
ONTAPツールのアップグレード	79
ONTAP toolsの最新リリースへのアップグレード	79
アップグレードのエラーコード	81
ONTAPツールの移行	83
最新リリースのONTAP toolsに移行する	83
一般的な移行手順	83
SRAの移行手順	83
VASA Providerの移行手順	84
REST APIによる自動化	88
REST APIの概要	88
ONTAP tools for VMware vSphere REST APIにアクセスする方法	88

ネットワークに関する考慮事項	88
ONTAP Tools for VMware vSphere APIオンラインドキュメントページ	88
カスタムのソフトウェアとツール	88
API要求を制御する入力変数	89
HTTP メソッド	89
要求ヘッダー	89
リクエストの本文	90
オブジェクトのフィルタリング	90
特定のオブジェクトフィールドの要求	90
出力セット内のオブジェクトのソート	91
コレクション内のオブジェクトを取得するときのページネーション	91
サイズのプロパティ	92
Swagger UIからONTAP Tools for VMware vSphere APIのリファレンスドキュメントにアクセス	93
REST APIの使用を開始する	93
Hello world	93
ワークフロー	94
ストレージ検出	94
SVMアグリゲートのマッピングの要件	95
vCenter Serverインスタンスを使用したオンボードストレージバックエンド（SVMまたはクラスタ）	95
vVolデータストアの作成	96
vVolデータストアのマウントとアンマウント	97
VVolデータストアのストレージの拡張または縮小	98
vVolデータストアの削除	100
ストレージしきい値の管理	101
ネットワークアクセスの管理	102
法的通知	103
著作権	103
商標	103
特許	103
プライバシーポリシー	103
オープンソース	103

ONTAP Tools for VMware vSphereのドキュメント

リリースノート

リリースノート

ONTAP Tools for VMware vSphere 10.1の新機能と拡張機能について説明します。

新機能と拡張機能の一覧については、を参照してください[ONTAP Tools for VMware vSphere 10.1の新機能](#)。

ONTAP tools for VMware vSphere 9からONTAP tools 10.1への移行が導入環境に適しているかどうかの詳細については、を参照して[ONTAP Tools for VMware vSphere 9とONTAP Tools for VMware vSphere 10の機能比較](#)ください。ONTAP tools for VMware vSphere 9.10D2、9.11D4、9.12、9.13リリースからONTAP tools 10.1への移行がサポートされます。

ONTAP tools for VMware vSphere 10.1の既知の問題および制限事項の詳細については、を参照して "[ONTAP Tools for VMware vSphere 10.1リリースノート](#)"ください。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 10.1の新機能

ONTAP Tools for VMware vSphere 10.1の新機能について説明します。

更新	製品説明
NFSおよびVMFSデータストアのサポート	このリリースのONTAP tools for VMware vSphereでは、VASA ProviderおよびNFS v3およびVMFSデータストアを使用したVVolデータストアのプロビジョニングがサポートされます。データストアの作成、サイズ変更、マウント、アンマウント、削除などの処理がサポートされます。iSCSIプロトコルを使用してVMFSデータストアをプロビジョニングできます。VMware管理者は、iSCSI VMFSデータストアをONTAP tools for VMware vSphere 9.xxから10.1バージョンにシームレスに導入、アップグレード、移行できます。ONTAP tools for VMware vSphere 9.10D2、9.11D4、9.12、9.13リリースから10.1リリースへの移行がサポートされます。
NFSおよびVMFSデータストア用のStorage Replication Adapter (SRA)	SRAは、VMware Site Recovery Manager (SRM) 仕様ベースのディザスタリカバリ (DR) を実装します。NFSデータストアの場合、ONTAPボリュームはNFS v3プロトコルを使用してESXiホストにマウントされます。VMFSデータストアの場合、ONTAP LUNはiSCSIプロトコルを使用してESXiホストにマウントされます。 ONTAP SnapMirror関係では、デスティネーションサイトのボリュームとLUNがレプリケートされます。SRAでは、VMware SRMから呼び出されるtestFailover、failover、およびreprotectコマンドが実装されます。実装の一環として、SRAは、リカバリインシデントですべてのボリュームとLUNがデスティネーションにマウント可能になり、セカンダリサイトのボリュームとLUNが読み取られてデータの不一致を回避します。

更新	製品説明
すべてのワークフローに対応する豊富なvCenterユーザインターフェイス (UI) 統合をサポート	ONTAP tools for VMware vSphere 10.1は、ワークフロー向けのグラフィカルユーザインターフェイスを提供し、ONTAP tools for VMware vSphere 9.xxリリースと同等の機能を提供します。リモートプラグインは、次の機能をサポートしています。 • NFS、VMFS、vVolデータストアのオブザーバビリティと監視 • NFSおよびVMFSデータストア向けStorage Replication Adapter • VASA Providerの登録と登録解除 • VAAIフラクインノインストール • 選択したvCenterのログバンドルダウンロード
簡単な展開バリエーションのサポート	ONTAP Tools for VMware vSphere 10.1を迅速にオンボードし、簡単な導入オプションを使用してその機能を体験できます。簡単な導入でSnapshotベースのリカバリがサポートされます。
すべてのONTAP tools管理ワークフローに対応するONTAP tools Manager UI	ONTAP tools Managerを使用すると、ONTAP tools管理者は、管理対象のvCenterインスタンスやオンボードストレージバックエンドをより細かく制御できます。ONTAP Tools Managerは、次のことを支援します。 • vCenterの管理- ONTAP tools for VMware vSphereにvCenter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ストレージクラスをONTAP tools for VMware vSphereに追加および管理し、オンボードされたvCenter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、すべての証明書を更新または更新します。 • パスワード管理- OVAアプリケーションのユーザパスワードをリセットします。
証明書管理	ONTAP tools for VMware vSphereの単一インスタンスで、複数のvCenterインスタンスを管理できます。ONTAP tools for VMware vSphereを導入すると、デフォルトではすべてのvCenterインスタンスに自己署名証明書が割り当てられます。複数のvCenterインスタンスを管理していて、複数のvCenterインスタンスでVVol機能を有効にする場合は、ONTAP tools Managerインターフェイスを使用して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。同じインターフェイスを使用して、すべての証明書を更新または更新できます。
ゼロ目標復旧時点 (RPO) リカバリ	ONTAP tools for VMware vSphereのセットアップを失った場合は、ONTAP データ管理ソフトウェアを使用してONTAP toolsのセットアップをリカバリしても、データを損失することはありません。簡単な導入オプションでは、ゼロRPOリカバリはサポートされていません。

更新	製品説明
導入時のiSCSIプロトコルのサポート	Tridentでは、永続ボリュームのプロビジョニングでNFSプロトコルとiSCSIプロトコルがサポートされています。ONTAP tools for VMware vSphereを導入する際には、iSCSIプロトコルを使用してVASAプロバイダサービスのデータを永続ボリュームに格納できます。
ストレージとvCenterのオンボーディングでのIPv6アドレスのサポート	IPv4アドレス、IPv6アドレス、またはFully Qualified Domain Name (FQDN；完全修飾ドメイン名) を使用してストレージバックエンドをオンボードできます。ストレージサービスとストレージプロキシサービスは、同じIPv4またはIPv6アドレスのオンボードクレデンシャルを使用してONTAP REST APIと通信します。データパスは、エクスポートポリシールールを使用して、IPv4アドレス、IPv6アドレス、またはFQDNでサポートされます。

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への移行が適しているかどうかをご確認ください。互換性に関する最新情報については、[を参照してください "NetApp Interoperability Matrix Tool"](#)。

機能	ONTAPツール9.13	ONTAPツール10.1
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、運用開始から運用を合理化、簡易化	高可用性、パフォーマンス、拡張性の制限を拡張しながら、ONTAP tools 10.xを9.xパリティに移行
ONTAPリリースの認定	ONTAP 9 .9.1からONTAP 9 .15.1へ	ONTAP 9 .12.1からONTAP 9 .14.1へ
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へ	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7からVMware Live Site Recovery 9.0へ
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) vVol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) vVolデータストア：iSCSI、NFS v3
拡張性	ホストとVM：300台のホスト、最大10、000台のVMデータストア：NFS×600、VMFS×最大50、VVOL×最大250：最大14K	ホストとVM：600個のホストVVOL：最大140K
オブザーバビリティ	パフォーマンス、容量、ホストコンプライアンスのダッシュボードVMとデータストアの動的なレポート	パフォーマンス、容量、ホストコンプライアンスに関するダッシュボードが更新されました。Dynamic VMとデータストアに関するレポートが更新されました。

機能	ONTAPツール9.13	ONTAPツール10.1
データ保護	VMFS用とNFS用のSRAレプリケーション FlexVolベースのレプリケーション でvVol SCVを統合し、バックアップに相互運用可能	iSCSI VMFSデータストアおよびNFS v3データストア用のSRAレプリケーション

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一連のツールです。VMwareエコシステムと統合することで、データストアのプロビジョニングや仮想マシンの基本的な保護を支援します。ONTAP Tools for VMware vSphereにより、管理者はストレージライフサイクル管理をシームレスに管理できます。

ONTAP tools for VMware vSphere 10.1リリースは、拡張性に優れたイベントベースのマイクロサービスを、オープン仮想アプライアンス（OVA）として導入したものです。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は次のコンポーネントで構成されています。

- 基本的な保護やディザスタリカバリなどの仮想マシン機能
- VASA ProviderによるVMのきめ細かな管理
- ポリシーベースのストレージ管理
- Storage Replication Adapter（SRA）

主要な概念と用語

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

認証局（CA）

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

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アドレスの両方の同時使用をサポートするネットワーク環境です。

高可用性（HA）

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

論理ユニット番号（LUN）

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

ONTAP ツール マネージャ

ONTAP tools Managerを使用すると、管理対象のvCenter Serverインスタンスやオンボードストレージバックエンドに対して、VMware vSphere管理者向けのONTAP toolsをより細かく制御できます。ONTAP Tools Mangerを使用すると、vCenter Serverインスタンス、ストレージバックエンド、証明書、パスワード、ログバンドルのダウンロードを管理できます。

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

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

SnapMirrorアクティブ (SMAS)

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

Storage Replication Adapter (SRA)

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

Storage Virtual Machine (SVM)

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

Virtual Machine File System (VMFS)

VMFSは、VMware vSphere環境に仮想マシンファイルを格納するために特別に設計されたクラスタファイルシステムです。

仮想ボリューム (VVOL)

VVOLは、仮想マシンで使用されるストレージをボリュームレベルで抽象化します。これにはいくつかの利点があり、従来のLUNを使用する代わりに使用できます。VVOLデータストアは、通常、VVOL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

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

VMware Site Recovery Manager (SRM)

SRMは、VMware仮想環境のビジネス継続性、ディザスタリカバリ、サイト移行、および無停止テスト機能を提供します。

VMware vSphere APIs for Storage Awareness (VASA)

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

VMware vSphere Storage APIs - Array Integration (VAAI)

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

vVolデータストア

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

RPOゼロ

RPOはRecovery Point Objective（目標復旧時点）の略で、所定の時間内に許容可能とみなされるデータ損失量です。RPOがゼロの場合は、データ損失が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でのロールベースアクセス制御の概要

vCenter Serverには、vSphereオブジェクトへのアクセスを制御するためのRole-Based Access Control (RBAC；ロールベースアクセス制御) が用意されています。vCenter Serverは、ロールとPrivilegesでユーザ権限とグループ権限を使用して、インベントリ内のさまざまなレベルで一元的な認証および承認サービスを提供します。

コンポーネント	製品説明
権限	vSphereで操作を実行するためのアクセスを有効または拒否します。
役割	ロールには、1つ以上のシステム権限が含まれています。各権限は、システム内の特定のオブジェクトまたはタイプのオブジェクトに対する管理権限を定義します。ユーザにロールを割り当てると、そのロールで定義されている権限の機能が継承されます。
ユーザとグループ	ユーザとグループは、Active Directory (AD) からロールを割り当てる権限で使用されます。vCenter Serverには、使用可能な独自のローカルユーザとローカルグループがあります。
権限	権限を使用すると、Privilegesをユーザまたはグループに割り当てて、特定の操作を実行し、vCenter Server内のオブジェクトに変更を加えることができます。vCenter Serverの権限は、ESXiホストに直接ログインするユーザではなく、vCenter Serverにログインするユーザにのみ影響します。

オブジェクト	アクションが実行されるエンティティ。VMware vCenterオブジェクトは、データセンター、フォルダ、リソースプール、クラスタ、ホスト、 およびVM
--------	--

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



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

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

vCenter Serverのロールの割り当てと変更に関するキーポイント

vCenter Serverのロールは、vSphereのオブジェクトおよびタスクへのアクセスを制限する場合にのみ設定します。それ以外の場合は、管理者としてログインできます。このログインにより、すべてのvSphereオブジェクトに自動的にアクセスできるようになります。

ロールを割り当てる場所によって、ユーザが実行できるONTAP Tools for VMware vSphereタスクが決まります。一度に1つのロールを変更できます。ロール内の権限を変更した場合、そのロールに関連付けられているユーザは、更新されたロールを有効にするためにログアウトしてから再度ログインする必要があります。

ONTAP Tools for VMware vSphereに付属の標準ロール

vCenter Serverの権限とRBACを簡単に使用できるように、ONTAP Tools for VMware vSphereには、主要なONTAPツールfor VMware vSphereタスクを実行できる標準のONTAPツールfor VMware vSphereロールが用意されています。タスクを実行せずに情報を表示できる読み取り専用ロールもあります。

ONTAP Tools for VMware vSphereの標準ロールを表示するには、vSphere Clientのホームページで*[ロール]*をクリックします。ONTAP Tools for VMware vSphereのロールで、次のタスクを実行できます。

* 役割 *	* 概要 *
VMware vSphere管理者向けNetApp ONTAPツール	ONTAP tools for VMware vSphereの一部のタスクを実行するために必要なvCenter Server標準の権限とONTAP tools固有の権限がすべて含まれています。
NetApp ONTAP Tools for VMware vSphere読み取り専用	ONTAP toolsへの読み取り専用アクセスを許可します。アクセスが制御されたONTAP tools for VMware vSphereアクションを実行することはできません。
NetApp ONTAP Tools for VMware vSphereのプロビジョニング	ストレージのプロビジョニングに必要なvCenter Server標準の権限とONTAP tools固有の権限が含まれています。次のタスクを実行できます。 - 新しいデータストアを作成する - データストアの管理

ONTAP tools Managerの管理者ロールがvCenter Serverに登録されていません。このロールは、ONTAP tools Managerに固有です。

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

この場合は、必要なONTAP tools for VMware vSphereロールのクローンを作成し、そのクローンを編集してユーザに必要な権限だけを付与します。

ONTAPストレージバックエンドとvSphereオブジェクトの権限

vCenter Serverアクセス許可が十分であれば、ONTAP tools for VMware vSphereは、ストレージバックエンドのクレデンシャル（ユーザ名とパスワード）に関連付けられているONTAP RBAC権限（ONTAPロール）を確認します。そのストレージバックエンドでONTAP tools for VMware vSphereタスクに必要なストレージ処理を実行するための十分な権限があるかどうかを確認する。正しいONTAP Privilegesがあれば、ストレージバックエンドにアクセスしてONTAP Tools for VMware vSphereタスクを実行できます。ストレージバックエンドで実行できるONTAP Tools for VMware vSphereタスクは、ONTAPロールで決まります。

vCenter Serverアクセス許可のコンポーネント

vCenter Serverで認識されるのはアクセス許可で、Privilegesではありません。各vCenter Serverアクセス許可は3つのコンポーネントで構成されます。

vCenter Serverには次のコンポーネントがあります。

- 1つ以上のPrivileges（ロール）

ユーザが実行できるタスクを定義します。

- vSphereオブジェクト

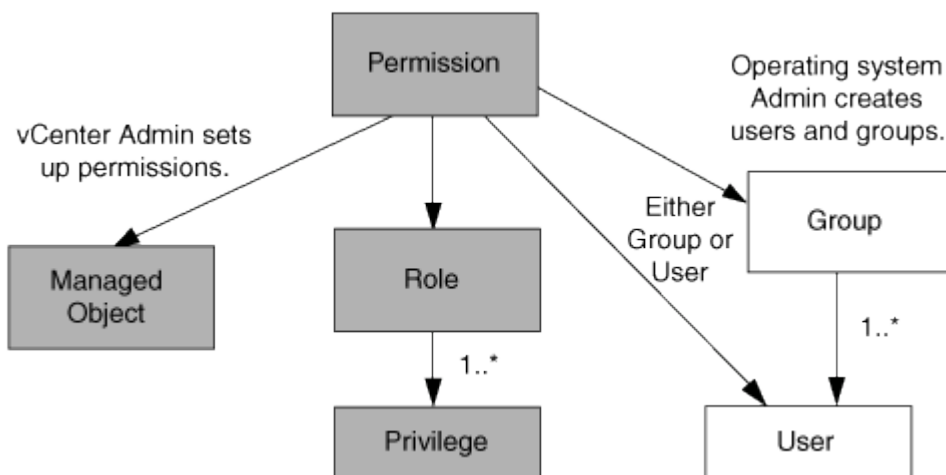
オブジェクトはタスクのターゲットです。

- ユーザまたはグループ

タスクを実行できるユーザまたはグループを定義します。



グレーのボックスはvCenter Serverにあるコンポーネント、白のボックスはvCenter Serverを実行しているオペレーティングシステムにあるコンポーネントを示しています。



権限

ONTAP Tools for VMware vSphereには、次の2種類のPrivilegesが関連付けられています。

- vCenter Server Privileges標準

これらのPrivilegesはvCenter Serverに付属しています。

- ONTAP tools固有のPrivileges

これらの権限は、特定のONTAP Tools for VMware vSphereタスク用に定義されています。ONTAP Tools for VMware vSphereに固有の機能です。

ONTAP tools for VMware vSphereのタスクには、ONTAP tools固有の権限とvCenter Server標準の権限の両方が必要です。これらの権限は、ユーザーのロールを構成しますアクセス許可には複数の権限を含めることができます。これらのPrivilegesは、vCenter Serverにログインしているユーザ用です。



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

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

vSphereオブジェクト

アクセス許可はvSphereオブジェクトに関連付けられます。vCenter Server、ESXiホスト、仮想マシン、データストア、データセンター、フォルダなどがあります。任意のvSphereオブジェクトに権限を割り当てることができます。vSphereオブジェクトに割り当てられたアクセス許可に基づいて、そのオブジェクトに対してどのユーザがどのタスクを実行できるかがvCenter Serverによって決まります。ONTAP tools for VMware vSphere固有のタスクの場合、アクセス許可の割り当てと検証はルートフォルダレベル（vCenter Server）でのみ行われ、他のエンティティでは行われません。ただしVAAIプラグインの処理は例外で、該当するESXiホストに対して権限が検証されます。

ユーザとグループ

ユーザとグループは、Active Directory（またはローカルのvCenter Serverマシン）を使用して設定できます。その後、vCenter Serverアクセス許可を使用してこれらのユーザまたはグループにアクセスを許可し、特定のONTAP Tools for VMware vSphereタスクを実行できるようにします。



これらのvCenter Serverアクセス許可は、ONTAP tools for VMware vSphere vCenterユーザに適用され、ONTAP tools for VMware vSphere管理者には適用されません。ONTAP tools for VMware vSphereの管理者には、デフォルトでフルアクセス権が付与され、権限を割り当てる必要はありません。

ユーザとグループにはロールは割り当てられません。vCenter Serverアクセス許可に含まれることでロールにアクセスできます。

vCenter Serverの権限の割り当てと変更

vCenter Serverのアクセス許可を使用する場合は、いくつかの重要な点に注意する必要

があります。ONTAP tools for VMware vSphereのタスクを実行できるかどうかは、アクセス許可を割り当てた場所や、アクセス許可の変更後にユーザが実行した操作によって異なります。

権限の割り当て

vCenter Serverのアクセス許可は、vSphereのオブジェクトおよびタスクへのアクセスを制限する場合にのみ設定します。それ以外の場合は、管理者としてログインできます。このログインにより、すべてのvSphereオブジェクトに自動的にアクセスできるようになります。

権限の割り当て先によって、ユーザが実行できるONTAP tools for VMware vSphereタスクが決まります。

場合によっては、タスクを確実に完了させるために、ルートオブジェクトなどの上位レベルに権限を割り当てる必要があります。これは、特定のvSphereオブジェクトには適用されない権限（タスクの追跡など）がタスクに必要な場合や、必要な権限がvSphere以外のオブジェクト（ストレージシステムなど）に適用される場合に該当します。

このような場合は、子エンティティに継承されるようにアクセス許可を設定できます。子エンティティに他の権限を割り当てることもできます。子エンティティに割り当てたアクセス許可は、親エンティティから継承されたアクセス許可を上書きします。つまり、子エンティティにアクセス許可を付与して、ルートオブジェクトに割り当てられ、子エンティティに継承されるアクセス許可の範囲を制限できます。



会社のセキュリティポリシーでアクセス許可の制限が厳しい場合を除き、ルートオブジェクト（ルートフォルダとも呼ばれます）にアクセス許可を割り当てることをお勧めします。

アクセス許可と非vSphereオブジェクト

作成したアクセス許可はvSphere以外のオブジェクトに適用されます。たとえば、ストレージシステムはvSphereオブジェクトではありません。ストレージシステムの環境権限がある場合は、tools for VMware vSphereルートオブジェクトに割り当てることができるvSphereオブジェクトがないため、その権限を含むアクセス許可をONTAP tools for VMware vSphereルートオブジェクトに割り当てする必要があります。

たとえば、ONTAP tools for VMware vSphereの「Add/Modify/Skip storage systems」などの権限を含むすべてのアクセス許可は、ルートオブジェクトレベルに割り当てする必要があります。

アクセス許可の変更

変更できる権限は一度に1つです。

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

ONTAP Tools for VMware vSphereのタスクに必要な権限

ONTAP Tools for VMware vSphereのタスクごとに、ONTAP Tools for VMware vSphere固有の権限とvCenter Server標準の権限の組み合わせが異なります。

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

View *権限では、VMware vSphere用のONTAPツールにアクセスできます。この権限では、ONTAP tools for VMware vSphere内でタスクを実行することはできません。ONTAP tools for VMware vSphereのタスクを実行するには、タスクに対する適切なONTAP tools固有の権限とvCenter Server標準の権限が必要です。

割り当てレベルによって、UIのどの部分を表示できるかが決まります。ルートオブジェクト（フォルダ）にView権限を割り当てると、NetAppアイコンをクリックしてONTAP tools for VMware vSphereにアクセスできるようになります。

別のvSphereオブジェクトレベルにView権限を割り当てることもできますが、その場合、表示および使用できるONTAP Tools for VMware vSphereメニューが制限されます。

View権限を含むアクセス許可は、ルートオブジェクトに割り当ててを推奨します。

ONTAP Tools for VMware vSphereで推奨されるONTAPロール

ONTAP tools for VMware vSphereおよびRole-Based Access Control（RBAC；ロールベースアクセス制御）を使用する際に推奨されるONTAPロールを設定できます。これらのロールには、ONTAP tools for VMware vSphereタスクで実行するストレージ処理の実行に必要なONTAP権限が含まれています。

新しいユーザロールを作成するには、ONTAPを実行するストレージシステムの管理者としてログインする必要があります。ONTAP System Manager 9.8P1以降を使用してONTAPロールを作成できます。

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

セキュリティ対策として、ONTAP Tools for VMware vSphere固有のONTAPロールは階層構造になっています。最初のロールは最も制限が高く、ONTAP tools for VMware vSphereのストレージ処理の最も基本的なセットに関連する権限のみが含まれています。次のロールには、そのロール独自の権限と、前のロールに関連付けられているすべての権限が含まれます。ロールを追加するたびに、サポートされるストレージ処理に対する制限が少なくなります。

ONTAP Tools for VMware vSphereを使用する際に推奨されるONTAP RBACロールの一部を次に示します。ロールを作成したら、仮想マシンのプロビジョニングなど、ストレージに関するタスクを実行する必要があるユーザに割り当てることができます。

* 役割 *	権限
調査	ストレージシステムを追加できます。
ストレージの作成	ストレージを作成できます。また、Discoveryロールに関連付けられているすべての権限が含まれます。
ストレージの変更	ストレージを変更できます。また、DiscoveryロールとCreate Storageロールに関連付けられているすべての権限が含まれます。
ストレージの削除	ストレージを破棄できます。また、Discoveryロール、Create Storageロール、Modify Storageロールに関連付けられているすべての権限が含まれます。

ONTAP tools for VMware vSphereを使用している場合は、Policy-Based Management（PBM；ポリシーベー

ス管理) ロールも設定します。ストレージポリシーを使用してストレージを管理できます。このロールを使用するには、「検出」ロールも設定する必要があります。

ONTAP tools for VMware vSphereの高可用性

ONTAP tools for VMware vSphereは、障害発生時にONTAP tools for VMware vSphereの機能を中断なく提供するためのハイアベイラビリティ (HA) 構成をサポートしています。

高可用性 (HA) ソリューションでは、次の原因でシステムが停止した場合に迅速にリカバリできます。

- ホストノショウカイ



単一ノード障害のみがサポートされます。

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

高可用性 (HA) を実現するためにONTAP tools for VMware vSphereを追加で設定する必要はありません。



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

AutoSupport

AutoSupportは、システムヘルスをプロアクティブに監視し、NetAppテクニカルサポート、社内のサポート部門、およびサポートパートナーにメッセージを自動的に送信するメカニズムです。

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

AutoSupportを有効または無効にできるのは導入時のみです。有効のままにしておくことをお勧めします。AutoSupportを有効にすると、問題の検出時間が短縮され、解決までの時間が短縮されます。AutoSupportが無効になっている場合でも、AutoSupportの情報が収集されてローカルに格納されます。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。送信を成功させるには、ネットワークに216.240.21.18 // support.netapp.com URLを含める必要があります。

ONTAP Tools for VMware vSphereの導入

ONTAP Tools for VMware vSphereを導入するための前提条件

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

ONTAP Tools for VMware vSphereは、VMware vCenter Server Virtual Appliance (vCSA) で使用できます。ONTAP Tools for VMware vSphereは、ESXiシステムを含むサポートされているvSphere Clientに導入する必要があります。

- ノードあたりのインストールパッケージのスペース要件
 - シンプロビジョニング環境の場合は10GB
 - シックプロビジョニングの場合は248GB
- *ノードあたりのホストシステムのサイジング要件*導入サイズおよびノードあたりの推奨メモリは次の表のとおりです。

展開の種類	* CPU *	メモリ (GB)
小 (S)	8	16
中 (M)	12	24
大 (L)	16	32

"ONTAP tools for VMware vSphereを導入するための構成の制限"詳細については、を参照してください。

ストレージとアプリケーションの最小要件

ストレージ、ホスト、およびアプリケーション	最小バージョン要件
ONTAP	ONTAP 9.12.1、9.13.1、または9.14.1の最新パッチリリース
ESXiホスト	ESXi 7.0.3
vCenterサーバ	vCenter 7.0U3
VASA Provider	3.0
OVAアプリケーション	10.1

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

["Interoperability Matrix Tool"](#)

導入に関するその他の考慮事項

ONTAP toolsの導入をカスタマイズするときは、いくつかの要件を考慮する必要があります。

アプリケーションユーザのパスワード

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

アプライアンスのメンテナンスコンソールのクレデンシャル

メンテナンスコンソールには「maint」ユーザ名を使用してアクセスする必要があります。導入時に「maint」ユーザのパスワードを設定できます。vCenter ServerでVMを再起動する際に使用できる[Restart guest OS]オプションを使用して、パスワードを変更できます。

アプライアンスのネットワークプロパティ

ONTAP tools for VMware vSphereの有効なDNSホスト名（非修飾）と静的IPアドレス、およびその他のネットワークパラメータを指定します。指定したIPアドレスに、導入時に選択したVLANネットワークからアクセスできる必要があります。DHCPは、ONTAP tools for VMware vSphere 10.1リリースではサポートされません。これらのパラメータはすべて、適切なインストールと操作に必要です。

ONTAP Tools for VMware vSphereのダウンロード

`.zip`ONTAP tools for VMware vSphereのバイナリ（
`\_ova\_`）と署名済み証明書を含むファイルは、からダウンロードできます
[https://mysupport.netapp.com/site/products/all/details/otv/downloads-](https://mysupport.netapp.com/site/products/all/details/otv/downloads-tab[\)
[tab\[\"NetAppサポートサイト\"\]](https://mysupport.netapp.com/site/products/all/details/otv/downloads-tab[\)。

導入が完了すると、ONTAP Tools for VMware vSphereおよびVASA製品が環境にインストールされます。デフォルトでは、導入モデルを決定し、要件に基づいてVASA Providerを有効にするかどうかを選択すると、すぐにONTAP Tools for VMware vSphereが機能し始めます。詳細は、を参照してください "[VASA ProviderをvCenter Serverインスタンスに登録する](#)"。

コンテンツライブラリ

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



コンテンツライブラリは、クラスタ内のすべてのホストがアクセスできるように、共有データストアに格納します。HA構成にOVAを導入する前に、OVAを格納するコンテンツライブラリを作成する必要があります。次の手順に従ってコンテンツライブラリを作成します。

• 手順 *

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
2. vSphere Clientの横の省略記号を選択し、*[Content library]*を選択します。
3. ページの右側にある*[作成]*を選択します。
4. ライブラリの名前を指定し、コンテンツライブラリを作成します。

- 作成したコンテンツライブラリに移動します。
- ページの右側の*を選択し、[Import item]*を選択してOVAファイルをインポートします。

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

次の表は、VMware vSphere用のONTAP toolsを設定する際のガイドとして使用できます。

* 導入 *	* タイプ *	* VVOLの数*	ホスト数	プロトコルタイプ
容易な導入	小 (S)	~12、000	32	NFS、iSCSI
容易な導入	中 (M)	最大24、000	64	NFS、iSCSI
高可用性	小 (S)	最大24、000	64	NFS、iSCSI
高可用性	中 (M)	約50k	128	NFS、iSCSI
高可用性	大 (L)	~100k	256 [注]表のホスト数は、複数のvCenterからのホストの総数を示しています。	NFS、iSCSI

ノードごとのホストシステムのサイジング要件の詳細については、を参照してください["ONTAP Tools for VMware vSphereを導入するための前提条件"](#)。

ONTAP Tools for VMware vSphere - Storage Replication Adapter (SRA)

次の表に、ONTAP tools for VMware vSphereを使用した場合に、SRMインスタンスごとにサポートされる数を示します。

* vCenterの導入規模*	小さい	中
アレイベースのレプリケーションを使用した保護用に構成された仮想マシンの総数	2000	5000
アレイベースのレプリケーション保護グループの総数	250	250
リカバリプランあたりの保護グループの総数	50	50
レプリケートされたデータストア数	255	255
VM数	4000	7000

次の表に、SRMの数と、VMware vSphereの導入規模に対応するONTAPツールを示します。

* SRMインスタンスの数*	* ONTAPツールの導入規模*
最大4	小規模

4～8	中
8人以上	大規模

詳細については、を参照してください ["VMware Live Site Recoveryの運用上の制限"](#)。

ONTAP Tools for VMware vSphereの導入準備

ONTAP tools for VMware vSphereの導入を開始する前に、ストレージバックエンドの基本要件、アプリケーション要件、およびライセンス要件を確認しておく必要があります。事前に導入計画を立て、環境でONTAP tools for VMware vSphereをどのように設定するかを決めておきます。

導入の準備

導入を進める前のONTAP Tools for VMware vSphereの要件は次のとおりです。

1. vCenter Server 環境を設定およびセットアップします。
2. `_ova_` ファイルをダウンロードします。
3. (任意) NetAppが提供するPostmanコレクションJSONファイルを自動化ユーザ収集するために使用します。
4. OVAを導入するための親vCenter Serverのクレデンシャル。vCenter Serverの親のパスワードに次の特殊文字を使用することはできません (\$、'、")。
5. OVAを導入するホストまたはリソースプールに、["ONTAP Tools for VMware vSphereを導入するための前提条件"](#)セクションに記載されている最小限のリソースがあることを確認します。
6. 導入後にONTAP tools for VMware vSphereが登録用に接続するvCenter Serverインスタンスのログインクレデンシャル。
7. ブラウザキャッシュを削除します。
8. 非HA環境では、3つの空きIPアドレスが必要です。1つはロードバランサ用の空きIPアドレス、もう1つはKubernetesコントロールプレーン用の空きIPアドレス、もう1つはノード用のIPアドレスです。HA環境では、これら3つのIPアドレスとともに、2番目と3番目のノード用にさらに2つのIPアドレスが必要になります。ホスト名は、割り当てる前にDNSの空きIPアドレスにマッピングする必要があります。5つのIPアドレスはすべて、導入用に選択したVLAN上にある必要があります。
9. アップロードしたコンテンツライブラリテンプレートは、再起動時に使用されるため、展開後に削除しないでください。
10. vCenterが複数ある環境でカスタムCA証明書が必須である場合は、証明書を発行するドメイン名を仮想IPアドレスにマッピングします。ドメイン名に対して`_nslookup_check`を実行して、ドメインが目的の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、ロードバランサのIPアドレスのドメイン名とIPアドレスを使用して作成する必要があります。
11. IPv4/IPv6対応VLAN -ピュアIPv6はサポートされていません。mixedモードは、IPv6とIPv4の両方のアドレスを持つVLANでサポートされます。
12. 時刻の同期用にvCenter Serverに提供されるNTPサーバ。
13. 静的IPアドレスOVAを導入するノードまたはVMの設定の詳細 (必須) およびその他の詳細。
 - a. vCenter Serverのホスト名 (OVAが導入されているvCenter)

- b. vCenter Serverのユーザ名（OVAが導入されているvCenter）
 - c. vCenter Serverのパスワード（OVAが導入されているvCenter）
 - d. リソースプール
 - e. データLIF（IPv4 / IPv6）
 - f. 管理LIF
 - g. ONTAPユーザ名
 - h. ONTAPパスワード
 - i. SVM名
 - j. プロトコル
 - k. Kubernetesコントロールプレーンの仮想IPアドレス。
 - l. [HA/non-HA]ドロップダウン
 - m. ホスト名のリスト
 - n. IPアドレス（文字列）
 - o. コンテンツライブラリ名
 - p. OVFテンプレート名
 - q. IPv6ゲートウェイ（オプション）
14. 非HAの高度なHA構成およびHA構成でONTAP Tools for VMware vSphere 10.1をインストールする前に、技術情報アーティクル：を確認してください "[HAイカインコウシントHAコウセイノシヨウケン](#)"。

非HAシングルノード構成の導入

非HAのシングルノード構成は、小規模または中規模構成に導入できます。

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

ネットワークルートが存在することを確認します。ストレージデータネットワークにVM管理ネットワークからアクセスする必要があります。例：c1_sti67 -vsim -ucs154k_1679633108：：：> network route create -vserver <SVM>-destination 0.0.0.0/0 -gateway <gateway_ip>

- 手順 *

1. vSphereサーバにログインします。
2. OVAを導入するリソースプール、クラスタ、またはホストに移動します。
3. 目的の場所を右クリックし、*[Deploy OVF template...]*を選択します。



管理対象のVVOLデータストアには、ONTAP tools VMware vSphere仮想マシンを導入しないでください。

4. .ova_fileのURLを入力するか、または.ova_fileが保存されているフォルダを参照して、*[Next]*を選択

します。

5. 仮想マシンの名前とフォルダを選択し、*[Next]*を選択します。
6. ホストを選択して*[次へ]*を選択します。
7. テンプレートの概要を確認し、* Next *を選択します。
8. ライセンス契約を読んで同意し、* Next *を選択します。
9. * Configuration ウィンドウで Easy deployment (S) 、 Easy deployment (M) 、 Advanced deployment (S) または Advanced deployment (M) * configurationを選択します。

高度な導入オプションでは、ONTAPでボリュームを作成するための動的ストレージプロビジョニングツールとしてTridentを使用し、簡単な導入ではローカルストレージを使用してボリュームを作成します。

10. OVAを導入するデータストアを選択し、*[次へ]*を選択します。
11. ソースとデスティネーションのネットワークを選択し、*[次へ]*を選択します。
12. >[システム構成]*ウィンドウを選択します。

System Configuration	8 settings
Application username(*)	Username to assign to the Application
Application password(*)	Password to assign to the Application Password Enter a password to enable authentication. Confirm Password
Enable ASUP	Select this checkbox to enable ASUP ☒
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only 'a', ' ', '.', '!', '!' special characters are supported
Administrator password(*)	Password to assign to the Administrator Password Enter a password to enable authentication. Confirm Password
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
Maintenance user password(*)	Password to assign to maint user account Password Enter a password to enable authentication. Confirm Password

次の詳細を入力します。アプリケーションのユーザ名とパスワード：このユーザ名とパスワードは、VASA ProviderとSRAの両方をvCenter Serverに登録するときに使用します。..[Enable ASUP]*チェックボックスはデフォルトで選択されています。

AutoSupportを有効または無効にできるのは導入時のみです。..フィールドに、**AutoSupport**データ転送用のファイアウォールブロックを回避するためにこの**URL**を指定します。..管理者のユーザー名と管理者のパスワード：**ONTAP**ツールマネージャへのログインに使用するパスワードです。..[NTP Servers]フィールドに**NTP**サーバ情報を入力します。..メンテナンスユーザのパスワード：「メンテナンスコンソールオプション」へのアクセスを許可するために使用します。です。**[Customize template]>*Deployment Configuration ***ウィンドウで、次の詳細情報を入力します。

Load balancer IP(*)	Load balancer IP (*) eg: 10.0.0.1
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane eg: 10.0.0.1
Enable SVM scoping	Ignore when cluster scoping is required ☐
Protocol	Internet Small Computer Systems Interface (iSCSI)/Network File System (NFS) NFS
ONTAP/SVM management LIF(*)	Specify the management LIF for trident eg: 172.17.0
ONTAP/SVM data LIF(*)	Specify the data LIF for trident. IPv6gateway field is mandatory if you provide IPv6 address here. Ignored when SVM scoping
ONTAP/SVM username(*)	Specify the ONTAP cluster username eg: username
ONTAP/SVM password(*)	Specify the ONTAP cluster password Password: Confirm Password:
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. ☒

1. Kubernetesコントロールプレーンの[Virtual IP address]に、使用可能なIPアドレスを入力します。これはKubernetes APIサーバに必要です。
2. 直接追加したSVMユーザアカウントを使用する場合は、*[SVMスコープを有効にする]*オプションを選択します。ONTAPクラスタを使用する場合は、このチェックボックスをオフにします。



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

3. [プロトコル]*フィールドでNFSまたはiSCSIを選択します。
4. [ONTAP / SVM管理LIF]フィールドに、ONTAPクラスタまたはSVM管理IPアドレスを入力します。
5. ONTAPクラスタまたはSVM ONTAP/SVMデータLIFを入力します。データLIFは選択したプロトコルに属している必要があります。たとえば、iSCSIプロトコルを選択した場合は、iSCSIデータLIFを指定する必要があります。
6. Storage VMについては、ONTAPのデフォルトのStorage VMの詳細を指定するか、新しいStorage VMを作成するかを選択できます。[SVMスコープを有効にする]を選択した場合は、*[Storage VM]*フィールドには値を入力しないでください。このフィールドは無視されます。
7. ONTAP / SVMのユーザ名を入力します。高度な導入またはHA導入の場合にTridentでサービスのデータを格納するボリュームを作成し、ノード障害時にボリュームからデータをリカバリするには、ONTAP / SVMのユーザ名とパスワードが必要です。
8. ONTAP / SVMのパスワードを入力します。
9. プライマリVMはデフォルトで有効になっています。この選択は変更しないでください。
 - a. >[Node Configuration]*ウィンドウで、OVAのネットワークプロパティを入力します。



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

10. ホスト名を入力します。大文字（A～Z）、小文字（a～z）、数字（0～9）、および特殊文字ハイフン（-）で構成されるホスト名のみがサポートされます。デュアルスタックを設定する場合は、IPv6アドレスにマッピングされたホスト名を指定します。
11. ホスト名にマッピングされたIPアドレス（IPv4）を入力します。デュアルスタックの場合は、IPv6アドレスと同じVLAN内の使用可能なIPv4 IPアドレスを指定します。
12. 展開されたネットワーク上のIPv6アドレスは、デュアルストークが必要な場合にのみ入力します。
13. IPv6の場合にのみプレフィックス長を指定してください。
14. 導入したネットワークで使用するサブネットを[ネットマスク（IPv4の場合のみ）]フィールドに指定します。
15. 導入したネットワーク上のゲートウェイを指定します。
16. プライマリDNSサーバのIPアドレスを指定します。
17. セカンダリDNSサーバのIPアドレスを指定します。
18. ホスト名を解決するときに使用する検索ドメイン名を指定します。
19. デュアルスタックが必要な場合にのみ、導入されたネットワーク上のIPv6ゲートウェイを指定します。
 - a. [選択内容の確認]ウィンドウで詳細を確認し、*[終了]*を選択します。

導入タスクが作成されると、進行状況がvSphereタスクバーに表示されます。

- b. タスクが完了したら、VMの電源をオンにします。

インストールが開始されます。インストールの進行状況は、VMのWebコンソールで追跡できます。インストールの一環として、ノード構成が検証されます。OVFフォームの[Customize template]の下のさまざまなセクションで入力された内容が検証されます。不一致がある場合は、修正措置を講じるように求めるダイアログが表示されます。

- c. ダイアログプロンプトで必要な変更を行います。タブボタンを使用してパネルを移動し、* OK *または*キャンセル*の値を入力します。
- d. [OK]*を選択すると、指定した値が再度検証されます。ONTAP Tools for VMwareでは、無効な値の修正を3回試行できます。3回試行しても問題を修正できない場合は、製品のインストールが停止し、新しいVMでインストールを試すことを推奨します。
- e. インストールが完了すると、WebコンソールにONTAP tools for VMware vSphereの状態が表示されます。

HA構成を導入する

HA 3ノードは、小規模、中規模、大規模のいずれかの構成で構成できます。HA環境では、Tridentを使用してサービスデータを格納します。

- 小規模なHA 3ノードには、ノードあたり8個のCPUと16GBのRAMが搭載されています。
- 中規模HA 3つのノードには、ノードあたり12個のCPUと24GBのRAMが搭載されています。

- 大規模なHA 3ノードには、ノードあたり16個のCPUと32GBのRAMが搭載されています。
- 始める前に *

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



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

OVAがコンテンツライブラリにインポートされていることを確認します。コンテンツライブラリの名前と、OVAアイテムに付けたライブラリアイテムの名前を手元に置いておきます。



導入を進める前に、ONTAPツールのインストール中に、インベントリ上のクラスターのDistributed Resource Scheduler (DRS) を「保守的」に設定してください。これにより、インストール中にVMが移行されなくなります。

• 手順 *

1. vSphereサーバから導入する手順は次のとおりです。

- a. vSphereサーバにログインします。
- b. OVAを導入するリソースプールまたはホストに移動し、VMの導入先を右クリックして*[Deploy OVF template...]*を選択します。



管理対象のVVOLデータストアには、ONTAP tools VMware vSphere仮想マシンを導入しないでください。

- c. `.ova_file`のURLを入力するか、または`.ova_file`が保存されているフォルダを参照して、*[Next]*を選択します。

2. コンテンツライブラリから配備するには'次の手順に従います

- a. コンテンツライブラリに移動し、展開するライブラリアイテムをクリックします。
- b. >[New VM from this Template]*をクリックします。

3. 仮想マシンの名前とフォルダを選択し、*[Next]*を選択します。

4. ホストを選択して*[次へ]*を選択します。

5. テンプレートの概要を確認し、* Next *を選択します。

6. ライセンス契約を読んで同意し、* Next *を選択します。

7. [Configuration]ウィンドウ*で、要件に応じて*、[High-Availability Deployment (M)]、または[High-Availability Deployment (L)]*構成を選択します。

8. 構成ファイルとディスクファイルのストレージを選択し、* Next *を選択します。

9. 各ソースネットワークのデスティネーションネットワークを選択し、*[Next]*を選択します。

10. >[システム構成]*ウィンドウを選択します。

System Configuration		8 settings
Application username(*)	Username to assign to the Application ⓘ	
Application password(*)	Password to assign to the Application Password ⓘ ⓘ Enter a password to enable authentication. Confirm Password ⓘ	
Enable ASUP	Select this checkbox to enable ASUP ☒	
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle. 	
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '.', '-', '_', '!', '!' special characters are supported ⓘ	
Administrator password(*)	Password to assign to the Administrator Password ⓘ ⓘ Enter a password to enable authentication. Confirm Password ⓘ	
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 	
Maintenance user password(*)	Password to assign to maint user account Password ⓘ ⓘ Enter a password to enable authentication. Confirm Password ⓘ	

次の詳細を入力します。

- a. アプリケーションのユーザ名とパスワード：このユーザ名とパスワードは、VASA ProviderとSRAの両方をvCenter Serverに登録するとき使用します。
 - b. AutoSupportを有効にする*チェックボックスはデフォルトで選択されています。AutoSupportを有効または無効にできるのは導入時のみです。
 - c. [ASUPプロキシURL]*フィールドに、AutoSupportデータ転送用のファイアウォールブロックを回避するためにこのURLを指定します。
 - d. 管理者のユーザー名と管理者のパスワード：ONTAP tools Managerへのログインに使用するパスワードです。
 - e. [NTP Servers]フィールドにNTPサーバ情報を入力します。
 - f. メンテナンスユーザのパスワード：「メンテナンスコンソールオプション」へのアクセスを許可するために使用します。
11. [Customize template]*>[Deployment Configuration *]ウィンドウで、次の詳細情報を入力します。

Load balancer IP(*)	Load balancer IP (*) eg: 10.0.0.1
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane eg: 10.0.0.1
Enable SVM scoping	Ignore when cluster scoping is required ☐
Protocol	Internet Small Computer Systems Interface (iSCSI)/Network File System (NFS) NFS ▾
ONTAP/SVM management LIF(*)	Specify the management LIF for trident eg: 172.17.0
ONTAP/SVM data LIF(*)	Specify the data LIF for trident. IPv6gateway field is mandatory if you provide IPv6 address here. Ignored when SVM scoping is enabled
ONTAP/SVM username(*)	Specify the ONTAP cluster username eg: username
ONTAP/SVM password(*)	Specify the ONTAP cluster password Password: Confirm Password:
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. ☒

- a. Kubernetesコントロールプレーンの[Virtual IP address]に、使用可能なIPアドレスを入力します。これはKubernetes APIサーバに必要です。
- b. 直接追加したSVMユーザアカウントを使用する場合は、高度な導入オプションで*[SVMスコープを有効にする]*オプションを選択します。ONTAPクラスタを使用する場合は、このチェックボックスをオフにします。



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

- c. [プロトコル]*フィールドでNFSまたはiSCSIを選択します。
 - d. [ONTAP / SVM管理LIF]フィールドに、ONTAPクラスタまたはSVM管理IPアドレスを入力します。
 - e. ONTAPクラスタまたはSVM ONTAP/SVMデータLIFを入力します。データLIFは選択したプロトコルに属している必要があります。たとえば、iSCSIプロトコルを選択した場合は、iSCSIデータLIFを指定する必要があります。
 - f. Storage VMについては、ONTAPのデフォルトのStorage VMの詳細を指定するか、新しいStorage VMを作成するかを選択できます。[SVMスコープを有効にする]を選択した場合は、*[Storage VM]*フィールドには値を入力しないでください。このフィールドは無視されます。
 - g. ONTAP / SVMのユーザ名を入力します。高度な導入またはHA導入の場合にTridentでサービスのデータを格納するボリュームを作成し、ノード障害時にボリュームからデータをリカバリするには、ONTAP / SVMのユーザ名とパスワードが必要です。
 - h. ONTAP / SVMのパスワードを入力します。
 - i. プライマリVMはデフォルトで有効になっています。この選択は変更しないでください。
12. テンプレートのカスタマイズ>*コンテンツライブラリの詳細*ウィンドウで、コンテンツライブラリ名*と OVFテンプレート名*を入力します。
 13. [テンプレートのカスタマイズ]>[vCenter構成]*ウィンドウで、コンテンツライブラリがホストされているvCenter Serverの詳細を入力します。

14. [テンプレートのカスタマイズ]>[ノード構成]ウィンドウで、3つすべてのノードのOVAのネットワークプロパティを入力します。



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

- a. ホスト名を入力します。大文字（A～Z）、小文字（a～z）、数字（0～9）、および特殊文字ハイフン（-）で構成されるホスト名のみがサポートされます。デュアルスタックを設定する場合は、IPv6アドレスにマッピングされたホスト名を指定します。
 - b. ホスト名にマッピングされたIPアドレス（IPv4）を入力します。デュアルスタックの場合は、IPv6アドレスと同じVLAN内の使用可能なIPv4 IPアドレスを指定します。
 - c. デュアルスタックが必要な場合にのみ、導入されたネットワーク上のIPv6アドレスを入力します。
 - d. IPv6の場合にのみプレフィックス長を指定してください。
 - e. 導入したネットワークで使用するサブネットを[ネットマスク（IPv4の場合のみ）]フィールドに指定します。
 - f. 導入したネットワーク上のゲートウェイを指定します。
 - g. プライマリDNSサーバのIPアドレスを指定します。
 - h. セカンダリDNSサーバのIPアドレスを指定します。
 - i. ホスト名を解決するときに使用する検索ドメイン名を指定します。
 - j. デュアルスタックが必要な場合にのみ、導入されたネットワーク上のIPv6ゲートウェイを指定します。
15. [テンプレートのカスタマイズ（Customize template）]>[ノード2の構成（Node 2 Configuration）]および[ノード3の構成（Node 3 Configuration）]ウィンドウで、次の詳細を入力します。
- a. ホスト名2および3 -大文字（A_Z）、小文字（a_z）、数字（0～9）、およびハイフン（-）特殊文字で構成されるホスト名のみがサポートされます。デュアルスタックを設定する場合は、IPv6アドレスにマッピングされたホスト名を指定します。
 - b. IPアドレス
 - c. IPv6アドレス
16. [選択内容の確認]ウィンドウで詳細を確認し、*[終了]*を選択します。
- 導入タスクが作成されると、進行状況がvSphereタスクバーに表示されます。
17. タスクが完了したら、VMの電源をオンにします。
- インストールが開始されます。インストールの進行状況は、VMのWebコンソールで追跡できます。インストールの一環として、ノード構成が検証されます。OVFフォームの[Customize template]の下のさまざまなセクションで入力された内容が検証されます。不一致がある場合は、修正措置を講じるように求めるダイアログが表示されます。
18. ダイアログプロンプトで必要な変更を行います。タブボタンを使用してパネルを移動し、* OK *または*キャンセル*の値を入力します。
19. [OK]*を選択すると、指定した値が再度検証されます。ONTAP Tools for VMwareでは、無効な値の修正を3回試行できます。3回試行しても問題を修正できない場合は、製品のインストールが停止し、新

しいVMでインストールを試すことを推奨します。

20. インストールが完了すると、WebコンソールにONTAP tools for VMware vSphereの状態が表示されます。

ONTAP Tools for VMware vSphereセットアップのリカバリ

ONTAP tools for VMware vSphereのセットアップを失った場合は、ONTAPボリュームのデータに含まれているデータを使用してONTAP tools for VMware vSphereのセットアップをリカバリできます。セットアップが失われたら、セットアップを正常に停止してください。



vCenter ServerまたはONTAPデータ管理ソフトウェアで問題があると、ONTAP tools for VMware vSphereのセットアップをリカバリできません。

• 手順 *

1. vSphereサーバにログインします。
2. OVAを導入するリソースプール、ノードクラス、またはホストに移動します。
3. 目的の場所を右クリックし、*[Deploy OVF Template]*を選択します。
4. .ova_fileのURLを入力するか、または.ova_fileが保存されているフォルダを参照して、*[Next]*を選択します。



リカバリセットアップのインストールに使用したのと同じOVAビルドを使用する必要があります。

5. 仮想マシンの名前とフォルダを選択し、*[Next]*を選択します。
6. ホストを選択し、*[次へ]*を選択します。
7. テンプレートの概要を確認し、* Next *を選択します。
8. ライセンス契約を読んで同意し、* Next *を選択します。
9. [設定]ウィンドウで、*[リカバリ]*オプションを選択します。
10. [ストレージの選択]ウィンドウで、構成ファイルとディスクファイルのストレージを選択します。
11. [ネットワークの選択]ウィンドウで、各ソースネットワークの宛先ネットワークを選択します。



ロードバランサのIPアドレスとKubernetes APIサーバのIPアドレスは保持する必要があります。ノードのIPアドレスを変更することも、同じIPアドレスを維持することもできます。

12. >[システム構成]ウィンドウを選択します。次の詳細を入力します。
 - a. アプリケーションのユーザ名とパスワード：このユーザ名とパスワードは、VASA ProviderとSRAの両方をvCenter Serverに登録するときに使用します。初期導入時に指定したユーザ名とパスワードとは異なる場合があります。
 - b. [Enable ASUP]*チェックボックスはデフォルトで選択されています。

AutoSupportを有効または無効にできるのは導入時のみです。..フィールドに、**AutoSupport**データ転送用の

ファイアウォールブロックを回避するためにこのURLを指定します。..管理者のユーザー名と管理者のパスワード：**ONTAP**ツールマネージャへのログインに使用するパスワードです。初期導入時に指定したユーザ名とパスワードとは異なる場合があります。..**[NTP Servers]**フィールドに**NTP**サーバ情報を入力します。..**maintenance user password**：メンテナンスコンソールのオプションへのアクセスを許可する場合に使用します。です。**[テンプレートのカスタマイズ]>[展開構成]***ウィンドウで、展開時に指定した詳細を入力します。このセクションの値は、データLIFの値を除き、初期導入時に指定した値と同じにする必要があります。



リカバリデータが格納されるストレージSVM名は変更しないでください。この環境によってSVMユーザアカウントも直接追加されました。です。HA導入のリカバリの場合は、次の詳細を指定します。コンテンツライブラリの詳細。.. vCenter構成の詳細です。>**[Node Configuration]**ウィンドウで、リカバリしようとしているセットアップ（非**HA**または**HA**のセットアップ）に従って詳細を入力します。です。**[選択内容の確認]**ウィンドウで詳細を確認し、**[終了]***を選択します。

+導入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。です。タスクが完了したら、VMの電源をオンにします。

+インストールが開始されます。インストールの進行状況は、VMのWebコンソールで追跡できます。インストールの一環として、ノード構成が検証されます。OVFフォームの**[Customize template]**の下のさまざまなセクションで入力された内容が検証されます。不一致がある場合は、修正措置を講じるように求めるダイアログが表示されます。です。ダイアログプロンプトで必要な変更を行います。タブボタンを使用してパネルを移動し、* **OK** *または* **キャンセル** *の値を入力します。です。**[OK]***または**[キャンセル]***を選択すると、指定した値が再度検証されます。ONTAP Tools for VMwareでは、無効な値の修正を3回試行できます。3回試行しても問題を修正できない場合は、製品のインストールが停止し、新しいVMでインストールを試すことを推奨します。です。インストールが完了すると、WebコンソールにONTAP tools for VMware vSphereの状態が表示されます。インストールが完了したら、ページのガイドラインに従ってハードウェア要件を手動で編集する必要があります **"ONTAP Tools for VMware vSphereを導入するための前提条件"**。

導入エラーコード

ONTAP tools for VMware vSphereの導入、リブート、およびリカバリの処理中にエラーコードが発生することがあります。エラーコードは5桁で、最初の2桁は問題に遭遇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。

問題の追跡と解決を容易にするために、すべてのエラーログが**ansible-perl-errors.log**ファイルに記録されます。このログファイルには、エラーコードと失敗したAnsibleタスクが記録されます。



このページに記載されているエラーコードは参照用です。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、モードアップグレード
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl、導入、HA

04	firstboot-deploy-otv-ng.pl、デプロイ、非HA
05	firstboot-deploy-otv-ng.pl、リブート
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

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。

展開エラーコード	* ワークフロー *	解像度
050	SSHキーを生成できませんでした	プライマリ仮想マシン（VM）を再起動します。
051	セカンダリVMを導入できませんでした	* 2つ目と3つ目のVMが作成されている場合は、セカンダリVMの電源をオンにしてプライマリVMを再起動する前に、十分なCPU / メモリリソースが使用可能であることを確認してください。* 2台目と3台目のVMがONTAP tools for VMware vSphereテンプレートの導入タスクに含まれている場合は、タスクが完了するまで待ち、VMの電源をオンにしてプライマリVMをリブートします。*再展開。
052	SSHキーのコピーに失敗しました	プライマリ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、再導入します。sudo rke2-killall.sh（すべてのVM）sudo rke2-uninstall.sh（すべてのVM）。
054	kubeconfigを設定できませんでした	再導入
055	レジストリのデプロイに失敗	レジストリポッドが存在する場合は、ポッドの準備が完了するまで待つから、プライマリVMを再起動するか、再導入します。
056	ログインiSCSIに失敗しました	ONTAPでiSCSIプロトコルが有効になっていて、正しく設定されていることを確認します。指定したiSCSIデータLIFのIPアドレスが正しいオンラインであることを確認します。以前のポイントが正しい場合は、VMを再起動します。それ以外の場合は再導入します。

057	Tridentの導入に失敗しました	管理LIFおよびデータLIFのIPアドレスにVMから到達できることを確認してください。ONTAPでNFSまたはiSCSIプロトコルが有効になっており、正しく設定されていることを確認します。*指定したNFS / iSCSIデータLIFのIPアドレスが正しいオンラインであることを確認します。*指定したユーザ名とパスワードが正しいこと、およびボリュームを作成するための十分な権限がユーザにあることを確認してください。*上記のすべての点が正しい場合は、再起動してください。それ以外の場合は再導入します。
058	Tridentのインポートに失敗しました	*指定したユーザ名とパスワードが正しいこと、およびボリュームを作成、マウント、クローニング、および削除するための十分な権限がユーザにあることを確認してください。*セットアップをリカバリし、リカバリを再試行するために同じONTAPセットアップが使用されていることを確認してください。
059	KubeVipの導入に失敗しました	導入時に指定したKubernetesコントロールプレーンの仮想IPアドレスとロードバランサのIPアドレスが同じVLANに属し、空いているIPアドレスであることを確認します。前のすべてのポイントが正しい場合は、再起動します。それ以外の場合は再導入します。
060	オペレータの配備に失敗しました	リスタート
061	サービスの導入に失敗しました	詳細とエラーログについては、/var/log/ ansible-perl-errors.log および/var/log/ ansible-run.log で、ntv-system名前空間でGETポッド、GET RS、GET svcなどの基本的なKubernetesデバッグを実行し、再導入します。
062	VASA ProviderとSRAの導入に失敗しました	詳細と再導入については、/var/log/ ansible-perl-errors.logにあるエラーログを参照してください。
064	version.xml検証に失敗しました	再導入
065	SwaggerページのURLにアクセスできません	再導入
066	導入後の手順が失敗しました	-

088	journaldのログローテーションの設定に失敗しました	プライマリVMを再起動します。
089	サマリーログのrotate構成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。

再起動エラーコード	* ワークフロー *	
067	rke2サーバがタイムアウトするのを待機しています	
101	保守/コンソールユーザーパスワードのリセットに失敗しました	
102	保守/コンソール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	ボルトの新しい保守/コンソールユーザーパスワードの更新に失敗しました	

リカバリエラーコード	* ワークフロー *	解像度
104	リカバリ後の手順に失敗しました。	-
105	リカバリボリュームへのコンテンツのコピーに失敗しました。	-
106	リカバリボリュームをマウントできませんでした。	同じ SVM を使用し、リカバリボリュームが SVM に存在することを確認します。（リカバリボリューム名が otvng_lif_recovery で始まる）*管理 Trident およびデータの IP アドレスに VM から到達できることを確認してください。ONTAPでNFS/iSCSIプロトコルが有効になっており、正しく設定されていることを確認します。*指定したNFS/iSCSI DAT LIFのIPアドレスが正しいオンラインであることを確認します。*指定したユーザ名、パスワード、プロトコルが正しいこと、および作成、マウント、クローニング、削除を行うための十分な権限がユーザにあることを確認してください。*リカバリを再試行してください

ONTAPツールの設定

ONTAP tools Managerユーザインターフェイス

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 tools Managerを使用すると、管理対象のvCenter Serverインスタンスとオンボードストレージバックエンドを使用して、VMware vSphere管理者向けのONTAP toolsをより細かく制御できます。

ONTAP Tools Managerは、次のことを支援します。

- vCenter Serverインスタンス管理- vCenter ServerインスタンスをONTAPツールに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をONTAP tools for VMware vSphereに追加および管理し、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、すべての証明書を更新または更新します。
- パスワード管理- OVAアプリケーションのユーザパスワードをリセットします。

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

vCenter Serverインスタンスの追加と管理

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

vCenter Serverインスタンスを追加する

- このタスクについて *

ONTAP tools for VMware vSphereの1つのインスタンスを使用して、複数のvCenter Serverインスタンスを追加および管理できます。

- 手順 *
- 1. WebブラウザからONTAP Tools Managerを起動します。
<https://loadBalanceIP:8443/virtualization/ui/>
- 2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
- 3. サイドバーから* vCenters *を選択します。
- 4. vCenter Serverインスタンスをオンボードするには*[追加]*を選択し、vCenterのIPアドレス/ホスト名、ユーザ名、パスワード、およびポートの詳細を指定します。

vCenter ServerインスタンスをONTAP toolsに追加すると、次の処理が自動的に実行されます。

- vCenter Client Plug-inが登録されている
- プラグインとAPIのカスタム権限がvCenter Serverインスタンスにプッシュされる
- ユーザを管理するためのカスタムロールが作成されます。

ONTAP Tools for VMware vSphereプラグインをvCenter Serverインスタンスに登録

vCenter Serverインスタンスを追加すると、ONTAP tools for VMware vSphereプラグインがリモートプラグインとしてvCenter Serverに自動的に登録されます。プラグインは、vSphereユーザインターフェイスのショートカットに表示されます。

プラグインは、vCenter Serverインスタンスへのキー_com.netapp.otv_で登録され、vCenter ServerインスタンスのExtensionManagerで確認できます。

ONTAP Tools for VMware vSphereプラグインの登録解除

vCenter ServerインスタンスからONTAP tools for VMware vSphere Plug-inの登録を解除するには、次の手順を実行します。

- 手順 *
 1. WebブラウザからONTAP Tools Managerを起動します。
<https://loadBalanceIP:8443/virtualization/ui/>
 2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
 3. サイドバーから[vCenters]を選択します。
 4. 削除するvCenterの縦の省略記号をクリックし、*[削除]*オプションを選択します。



ストレージマッピングが接続されているvCenter Serverインスタンスは削除できません。vCenter Serverインスタンスを削除する前に、マッピングを削除する必要があります。

ONTAP toolsでvCenter Serverインスタンスを削除すると、次の処理が自動的に実行されます。

- プラグインの登録が解除されました。
- プラグイン権限とプラグインロールが削除されました。

VASA ProviderをvCenter Serverインスタンスに登録する

ONTAP tools for VMware vSphereリモートプラグインインターフェイスを使用して、vCenter ServerインスタンスへのVASA Providerの登録と登録解除を行うことができます。[VASA Provider Settings]セクションには、選択したvCenter ServerのVASA Providerの登録状態が表示されます。

- 手順 *
 1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
 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 tools *をクリックします。

3. >[VASA Provider settings]*を選択します。VASA Providerの登録状態がNot Registeredと表示される。
4. [登録]*ボタンをクリックしてVASA Providerを登録します。
5. VASA Providerの名前を入力し、ONTAP tools for VMware vSphereアプリケーションのユーザクレデンシャルを指定して、*[登録]*をクリックします。
6. 登録が完了してページが更新されると、登録されているVASA Providerの状態、名前、バージョンがUIに表示されます。登録解除アクションがアクティブになります。
7. VASA Providerの登録を解除するには、次の手順を実行します。
 - a. VASA Providerの登録を解除するには、画面下部の*[登録解除]*オプションを選択します。
 - b. ページでは、**VASA Provider**の名前を確認できます。このページで、アプリケーションのユーザクレデンシャルを入力し、[登録解除]*をクリックします。

登録された**VASA**プロバイダを確認

オンボードしたVASA Providerが、vCenter Client UIおよびリモートプラグインUIの[VASA Provider]の下に表示されていることを確認します。

• 手順 *

1. vCenter Client UIからVASA Providerを確認するには、次の手順を実行します。
 - a. vCenter Serverに移動します。
 - b. 管理者のクレデンシャルでログインします。
 - c. [ストレージプロバイダ]*を選択します。
 - d. 「* Configure *」を選択します。
 - e. [Storage Provider/storage backends]で、オンボードしたVASAプロバイダが正しく表示されていることを確認します。
2. リモートプラグインUIからVASA Providerを確認するには、次の手順を実行します。
 - a. 次のコマンドを使用してvSphere Clientにログインします。 `https://vcenterip/ui`
 - b. ショートカットページで、プラグインセクションの* NetApp ONTAP tools *をクリックします。
 - c. 登録されているVASA Providerは、概要ページと*>[VASA Provider設定]*ページで確認できます。

NFS VAAIプラグインをインストールする

ONTAP tools for VMware vSphereを使用して、NetApp NFS Plug-in for VMware vStorage APIs for Array Integration (VAAI) をインストールできます。

• 必要なもの *

- (.vib) NetAppサポートサイトからNFS Plug-in for VAAIのインストールパッケージをダウンロードしておく必要があります。 "[NetApp NFS Plug-in for VMware VAAI](#)"
- ESXiホスト7.0U3の最新パッチを最小バージョンとしてインストールし、ONTAP 9.12.1Px（最新のリリース）9.13.1Px、9.14.1Px以降をインストールしておく必要があります。
- ESXiホストの電源をオンにし、NFSデータストアをマウントしておく必要があります。

- `DataMover.HardwareAcceleratedMove`、`DataMover.HardwareAcceleratedInit`、および `VMFS3.HardwareAcceleratedLocking` ホスト設定の値を「1」に設定しておく必要があります。

これらの値は、[推奨設定]ダイアログボックスを更新するとESXiホストに自動的に設定されます。

- ``vserver nfs modify -vserver vserver_name -vstorage enabled`` コマンドを使用して、Storage Virtual Machine (SVM) でvstorageオプションを有効にしておく必要があります。
- NetApp NFS VAAI Plug-in 2.0を使用している場合は、ESXi 7.0U3以降が必要です。
- vSphere 6.5が廃止されたため、vSphere 7.0U3の最新のパッチリリースが必要です。
- vSphere 8.xは、NetApp NFS VAAIプラグイン2.0.1（ビルド16）でサポートされます。
- 手順 *
 1. ONTAP tools for VMware vSphereのホームページで*[設定]*をクリックします。
 2. NFS VAAI ツール * タブをクリックします。
 3. VAAIプラグインをvCenter Serverにアップロードしたら、* Existing version セクションで Change 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。
 4. `.vib`` ファイルを参照して選択し、*[アップロード]*をクリックしてONTAP toolsにファイルをアップロードします。
 5. をクリックし、**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]*をクリックします。

プラグインのインストールに対応するESXiホストのみが表示されます。画面に表示される手順に従ってインストールを完了する必要があります。インストールの進捗状況は、vSphere Web Client の[Recent Tasks]セクションで監視できます。

6. インストールが完了したら、ESXiホストを手動でリブートする必要があります。

VMware管理者がESXiホストをリブートすると、ONTAP tools for VMware vSphereによってNFS VAAI プラグインが自動的に検出されます。このプラグインを有効にするために追加の手順を実行する必要はありません。

ホストデータの更新

ESXiホストでオンデマンド検出を実行して、ストレージデータの最新の更新を取得できます。

- 手順 *
 1. VMware vSphere Web Clientの[ホーム]ページで、*[ホストおよびクラスター]*をクリックします。
 2. ホストを右クリックし、* NetApp ONTAP tools >[ホストデータの更新]*を選択します。
 3. ポップアップウィンドウで[はい]*を選択して、接続されているすべてのストレージシステムの検出を再開します。

ESXiホストの設定

ESXiサーバのマルチパスとタイムアウトの設定

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 *

構成やシステムの負荷によっては、このプロセスに時間がかかることがあります。タスクの進行状況は、[最近のタスク]パネルに表示されます。タスクが完了すると、ホストのステータスを示す[アラート]アイコンが[正常]アイコンまたは[リブートを保留中]アイコンに変わります。

- 手順 *

1. VMware vSphere Web Clientの[ホーム]ページで、*[ホストおよびクラスター]*をクリックします。
2. ホストを右クリックし、* NetApp ONTAP tools >[ホストデータの更新]*を選択します。
3. ショートカットページで、プラグインセクションの* NetApp ONTAP tools *をクリックします。
4. ONTAP tools for VMware vSphereプラグインの概要（ダッシュボード）で、ESXiホストコンプライアンスカードに移動します。
5. [推奨設定の適用]*リンクを選択します。
6. ウィンドウで、**NetApp**の推奨されるホスト設定に準拠するホストを選択し、[次へ]*をクリックします。



ESXiホストを展開すると、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]*をクリックします。進捗状況は、[最近使用したタスク]パネルで追跡できます。

ESXiホストの値の設定

ONTAP Tools for VMware vSphereを使用してESXiホストでタイムアウトやその他の値を設定することで、最適なパフォーマンスが確保され、フェイルオーバーが正常に実行されるようにすることができます。ONTAP tools for VMware vSphereが設定する値は、社内のNetAppテストに基づいています。

ESXiホストで設定できる値は次のとおりです。

HBA / CNAアダプタ設定

NetAppストレージシステムに推奨されるHBAタイムアウト設定を設定します。

- * Disk.QFullSampleSize *

すべての構成でこの値を32に設定します。この値を設定すると、I/Oエラーを回避できます。

- * Disk.QFullThreshold *

すべての構成でこの値を8に設定します。この値を設定すると、I/Oエラーを回避できます。

- * Emulex FC HBA タイムアウト *

デフォルト値を使用します。

- * QLogic FC HBA タイムアウト *

デフォルト値を使用します。

MPIO設定

MPIO設定では、NetAppストレージシステムの優先パスを定義します。MPIOの設定によって、（インターコネクトケーブルを経由する最適化されていないパスではなく）最適化されたパスが決まり、そのうちの1つに優先パスが設定されます。

ハイパフォーマンス環境や、単一のLUNデータストアでパフォーマンスをテストする場合は、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設定である1000から1に変更することを検討してください。

NFS 設定

- * Net.TcpipHeHeapSize *

この値を32に設定します。

- * Net.TcpipHeapMax *

この値を1,024MBに設定します。

- * NFS.MaxVolumes *

この値を256に設定します。

- * NFS41.MaxVolumes*

この値を256に設定します。

- * NFS.MaxQueueDepth *

キューイングのボトルネックを回避するには、この値を128以上に設定します。

- * nfs.HeartbeatMaxFailures*

すべてのNFS構成で、この値を10に設定します。

- * nfs.HeartbeatFrequency*

すべてのNFS構成で、この値を12に設定します。

- * nfs.HeartbeatTimeout *

すべてのNFS構成で、この値を5に設定します。

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、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がONTAP Toolsによって検出されます。

- 必要なもの *
- すべてのESXiホストの電源をオンにして接続する必要があります。
- 検出対象のすべてのStorage Virtual Machine (SVM) が実行されている必要があり、使用中のストレージプロトコル (NFSまたはiSCSI) 用のデータLIFが各クラスターノードに少なくとも1つ設定されている必要があります。
- 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に関する情報の更新はいつでも実行でき、容量や構成に関する最新の情報を取得できます。ONTAP tools for VMware vSphereでストレージシステムへのログインに使用するクレデンシャルを変更することもできます。

ストレージシステムを検出する際、ONTAP tools for VMware vSphereは、vCenter Serverインスタンスで管理しているESXiホストから情報を収集します。

- 手順 *
- 1. vSphere Clientの[ホーム]ページで、*[ホストおよびクラスター]*を選択します。
- 2. 目的のデータセンターを右クリックし、* NetApp ONTAP tools * > *ホストデータの更新*を選択します。

ONTAP tools for VMware vSphereに*[確認]*ダイアログボックスが表示され、次のメッセージが表示されます。

"この処理は、接続されているすべてのストレージシステムの検出を再開します。これには数分かかることがあります。続行しますか?"

1. 「* はい *」をクリックします。
2. 検出されたステータスのストレージコントローラを選択し Authentication Failure、[操作]>*[変更]*をクリックします。
3. [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
4. `Authentication Failure`ステータスのすべてのストレージコントローラについて、手順4と5を繰り返します。

検出プロセスが完了したら、次の操作を実行します。

- ONTAP tools for VMware vSphereを使用して、[アダプタ設定]、[MPIO設定]、または[NFS設定]列に[アラート]アイコンが表示されているホストのESXiホストを設定します。
- ストレージシステムのクレデンシャルを入力します。

ストレージバックエンドを追加します

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。

- このタスクについて *

このタスクは、ONTAPクラスタをオンボードする際に役立ちます。ONTAP tools Managerを使用してストレージバックエンドを追加すると、ストレージバックエンドがグローバルクラスタに追加されます。グローバルクラスタをvCenter Serverインスタンスに関連付けて、SVMユーザにvVolデータストアのプロビジョニングを許可します。



vSphere Client UIを使用してストレージバックエンドを追加した場合、vVolデータストアでSVMユーザを直接追加することはできません。

ONTAP tools Managerを使用したストレージバックエンドの追加



ストレージバックエンドは、ONTAP tools ManagerまたはONTAP tools APIから追加するとグローバルになります。ストレージバックエンドは、vCenter Server APIから追加したときにローカルになります。たとえば、マルチテナントセットアップでは、SVMユーザクレデンシャルを使用するために、ストレージバックエンド（クラスタ）をグローバルに、SVMをローカルに追加できます。

- 手順 *

1. WebブラウザからONTAP Tools Managerを起動します。
<https://loadBalanceIP:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーから* Storage backends *を選択します。
4. 「* 追加」を選択します。
5. サーバのIPアドレスまたはFQDN、ユーザ名、パスワードを入力し、*[追加]*を選択します。



IPv4とIPv6の管理LIFがサポートされます。管理LIFを使用するSVMユーザベースのクレデンシャルもサポートされます。

vSphere Client UIを使用してストレージバックエンドを追加します。

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
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 tools *をクリックします。
3. ONTAP toolsの左側のペインで、[ストレージバックエンド]*に移動し、[追加]*を選択します。
4. ウィンドウで、サーバのIPアドレス、ユーザ名、パスワード、およびポートの詳細を指定し、[追加]*をクリックします。



クラスタベースのクレデンシャルとIPv4およびIPv6の管理LIFを追加するか、SVMの管理LIFにSVMベースのクレデンシャルを指定して、SVMユーザを直接追加できます。

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とvCenter Serverインスタンスの関連付け

vCenter Serverのリストページには、関連す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を関連付けるオプションがあります。

- このタスクについて *

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

- 手順 *

1. WebブラウザからONTAP Tools Managerを起動します。
`https://loadBalanceIP:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャル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の縦の省略記号をクリックします。
5. ポップアップのドロップダウンからストレージバックエンドを選択します。
6. vCenter Serverインスタンスを必要なストレージバックエンドに関連付けるには、*[ストレージバックエンドの関連付け]*オプションを選択します。

ネットワークアクセスの設定

ESXiホストのIPアドレスが複数ある場合は、ホストで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。すべてのIPアドレスをエクスポートポリシーに追加しない場合は、各vCenterに対して特定のIPアドレスをカンマで区切ったリスト、範囲、CIDR、またはこれら3つの組み合わせを許可する設定を指定します。

データストアのマウント処理で特定のESXiホストアドレスをいくつか許可するように選択できます。設定を指定しない場合は、マウント前の手順で検出したすべてのIPアドレスがエクスポートポリシーによって追加されます。この設定を指定すると、ONTAP tools for VMware vSphereは、表示されたIPアドレスまたは範囲内のIPアドレスのみを追加します。リストされているIPアドレスに属するホストのIPアドレスがない場合、そのホストでのマウントは失敗します。

手順

1. 次のコマンドを使用してvSphere Clientにログインします。 `https://vcenterip/ui`
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 tools *をクリックします。
3. ONTAPツールの左側のペインで、[設定]>*>[編集]*に移動します。

IPアドレスを区切るには、カンマ (,) を使用します。特定のIPアドレス、またはIPアドレスの範囲またはIPv6アドレスを指定できます。

4. [保存 (Save)] をクリックします。

ONTAPユーザのロールと権限の設定

ストレージバックエンドの管理に使用する新しいユーザロールと権限を設定するには、ONTAP tools for VMware vSphereおよびONTAP System Managerに付属のJSONファイルを使用します。

- 必要なもの *
- ONTAP PrivilegesファイルをONTAP tools for VMware vSphereから、`_ \ https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`を使用してダウンロードしておく必要があります。
- を使用して、ONTAP toolsからONTAP Privilegesファイルをダウンロードしておく必要があります
`https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`



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

- ストレージバックエンドの管理者権限でログインしている必要があります。
- 手順 *
- 1. ダウンロードした `_ \ https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip` を展開します。
- 2. 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。
- 3. クラスタまたはSVMのユーザとしてログインします。
- 4. >[設定]>[ユーザとロール]*ペインを選択します。
- 5. [Users]で[Add]*を選択します。
- 6. [ユーザーの追加*]ダイアログボックスで、[仮想化製品*]を選択します。
- 7. *参照*をクリックして、ONTAP Privileges JSONファイルを選択してアップロードします。

[Product]フィールドには自動的に値が入力されます。

8. 製品機能ドロップダウンメニューから必要な機能を選択します。

[ロール]*フィールドには、選択した製品機能に基づいて自動的に値が入力されます。

9. 必要なユーザ名とパスワードを入力します。
10. ユーザに必要な権限 ([Discovery]、[Create Storage]、[Modify Storage]、[Destroy Storage]、[NAS/SAN Role]) を選択し、*[Add]*をクリックします。

新しいロールとユーザが追加され、設定したロールの詳細な権限が表示されます。



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

SVMアグリゲートのマッピングの要件

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

REST API :

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

ONTAP CLI :

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

ONTAPのユーザとロールを手動で作成する

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

1. 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. クラスタまたはSVMのユーザとしてログインします。
3. >[設定]>[ユーザとロール]*ペインを選択します。
4. ロールの作成 :
 - a. テーブルの[追加]*を選択します。
 - b. [ロール名]*および[ロール属性]*の詳細を入力します。
 [REST API Path]*と該当するアクセスをドロップダウンから追加します。
 - c. 必要なAPIをすべて追加し、変更を保存します。
5. ユーザの作成 :
 - a. Users テーブルの Add *を選択します。

- b. [ユーザの追加]ダイアログボックスで、*[System Manager]*を選択します。
- c. [Username]*を入力します。
- d. 上記の*ロールの作成*ステップで作成したオプションから*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。ONTAPIとHTTPが必要なアプリケーションで、認証タイプは* Password *です。
- f. ユーザーの*パスワード*とユーザーの*保存*を設定します。

管理者以外のグローバルを対象としたクラスタユーザに必要な最小権限のリスト

このセクションには、users JSONファイルを使用せずに作成した管理者以外のグローバル対象のクラスタユーザに必要な最小権限を記載します。クラスタをローカルスコープで追加する場合は、JSONファイルを使用してユーザを作成することを推奨します。ONTAP tools for VMware vSphereでは、ONTAPでのプロビジョニングに読み取り権限だけでは不十分なためです。

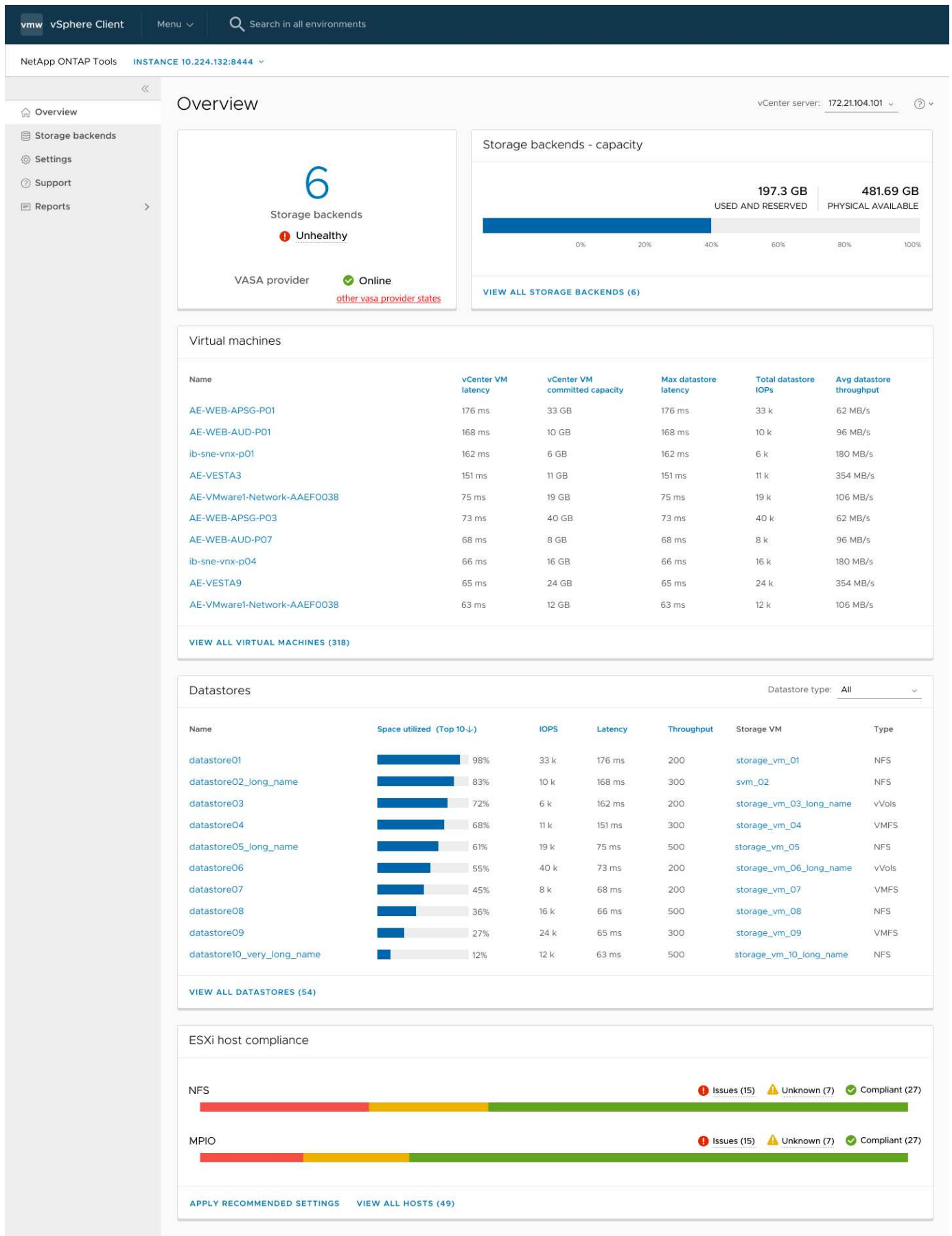
APIの使用：

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

NetApp ONTAP Tools for VMware vSphereプラグインのダッシュボードの概要

vCenter ClientのショートカットセクションでNetApp ONTAP tools for VMware vSphereプラグインのアイコンを選択すると、概要ページが表示されます。このページはダッシュボードのように機能し、ONTAP Tools for VMware vSphereプラグインの概要を確認できます。

Enhanced Linked Mode setup (ELM；拡張リンクモードセットアップ) の場合は、[vCenter Server select]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表示で使用できます。1つのページでvCenter Serverを選択した場合、プラグインのタブには表示されません。



ダッシュボードには、システムのさまざまな要素を示す複数のカードがあります。次の表に、さまざまなカー

ドとその意味を示します。

カード名	* 概要 *
ステータス	[Status]カードには、追加されたストレージバックエンドの数、ストレージバックエンドの全体的な健全性ステータス、vCenterのVASA Providerステータスが表示されます。すべてのストレージバックエンドのステータスがnormalの場合、ストレージバックエンドのステータスは「healthy」と表示されます。いずれかのストレージバックエンドに問題（Unknown / Unreachable / Degradedステータス）が設定されている場合、ストレージバックエンドのステータスは「Unhealthy」と表示されます。「異常」ステータスをクリックすると、ストレージバックエンドのステータスを示すツールヒントが開きます。任意のストレージバックエンドをクリックすると、詳細が表示されます。[Other VASA Provider (VP) states]リンクには、vCenter Serverに登録されているVP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。
仮想マシン	このカードには、上位10個のVMがパフォーマンス指標でソートされて表示されます。ヘッダーをクリックすると、選択した指標の上位10台のVMを昇順または降順でソートして表示できます。カードで行われたソートとフィルタリングの変更は、ブラウザ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、上位10個のデータストアがパフォーマンス指標でソートされて表示されます。ヘッダーをクリックすると、選択した指標の上位10個のデータストアが昇順または降順でソートされて表示されます。カードで行われたソートとフィルタリングの変更は、ブラウザキャッシュを変更またはクリアするまで保持されます。[Datastore type]ドロップダウンで、データストアのタイプ（NFS、VMFS、またはVVOL）を選択できます。
ESXiホストコンプライアンスカード	このカードには、選択したvCenterのすべてのESXiホスト設定の、推奨されるNetAppホスト設定に関する全体的な準拠ステータスが、設定グループ/カテゴリ別に表示されます。[推奨設定の適用]リンクをクリックすると、推奨設定を適用できます。[問題/不明]をクリックすると、ホストのリストが表示されます。

データストアを作成

ホストクラスタレベルでデータストアを作成すると、データストアが作成されてデスティネーションのすべてのホストにマウントされます。この操作は、現在のユーザに実行権限がある場合にのみ有効になります。

[Create Datastore]アクションウィザードでは、NFS、VMFS、およびvVolデータストアを作成できます。

vVolデータストアを作成する

vVolデータストアは、新しいボリュームまたは既存のボリュームを使用して作成できます。既存のボリュームと新しいボリュームが混在しているvVolデータストアを作成することはできません。



ルートアグリゲートがSVMにマッピングされていないことを確認します。

開始する前に

選択したvCenterにVASA Providerが登録されていることを確認してください。

手順

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
2. ホストシステム、ホストクラスタ、データセンターを右クリックし、* NetApp ONTAP tools >[Create Datastore]*を選択します。
3. ペインで、[データストアタイプ]*で[VVols]を選択します。
4. [名前とプロトコル]ペインで、[データストア名]*と[プロトコル]*の情報を指定します。
5. ペインで、[プラットフォーム]および[Storage VM]*を選択します。[アドバンスドオプション]*セクションで、カスタムのエクスポートポリシー（NFSプロトコルの場合）またはカスタムのイニシエータグループ名（iSCSIプロトコルの場合）を必要に応じて選択します。
 - [プラットフォーム]オプションと[非対称]オプションを使用すると、[SVM]ドロップダウンオプションをフィルタして除外できます。作成するSVMを選択するか、ボリュームをデータストアの作成に使用してください。
 - [非対称]*トグルボタンは、前の手順で[iSCSI]を選択し、[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]を選択した場合にのみ表示されます。
 - AFFプラットフォームの場合は[非対称]トグルボタンを選択し、ASAプラットフォームの場合は無効にします。
6. [ストレージ属性]*ペインで、新しいボリュームを作成するか、既存のボリュームを使用できます。新しいボリュームを作成するときに、データストアでQoSを有効にすることができます。
7. ペインで選択内容を確認し、[完了]*をクリックします。vVol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。

NFSデータストアを作成する

VMware Network File System (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、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. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
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 tools >[Create Datastore]*を選択します。
3. [タイプ]ペインで、*[データストアタイプ]*で[NFS]を選択します。

4. ペインで、データストア名、サイズ、およびプロトコル情報を入力します。アドバンストオプションで、[データストアクラスタ]および[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. ペインで、[プラットフォーム]および[Storage VM]を選択します。[アドバンストオプション]*セクションで[カスタムエクスポートポリシー]*を選択できます。
 - *非対称*トグルボタンは、プラットフォームの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表示されます。
 - *[プラットフォーム]ドロップダウンの[任意]*オプションを使用すると、プラットフォームフラグまたは非対称フラグに関係なく、vCenterに含まれるすべてのSVMを表示できます。
6. ペインで、ボリュームを作成するアグリゲートを選択します。アドバンストオプションで、必要に応じて[スペースリザベーション]および[QoSを有効にする]*を選択します。
7. ペインで選択内容を確認し、[完了]*をクリックします。

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データストアの作成

Virtual Machine File System (VMFS) は、VMware vSphere環境に仮想マシンファイルを格納するために特別に設計されたクラスタファイルシステムです。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ため、vMotionや高可用性などの機能が有効になります。

手順

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
2. ホストシステム、ホストクラスタ、またはデータストアを右クリックし、* NetApp ONTAP tools >[Create Datastore]*を選択します。
3. [タイプ]ペインで、*[データストアタイプ]*で[VMFS]を選択します。
4. ペインで、データストア名、サイズ、およびプロトコルの情報を入力します。ペインの[アドバンストオプション]*セクションで、このデータストアを追加するデータストアクラスタを選択します。
5. [ストレージ]ペインで[プラットフォームとStorage VM]を選択します。[非対称]トグルボタンを選択します。ペインの*セクションで[カスタムイニシエータグループ名]*を指定します（オプション）。データストア用に既存のigroupを選択するか、カスタム名を指定して新しいigroupを作成できます。

プラットフォームのドロップダウンで*[いずれか]*オプションを選択すると、プラットフォームフラグまたは非対称フラグに関係なく、vCenterに含まれるすべてのSVMが表示されます。

6. ストレージ属性ペインで、ドロップダウンメニューから*を選択します。必要に応じて[アドバンストオプション]セクションで[スペースリザベーション]、[既存のボリュームを使用]、[QoSを有効にする]*オプションを選択し、必要に応じて詳細を指定します。
7. ペインでデータストアの詳細を確認し、[終了]*をクリックします。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

SRAを有効にしてデータストアを保護する

ONTAP tools for VMware vSphereには、SRA機能を有効にしてディザスタリカバリを設定するためのオプションがあります。

- 必要なもの *
 - vCenter ServerインスタンスのセットアップとESXiホストの設定が完了している必要があります。
 - ONTAP toolsを導入しておく必要があります。
 - `.tar.gz` からSRAアダプタファイルをダウンロードしておく必要があります "[NetAppサポートサイト](#)"。
 - 手順 *
1. URL：を使用してSRMアプライアンス管理インターフェイスにログインし
`https://:<srm_ip>:5480`、VMware SRMアプライアンス管理インターフェイスで[Storage Replication Adapters]に移動します。
 2. [New Adapter]*を選択します。
 3. SRA プラグインの .tar.gz_installer を SRM にアップロードします。
 4. アダプタを再スキャンして、SRMの[Storage Replication Adapters]ページで詳細が更新されたことを確認します。

ディザスタリカバリ用のストレージシステムの設定

SAN環境およびNAS環境向けのSRAの設定

Site Recovery Manager (SRM) 向けStorage Replication Adapter (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環境用のSRAの設定

- 必要なもの *

保護対象サイトとリカバリサイトには、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。

- SRM

SRMのインストールに関するドキュメントは、VMwareサイトで参照できます。

["VMware Site Recovery Manager のドキュメント"](#)

- SRA

アダプタがSRMにインストールされている。

- 手順 *

1. 保護対象サイトのプライマリストレージシステムのLUNにプライマリESXiホストが接続されていることを確認します。
2. `ostype`プライマリストレージシステムで、LUNが属するigroupのオプションが`\_vmware\_`に設定されていることを確認します。
3. リカバリサイトのESXiホストからStorage Virtual Machine (SVM) への適切なiSCSI接続が確立されてい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、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する必要があります。

そのためには、ESXiホストのSVMでローカルLUNが接続されていることを確認するか、`iscsi show initiators`SVMでコマンドを実行します。ESXiホストでマッピングされたLUNへのLUNアクセスをチェックして、iSCSI接続を確認します。

NAS環境向けのSRAの設定

- 必要なもの *

保護対象サイトとリカバリサイトには、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。

- SRM

SRM のインストールに関するドキュメントは、VMware のサイトで入手できます。

["VMware Site Recovery Manager のドキュメント"](#)

- SRA

SRMとSRAサーバにアダプタをインストールします。

- 手順 *

1. 保護対象サイトのデータストアに、vCenter Serverに登録されている仮想マシンが含まれていることを確認します。
2. 保護対象サイトの ESXi ホストに、Storage Virtual Machine (SVM) の NFS エクスポートボリュームがマウントされていることを確認します。
3. Array Manager ウィザードを使用して SRM にアレイを追加するときに、NFS エクスポートが存在する IP アドレス、ホスト名、FQDN などの有効なアドレスが **NFS Address** フィールドに指定されていることを確認します。
4. `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のNFSエクスポートへの接続に使用されるIPアドレスにホストのVMkernelポートからアクセスできることを確認します。

大規模な環境向けのSRAの設定

大規模な環境で最適なパフォーマンスを実現するには、Storage Replication Adapter (SRA) の推奨設定に従ってストレージのタイムアウト間隔を設定する必要があります。

ストレージプロバイダの設定

大規模な環境では、SRM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 *
StorageProvider.resignatureTimeout	設定値を900秒から12000秒に増やします。
storageProvider.hostRescanDelaySec	60
storageProvider.hostRescanRepeatCnt	20
storageProvider.hostRescanTimeoutSec	高い値を設定します（例：99999）。

また、`StorageProvider.autoResignatureMode` オプションを有効にする必要があります。

ストレージプロバイダの設定の変更の詳細については、VMwareのドキュメントを参照してください。

["VMware vSphere のドキュメント：「ストレージプロバイダ設定の変更」"](#)

ストレージ設定

タイムアウトになった場合は `storage.commandTimeout`、との値を大きくして
`storage.maxConcurrentCommandCnt` 大きい値にします。



指定する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内で終了します。

詳細については、SANプロバイダの設定の変更に関するVMwareのドキュメントを参照してください。

["VMware Site Recovery Manager のドキュメント：「ストレージ設定の変更」"](#)

SRMアプライアンスでSRAを設定する

SRMアプライアンスを導入したら、SRMアプライアンスにSRAを設定する必要があります。SRAを正しく設定すると、ディザスタリカバリ管理のためにSRMアプライアンスがSRAと通信できるようになります。SRMアプライアンスとSRAの間の通信を有効にするには、ONTAP tools for VMware vSphere クレデンシャル（IPアドレス）をSRMアプライアンスに保存する必要があります。

- 必要なもの *

から `_tar.gz_` ファイルをダウンロードしておく必要があります ["NetAppサポートサイト"](#)。

- このタスクについて *

SRMアプライアンスでSRAを設定すると、SRAクレデンシャルがSRMアプライアンスに保存されます。

• 手順 *

1. SRMアプライアンスの画面で、**[Storage Replication Adapter]>*[New Adapter]***をクリックします。
2. SRM に .tar.gz_file をアップロードします。
3. puttyを使用して、管理者アカウントでSRM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ユーザに切り替えます。 `su root`
5. コマンドを実行し `cd /var/log/vmware/srm` でログディレクトリに移動します。
6. ログの場所で、コマンドを入力してSRAで使用されるDocker IDを取得します。 `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、SRMにONTAP tools for VMware vSphereのIPアドレスとパスワードを設定します。 `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>'`



Perlスクリプトでパスワードの特殊文字が入力の区切り文字として読み取られないようにするには、パスワードの値を一重引用符で囲む必要があります。

9. アダプタを再スキャンして、SRMの[Storage Replication Adapters]ページで詳細が更新されたことを確認します。

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。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。

SRAクレデンシャルの更新

SRMがSRAと通信するためには、クレデンシャルを変更した場合にSRMサーバでSRAクレデンシャルを更新する必要があります。

• 必要なもの *

トピックに記載されている手順を実行しておく必要があります ["SRMアプライアンスでのSRAの設定"](#)。

• 手順 *

1. 次のコマンドを実行して、SRMマシンフォルダのCached ONTAP toolsユーザ名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、SRAに新しいクレデンシャルを設定します。

- 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>`` パスワードの値は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。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

保護グループの設定

保護対象サイトで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。

- 必要なもの *

ソースサイトとターゲットサイトの両方が次のように構成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SRM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をペアリング
 - 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こと
 - 手順 *
 1. vCenter Serverにログインし、[サイトリカバリ]>*[保護グループ]*をクリックします。
 2. [* 保護グループ *] ウィンドウ枠で、[* 新規 *] をクリックします。
 3. 保護グループの名前と概要、方向を指定し、*次へ*をクリックします。
 4. [タイプ]*フィールドで、NFSおよびVMFSデータストアの[タイプ]フィールドオプション...[*]を[データストアグループ (アレイベースのレプリケーション)]として選択します。フォールトドメインは、レプリケーションが有効になっているSVMにすぎません。ピアリングのみが実装されていて問題がない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設定した仮想マシンがあるレプリケーショングループのいずれかを選択し、*次へ*をクリックします。
- 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、または新しいリカバリプランに追加 * をクリックして新しいプランを作成します。
 7. [完了準備完了] タブで、作成した保護グループの詳細を確認し、[完了] をクリックします。

保護対象サイトとリカバリサイトをペアリング

Storage Replication Adapter (SRA) でストレージシステムを検出できるようにするには、作成された保護対象サイトとリカバリサイトをvSphere Clientを使用してペアリング

する必要があります。



Storage Replication Adapter (SRA) では、ファンアウトSnapMirror構成がサポートされません。SnapMirrorのファンアウト構成は、ソースボリュームが2つの異なるデスティネーションにレプリケートされる構成です。SRMがデスティネーションから仮想マシンをリカバリする必要がある場合、リカバリ中に問題が発生します。

- 必要なもの *
- 保護対象サイトとリカバリサイトにSite Recovery Manager (SRM) をインストールしておく必要があります。
- 保護対象サイトとリカバリサイトにSRAをインストールしておく必要があります。
- 手順 *
 1. vSphere Client のホームページで [サイトのリカバリ] をダブルクリックし、[サイト] をクリックします。
 2. [* オブジェクト * > * アクション * > * サイトのペアリング *] をクリックします。
 3. ペアサイトリカバリマネージャサーバーダイアログボックスで、保護サイトのプラットフォームサービスコントローラのアドレスを入力し、次へ * をクリックします。
 4. [vCenter Serverの選択]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ることを確認します。
 - b. SSO 管理クレデンシャルを入力し、[* 終了 *] をクリックします。
 5. プロンプトが表示されたら、[はい] をクリックしてセキュリティ証明書を受け入れます。
- 結果 *

保護対象サイトとリカバリサイトの両方が [オブジェクト] ダイアログボックスに表示されます。

保護サイトとリカバリサイトのリソースを設定

ネットワークマッピングの設定

保護対象サイトの各リソースがリカバリサイトの適切なリソースにマッピングされるように、両方のサイトでVMネットワーク、ESXiホスト、フォルダなどのリソースマッピングを設定する必要があります。

次のリソース設定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
- 必要なもの *

保護対象サイトとリカバリサイトを接続しておく必要があります。

• 手順 *

1. vCenter Serverにログインし、* Site Recovery > Sites *をクリックします。
2. 保護されたサイトを選択し、* 管理 * をクリックします。
3. [管理] タブで、[ネットワークマッピング *] を選択します。
4. [新規]*をクリックして、新しいネットワークマッピングを作成します。

Create Network Mappingウィザードが表示されます。

5. Create Network Mappingウィザードで、次の手順を実行します。
 - a. を選択し、[Next]*をクリックします。
 - b. 保護対象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]*をクリックします。
 - c. マッピングが正常に作成されたら、* 次へ * をクリックします。
 - d. 前に使用したオブジェクトを選択してリバースマッピングを作成し、*[完了]*をクリックします。

• 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、同じ手順を実行できます。

フォルダマッピングの設定

保護対象サイトとリカバリサイトの間の通信を有効にするには、それらのサイトのフォルダをマッピングする必要があります。

• 必要なもの *

保護対象サイトとリカバリサイトを接続しておく必要があります。

• 手順 *

1. vCenter Serverにログインし、* Site Recovery > Sites *をクリックします。
2. 保護されたサイトを選択し、* 管理 * をクリックします。
3. [管理] タブで、[* フォルダーマッピング *] を選択します。
4. [フォルダ]アイコンを選択して、新しいフォルダマッピングを作成します。

Create Folder Mappingウィザードが表示されます。

5. Create Folder Mappingウィザードで、次の手順を実行します。
 - a. を選択し、[Next]*をクリックします。
 - b. 保護対象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]*をクリックします。
 - c. マッピングが正常に作成されたら、* 次へ * をクリックします。
 - d. 前に使用したオブジェクトを選択してリバースマッピングを作成し、*[完了]*をクリックします。

• 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、同じ手順を実行できます。

リソースマッピングの設定

仮想マシンがどちらか一方のホストグループにフェイルオーバーするように構成されるように、保護対象サイトとリカバリサイトのリソースをマッピングする必要があります。

• 必要なもの *

保護対象サイトとリカバリサイトを接続しておく必要があります。



Site Recovery Manager (SRM) では、リソースとしてリソースプール、ESXiホスト、vSphere クラスタがあります。

• 手順 *

1. vCenter Serverにログインし、* Site Recovery > Sites *をクリックします。
2. 保護されたサイトを選択し、* 管理 * をクリックします。
3. [管理] タブで、[* リソースマッピング *]を選択します。
4. [新規]*をクリックして、新しいリソースマッピングを作成します。

Create Resource Mappingウィザードが表示されます。

5. Create Resource Mappingウィザードで、次の手順を実行します。
 - a. を選択し、[Next]*をクリックします。
 - b. 保護対象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]*をクリックします。
 - c. マッピングが正常に作成されたら、* 次へ * をクリックします。
 - d. 前に使用したオブジェクトを選択してリバースマッピングを作成し、*[完了]*をクリックします。

• 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、同じ手順を実行できます。

プレースホルダデータストアの設定

プレースホルダデータストアを設定して、リカバリサイトのvCenterインベントリに保護対象の仮想マシン (VM) 用の場所を確保する必要があります。プレースホルダVMはサイズが小さく、数百KB以下なので、プレースホルダデータストアを大きくする必要はありません。

• 必要なもの *

- 保護対象サイトとリカバリサイトを接続しておく必要があります。
- リソースマッピングを設定しておく必要があります。
- 手順 *
 1. vCenter Serverにログインし、* Site Recovery > Sites *をクリックします。
 2. 保護されたサイトを選択し、* 管理 * をクリックします。
 3. [管理] タブで、[プレースホルダデータストア] を選択します。
 4. 新しいプレースホルダデータストアを作成するには、*[新規]*をクリックします。
 5. 適切なデータストアを選択し、「* OK 」をクリックします。



プレースホルダデータストアはローカルでもリモートでもかまいません。レプリケートしないでください。

6. 手順3~5を繰り返して、リカバリサイト用のプレースホルダデータストアを設定します。

アレイマネージャを使用したSRAの設定

Site Recovery Manager (SRM) のArray Managerウィザードを使用してStorage Replication Adapter (SRA) を設定し、SRMとStorage Virtual Machine (SVM) が連携できるようにすることができます。

- 必要なもの *
- SRMで保護対象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設定する前に、オンボードストレージを設定しておく必要があります。
- 保護対象サイトとリカバリサイト間のSnapMirror関係を設定し、レプリケートしておく必要があります。
- マルチテナンシーを有効にするには、SVM管理LIFを有効にしておく必要があります。

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。クラスタレベルでストレージを追加すると、クラスタ内のすべてのSVMを検出して処理を実行できます。SVMレベルでストレージを追加する場合は、そのSVMのみを管理できます。

- 手順 *
 1. SRM で、[* Array Managers*] をクリックし、[* Add Array Manager*] をクリックします。
 2. SRMでアレイについて次の情報を入力します。
 - a. [Display Name] フィールドに、アレイマネージャを識別する名前を入力します。
 - b. 「* SRA Type *」フィールドで、「* ONTAP 向け NetApp Storage Replication Adapter 」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設定するときは、ONTAP toolsでストレージシステムをオンボードしていたのと同じ接続（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、アレイマネージャの設定範囲がSVMである場合は、ONTAP tools for VMware vSphereのストレージをSVMレベルで追加する必要があります。

- d. クラスタに接続する場合は、SVM の名前を * SVM 名 * フィールドに入力します。

このフィールドは空白のままにすることもできます。

- e. 検出するボリュームを * Volume include list * フィールドに入力します。

保護対象サイトのソースボリュームとリカバリサイト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、保護対象サイトのフィールドでsrc_vol1を指定し、リカバリサイトのフィールドでdst_vol1を指定する必要があります。

- a. *（オプション）* Volume exclude list * フィールドに、検出対象から除外するボリュームを入力します。

保護対象サイトのソースボリュームとリカバリサイト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、volume_dst_vol1_とSnapMirror関係にあるvolume_src_vol1_を除外する場合は、保護対象サイトのフィールドで_src_vol1_を指定し、リカバリサイトのフィールドで_dst_vol1_を指定する必要があります。

1. 「* 次へ *」をクリックします。
2. アレイが検出され、[Add Array Manager]ウィンドウの下部に表示されていることを確認し、*[Finish]*をクリックします。

適切なSVM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（アレイペアの有効化）画面で、正しいアレイペアが選択され、有効にする準備ができ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確認

Storage Replication Adapter（SRA）を設定したら、保護対象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。レプリケートされたストレージシステムは、保護対象サイトとリカバリサイトの両方から検出可能である必要があります。

- 必要なもの *
- ストレージシステムを設定しておく必要があります。
- SRMアレイマネージャを使用して、保護対象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処理とフェイルオーバー処理を実行する前に、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。

- 手順 *

1. vCenter Serverにログインします。
2. [* Site Recovery] * > [* Array Based Replication] 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。

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

ONTAPツールの管理

データストアの管理

NFSデータストアとVMFSデータストアのマウント

データストアをマウントすると、追加の（NFS / VMFS）ホストにストレージ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に、そのホストにデータストアをマウントできます。



vSphere Client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、一部の右クリック操作が無効または使用できない場合があります。vSphere Client 8.0以降のバージョンを使用している場合、一部の右クリックオプションは非表示になります。vSphere 7.0U3からvSphere 8.0のバージョンでは、オプションが表示されていても、この操作は無効になります。

• 手順 *

1. vSphere Client のホームページで、* Hosts and Clusters * をクリックします。
2. ナビゲーションペインで、ホストを含むデータセンターを選択します。
3. ホストを追加する場合は、手順2を繰り返します。
4. ホストまたはホストクラスタにNFS / VMFSデータストアをマウントするには、データストアを右クリックし、* NetApp ONTAP tools > Mount Datastores *を選択します。
5. マウントするデータストアを選択し、*[マウント]*をクリックします。

進捗状況は、[最近のタスク]パネルで追跡できます。

vVolデータストアのマウント

VMware Virtual Volumes (vVol) データストアを1つ以上の追加ホストにマウントして、追加のホストにストレージアクセスを提供することができます。vVolデータストアをアンマウントできるのは、APIを使用する場合のみです。

• 手順 *

1. vSphere Client のホームページで、* Hosts and Clusters * をクリックします。
2. ナビゲーションペインで、データストアを含む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 tools > Mount datastore *を選択します。
4. 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]*をクリックします。

進捗状況は、[最近のタスク]パネルで追跡できます。

NFSデータストアと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拡張できま

す。データストアのサイズは、インフラ要件の変化に応じて変更できます。

- このタスクについて *

NFSデータストアとVMFSデータストアのサイズは、必ず拡張する必要があります。NFSデータストアとVMFSデータストアの一部であるFlexVolボリュームは、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 のホームページで、* Hosts and Clusters * をクリックします。
2. ナビゲーションペインで、データストアを含む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 tools > Resize datastore *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 * をクリックします。

vVolデータストアの拡張

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、[plug-in] セクションにONTAP tools for VMware vSphereでサポートされるアクションが表示されます。データストアのタイプと現在のユーザ権限に応じて、特定の操作が有効になります。

- 手順 *

1. vSphere Client のホームページで、* Hosts and Clusters * をクリックします。
2. ナビゲーションペインで、データストアを含む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 tools > Add storage to datastore *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、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できます。このUIはわかりやすいもので、説明を必要としません。選択した手順に従ってください。
5. ウィンドウで、選択内容を確認し、[展開]*をクリックします。進捗状況は、[最近のタスク]パネルで追跡できます。

vVolデータストアの縮小

[データストアの削除]操作を実行すると、選択したデータストアにVVolがない場合にデータストアが削除されます。

手順

1. vSphere Client のホームページで、* Hosts and Clusters * をクリックします。
2. ナビゲーションペインで、データストアを含む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 tools > [データストアからのストレージの削除]*を選択します。
4. vVolがないボリュームを選択し、*[削除]*をクリックします。



vVolが配置されているボリュームを選択するオプションが無効になります。

5. ポップアップで[ONTAPクラスタからボリュームを削除する]チェックボックスを選択してデータストアおよび**ONTAP**ストレージからボリュームを削除し、[削除]*をクリックします。

データストアの削除

[データストアからのストレージの削除]操作は、vCenter Serverで検出または管理されるすべてのONTAP tools for VMware vSphere vVolデータストアでサポートされます。この操作により、vVolデータストアからボリュームを削除できます。

削除オプションは、特定のボリュームにVVolがある場合は無効になります。データストアからのボリュームの削除に加えて、ONTAPストレージ上の選択したボリュームも削除できます。

vCenter ServerのONTAP tools for VMware vSphereからデータストアを削除すると、次の処理が実行されます。

- VVolコンテナをアンマウントします。
- igroupをクリーンアップします。igroupを使用していない場合は、iqnをigroupから削除します。
- VVolコンテナを削除します。
- Flexボリュームをストレージアレイに残します。

vCenter ServerからONTAP toolsからNFS、VMFS、またはVVolデータストアを削除するには、次の手順を実行します。

手順

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
2. ホストシステム、ホストクラスタ、またはデータストアを右クリックし、* NetApp ONTAP tools *>*データストアの削除*を選択します。



データストアを使用している仮想マシンがある場合は、データストアを削除できません。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。

- a. NFSまたはVMFSデータストアの場合は、ダイアログボックスに、そのデータストアを使用しているVMのリストが表示されます。
 - b. vVolデータストアの場合、[Delete datastore]操作を実行すると、関連付けられているvVolがないデータストアのみが削除されます。[Delete datastore]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。
3. ONTAPストレージの元のボリュームを削除するには、* ONTAPクラスタのボリュームを削除する*を選択します。

データストアの**ONTAP**ストレージビュー

ONTAP tools for VMware vSphereの[Configure]タブにあるONTAPストレージビューには、データストアとそのボリュームに関連するデータが表示されます。このビューに

は、データストアのストレージ側が表示されます。

NFSデータストア用のONTAPストレージビュー

手順

1. vSphere Clientで、NFSデータストアに移動します。
2. 右ペインの*[設定]*タブをクリックします。
3. NetApp ONTAP tools > ONTAP Storage を選択します。右側のペインに[ストレージの詳細]および NFSの詳細*が表示されます。
 - 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、およびボリュームに関する情報が表示されます。
 - [NFSの詳細]ページには、NFSデータストアに関連するデータが表示されます。

VMFSデータストア用のONTAPストレージビュー

手順

1. vSphere Clientで、VMFSデータストアに移動します。
2. 右ペインの*[設定]*タブをクリックします。
3. NetApp ONTAP tools > ONTAP Storage を選択します。右側のペインに[ストレージの詳細]および LUNの詳細*が表示されます。
 - 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、およびボリュームに関する情報が表示されます。
 - [LUNの詳細]ページには、LUNに関連するデータが表示されます。

vVolデータストアのONTAPストレージビュー

手順

1. vSphere Clientで、vVolデータストアに移動します。
2. 右ペインの*[設定]*タブをクリックします。
3. NetApp ONTAP tools > ONTAP Storage *を選択します。
4. ONTAPストレージビューには、すべてのボリュームが表示されます。ONTAPストレージペインでは、ストレージを拡張または削除できます。

"[vVolデータストアの拡張](#)"セクションの手順に従ってvVolデータストアを追加し、"[vVolデータストアの縮小](#)"セクションの手順に従ってデータストアを削除します。

仮想マシンストレージビュー

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



このビューは、ONTAP Tools for VMware vSphereで管理するvVolデータストア関連のディスクが1つ以上マウントされているVMに適用されます。

手順

1. vSphere Clientで、仮想マシンに移動します。
2. 右側のペインで* Monitor *タブをクリックします。
3. NetApp ONTAP tools > Storage を選択します。右側のペインに[ストレージ]*の詳細が表示されます。VMに存在するvVolのリストが表示されます。

[列の管理]オプションを使用すると、別の列の表示/非表示を切り替えることができます。

ストレージのしきい値の管理

ボリュームやアグリゲートの容量が特定のレベルに達したときにvCenter Serverで通知を受信するしきい値を設定できます。

手順：

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
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 tools *をクリックします。
3. ONTAPツールの左側のペインで、[設定]>*>[編集]*に移動します。
4. ウィンドウで、[ほぼフル]フィールドと[フル]*フィールドに必要な値を指定し、[保存]をクリックします。推奨値（「ほぼフル」が80、「フル」が90）にリセットできます。

ストレージバックエンドを管理

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。

ストレージの検出

ストレージバックエンドの検出は、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、次の手順を実行します。

手順

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
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 tools *をクリックします。
3. ONTAP toolsの左側のペインで、*[Storage backends]*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クリックし、*ストレージの検出*を選択します。

進捗状況は、[最近のタスク]パネルで追跡できます。

ストレージバックエンドの変更

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を実行します。

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>

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 tools *をクリックします。
3. ONTAP toolsの左側のペインで、*[Storage backends]*に移動し、ストレージバックエンドを選択します。
4. クレデンシャルまたはポート名を変更するには、縦の省略記号メニューをクリックし、*[変更]*を選択します。進捗状況は、[最近のタスク]パネルで追跡できます。

ONTAP tools Managerを使用してグローバルONTAPクラスタに対して変更処理を実行するには、次の手順を実行します。

1. WebブラウザからONTAP Tools Managerを起動します。
<https://loadBalanceIP:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャル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. 垂直の省略記号メニューをクリックし、*修正*を選択します。
6. クレデンシャル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、[Username]*と[Password]*を入力します。

ストレージバックエンドの削除

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

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
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 tools *をクリックします。
3. ONTAP toolsの左側のペインで、*[Storage backends]*に移動し、ストレージバックエンドを選択します。
4. 垂直の省略記号メニューをクリックし、*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ないことを確認します。進捗状況は、[最近のタスク]パネルで追跡できます。

ONTAP tools Managerを使用して、グローバルONTAPクラスタの削除処理を実行できます。

1. WebブラウザからONTAP Tools Managerを起動します。
<https://loadBalanceIP:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーから* Storage backends *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てください
5. 垂直の省略記号メニューをクリックし、*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表示されます。クラスタ内の個々の子ではなく、追加したストレージバックエンドに対してストレージの検出、変更、および削除の処理を実行できます。

ストレージバックエンドの親クラスタまたは子クラスタをクリックすると、コンポーネントの全体的な概要が

表示されます。親クラスタをクリックすると、処理ドロップダウンが表示され、ストレージの検出、変更、削除の各処理を実行できます。このオプションは、子SVMをクリックした場合は表示されません。

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た権限。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。権限はクラスタベースのストレージバックエンドでのみ表示されます。SVMをストレージバックエンドとして追加すると、権限の情報は表示されません。

[Interface]タブには、インターフェイスに関する詳細情報が表示されます。

[ローカル階層]タブには、アグリゲート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します。

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

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または関連付け解除する

vCenter Serverのリストページには、関連す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に関連付けまたは関連付け解除するオプションがあります。このタスクでは、ストレージバックエンドとオンボードされたvCenter Serverインスタンスの間のマッピングをグローバルに作成できます。

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

vCenter Serverインスタンスの変更

vCenter Serverインスタンスを変更するには、次の手順を実行します。

1. WebブラウザからONTAP Tools Managerを起動します。
`https://loadBalanceIP:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーから[vCenter Serverインスタンス]を選択します。
4. 変更するvCenter Serverの縦の省略記号をクリックし、*[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インスタンスの削除

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 Tools Managerを起動します。
`https://loadBalanceIP:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーから[vCenter Serverインスタンス]を選択します。
4. 削除するvCenter Serverの縦の省略記号をクリックし、*[削除]*を選択します。



削除したvCenter Serverインスタンスはアプリケーションで管理されなくなります。

証明書の管理

ONTAP tools for VMware vSphereの単一インスタンスで、複数のvCenter Serverインスタンスを管理できます。ONTAP Tools for VMware vSphereは、VASA Provider用の自己署名証明書を使用して導入されます。これにより、vVolデータストアに対して管理できるvCenter Serverインスタンスは1つだけです。複数のvCenter Serverインスタンスを管理していて、複数のvCenter ServerインスタンスでVVol機能を有効にする場合は、ONTAP tools Managerインターフェイスを使用して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。同じインターフェイスを使用して、すべての証明書を更新または更新できます。



カスタムCAに自己署名をアップグレードする場合、異なるドメインにマッピングされた別のロードバランサIPアドレスはサポートされません。

• 手順 *

1. WebブラウザからONTAP Tools Managerを起動します。
`https://loadBalanceIP:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャル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]>*>[更新]*オプションを選択します。



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]>*>[CAにアップグレード]*** オプションを選択します。
 - a. **[証明書をカスタムCA *にアップグレード]**ポップアップで、サーバ証明書、サーバ証明書の秘密鍵、ルートCA証明書、および中間証明書のファイルをアップロードします。ツールヒントには証明書の概要が表示されます。
 - b. この証明書を生成したドメイン名を入力します。
 - c. **[* アップグレード]** をクリックします。



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ます。

igroupとエクスポートポリシーを管理します。

ONTAPでは、エクスポートポリシーを使用してホストへのボリュームデータパスにアクセスし、イニシエータグループ (igroup) を使用してESXiホストへの論理ユニット番号 (LUN) データパスにアクセスします。VMware vSphere向けのONTAPツールを使用すると、igroupを簡単かつわかりやすく作成でき、充実したエンドツーエンドのワークフローが提供されます。整合性を確保するために、ストレージプラットフォームでigroupを直接作成することはサポートされていません。

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

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

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

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

ONTAP Tools for VMware vSphereメンテナンスコンソールへのアクセス

ONTAP Tools for VMware vSphereメンテナンスコンソールの概要

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ます。また、サポートバンドルの生成、さまざまなログレベルの設定、TLS設定の表示と管理、リモート診断の開始を行うこともできます。

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の導入後にVMware Toolsをインストールしておく必要があります。`maint`ONTAP toolsのメンテナンスコンソールにログインするには、導入時に設定したユーザ名とパスワードにを使用する必要があります。メンテナンスコンソールまたはrootログインコンソールでファイルを編集するには、`nano`を使用する必要があります。



`diag`リモート診断を有効にするときは、ユーザのパスワードを設定する必要があります。

メンテナンスコンソールにアクセスするには、導入したONTAP tools for VMware vSphereの`[概要]`タブを使用する必要があります。をクリックすると、メンテナンスコンソールが起動します。

* コンソール・メニュー *	* オプション *
アプリケーションの設定	1. サーバステータスの概要を表示します。 2. VASA ProviderサービスおよびSRAサービスのログレベルの変更 3. AutoSupportを無効にする
システム構成	1. 仮想マシンの再起動 2. 仮想マシンのシャットダウン 3. マネージャUIパスワードをリセットするためのトークンの生成 4. タイムゾーンの変更 5. 新しいNTPサーバの追加 6. jailディスクサイズを増やす (/jail) 7. アップグレード 8. VMware Toolsのインストール

ネットワーク構成	1. IPアドレス設定を表示します。 2. ドメイン名検索設定の表示 3. ドメイン名検索設定の変更 4. 静的ルートを表示します。 5. 静的ルートの変更 6. 変更のコミット 7. ホストへのpingの実行 8. デフォルト設定に戻す
サポートと診断	1. 診断シェルへのアクセス 2. リモート診断アクセスの有効化

リモート診断アクセスの設定

diagユーザのSSHアクセスを有効にするようにONTAP tools for VMware vSphereを設定できます。

- 必要なもの *

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

- このタスクについて *

SSHを使用してdiagユーザアカウントにアクセスする場合は、次の制限事項があります。

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

ログインセッションは翌日の午前0時まで有効です。

- SSHを使用してdiagユーザとして再度ログインした場合

- 手順 *

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

他のノードで**SSH**を開始する

アップグレードの前に、他のノードでSSHを開始する必要があります。

- 必要なもの *

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

- このタスクについて *

アップグレードの前に、各ノードでこの手順を実行してください。

- 手順 *
- 1. vCenter Serverで、VASA Providerへのコンソールを開きます。
- 2. maintenanceユーザとしてログインします。
- 3. と入力 `4` して[Support and Diagnostics]を選択します。
- 4. と入力し `1` て[診断シェルにアクセス]を選択します。
- 5. と入力し `y` て次に進みます。
- 6. コマンド `_sudo systemctl restart ssh_` を実行します。

vCenter Serverと**ONTAP**のクレデンシャルを更新する

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

- 必要なもの *

メンテナンスユーザのログインクレデンシャルが必要です。

- このタスクについて *

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

- 手順 *
- 1. vCenter Serverで、VASA Providerへのコンソールを開きます。
- 2. maintenanceユーザとしてログインします。
- 3. と入力 2 して[System Configuration Menu]を選択します。
- 4. と入力 9 してONTAP資格情報を変更します。
- 5. と入力 10 してvCenterクレデンシャルを変更する。

ONTAP Toolレポート

ONTAP Tools for VMware vSphereプラグインは、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NetApp ONTAP tools for VMware vSphereプラグインのアイコンを選択すると、ユーザインターフェイスが概要ページに移動します。[レポート]タブを選択して、仮想マシンとデータストアのレポートを表示します。

Virtual Machines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のディスクが少なくとも1本必要）のリストとパフォーマンス指標が表示されます。VMレコードを展開すると、ディスクに関連するすべてのデータストア情報が表示されます。

データストアレポートには、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、VMware vSphereで管理されるデータストアで検出または認識されるONTAPツールのリストと、パフォーマンス指標が表示されます。

[列の管理]オプションを使用すると、さまざまな列の表示と非表示を切り替えることができます。

ログファイルを収集する

ONTAP tools for VMware vSphereのログファイルは、ONTAP tools Managerユーザインターフェイスのオプションから収集できます。テクニカルサポートから、問題のトラブルシューティングに役立つログファイルの収集を求められることがあります。



ONTAP tools Managerからのログの生成には、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 Client UIからのログの生成範囲は、選択したvCenter Serverに限定されます。

• 手順 *

1. WebブラウザからONTAP Tools Managerを起動します。
`https://loadBalanceIP:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーから* Log Bundles *を選択します。

この処理には数分かかることがあります。

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

tar.gzファイルをダウンロードし、テクニカルサポートに送信します。

vCenter Client UIを使用してログバンドルを生成するには、次の手順を実行します。

手順

1. 次のコマンドを使用してvSphere Clientにログインします。 `https://vcenterip/ui`
2. vSphere Clientのホームページで、* Support > Log bundle > Generate *に移動します。
3. ログバンドルラベルを指定し、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わります。

仮想マシンの管理

仮想マシンの移行またはクローニングに関する考慮事項

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。

保護された仮想マシンの移行

保護された仮想マシンを次の場所に移行できます。

- 同じvVolデータストアが別のESXiホストにある
- 同じESXiホストにある互換性のある異なるvVolデータストア
- 別のESXiホストにある互換性のある異なるvVolデータストア

仮想マシンを別のFlexVolボリュームに移行すると、対応するメタデータファイルも仮想マシンの情報で更新されます。仮想マシンを同じストレージの別のESXiホストに移行した場合、基盤となるFlexVolボリュームメタデータファイルは変更されません。

保護対象の仮想マシンのクローン作成

保護された仮想マシンのクローンは、次の場所に作成できます。

- レプリケーショングループを使用する同じFlexVol volumeの同じコンテナ

同じFlexVol volume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する別のFlexVol volume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 volumeで、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 volumeでは、メタデータファイルによって更新された仮想マシンの詳細が取得されます。

VMwareでは、現在、VMテンプレートにクローニングされた仮想マシンはサポートされていません。

保護された仮想マシンのクローン作成がサポートされています。

仮想マシンのスナップショット

現時点では、メモリのない仮想マシンのスナップショットのみがサポートされています。仮想マシンにメモリ付きのSnapshotがある場合、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、メモリスナップショットを削除する必要があります。

NFSおよびVMFSデータストアを使用する仮想マシンをvVolデータストアに移行する

NFSおよびVMFSデータストアからVirtual Volumes (vVol) 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vVol機能を活用できます。vVolデータストアを使用すると、増加するワークロード要件に対応できます。

- 必要なもの *

移行する仮想マシンでVASA Provider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、管理処理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vVolデータストアに移行する場合、VMFSデータストアからのデータの移動にはvStorage APIs for Array Integration (VAAI) のオフロードがvCenter Serverで使用されますが、NFS VMDKファイルからのデータの移動には使用されません。VAAIのオフロードは、通常、ホスト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、* Migrate * (移行) をクリックします。
2. を選択し、[次へ]*をクリックします。
3. 仮想ディスクの形式、VMストレージポリシー、および移行するデータストアの機能に一致するvVolデータストアを選択します。「* 次へ *」をクリックします。
4. 設定を確認し、[完了]をクリックします。

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、VVOLデータストアを削除することを推奨します。

- 手順 *

1. https://OTV_IP:8143/Register.htmlに移動してプラグインの登録を解除します。
2. プラグインがvCenter Serverで使用できなくなったことを確認します。
3. ONTAP Tools for VMware vSphere VMをシャットダウンします。
4. ONTAP Tools for VMware vSphere VMを削除します。

ONTAPツールを使用した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。

- 必要なもの *

ESXiホストの設定が含まれている問題がある場合は、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。問題をクリックすると、問題があるESXiホストのホスト名またはIPアドレスを確認できます。

- 手順 *

1. 次のコマンドを使用してvSphere Clientにログインします。 <https://vcenterip/ui>
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 tools *をクリックします。
3. ONTAP tools for VMware vSphereプラグインの概要（ダッシュボード）で、* 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. [推奨設定の適用]*リンクを選択します。
5. ウィンドウで、**NetApp**の推奨されるホスト設定に準拠するホストを選択し、[次へ]*をクリックします。



ESXiホストを展開すると、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]*をクリックします。進捗状況は、[最近使用したタスク]パネルで追跡できます。

パスワードを管理します

ONTAP tools Managerのパスワードの変更

管理者パスワードは、ONTAP tools Managerを使用して変更できます。

- 手順 *

1. WebブラウザからONTAP Tools Managerを起動します。
<https://loadBalanceIP:8443/virtualization/ui/>
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. 画面右上の* administrator アイコンをクリックし、Change password *を選択します。
4. パスワードの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がUI画面に表示されます。
5. 変更を適用するには、*変更*をクリックします。

ONTAP tools Managerのパスワードのリセット

ONTAP tools Managerのパスワードを忘れた場合は、ONTAP tools for VMware vSphere メンテナンスコンソールで生成されたトークンを使用して管理者クレデンシャルをリセットできます。

- 手順 *

1. WebブラウザからONTAP Tools Managerを起動します。
`https://loadBalanceIP: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パスワードをリセットするには、ONTAP tools for VMware vSphereメンテナンスコンソール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。..vCenter Serverで、メンテナンスコンソールを開きます。「2」と入力して[System Configuration]オプションを選択します。「3」を入力してトークンを生成し、マネージャのパスワードをリセットします。
3. パスワードの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、ユーザ名、および新しいパスワードの詳細を入力します。
4. [リセット (Reset)]*をクリックして変更を適用します。パスワードがリセットされたら、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パスワードのリセット

アプリケーションユーザのパスワードは、SRAとVASA ProviderをvCenter Serverに登録するために使用されます。

• 手順 *

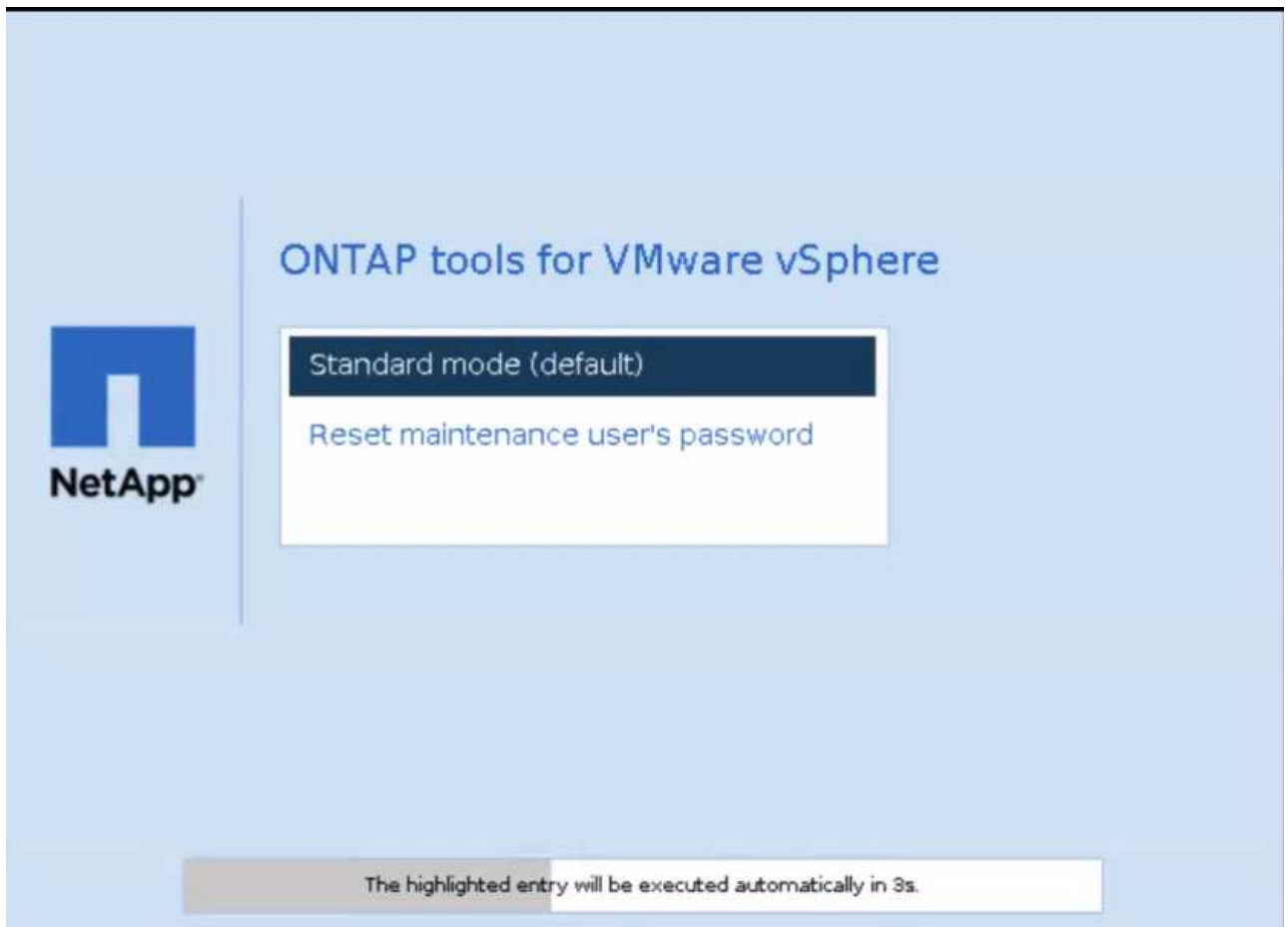
1. WebブラウザからONTAP Tools Managerを起動します。
`https://loadBalanceIP:8443/virtualization/ui/`
2. 導入時に指定したONTAP tools for VMware vSphere管理者のクレデンシャルを使用してログインします。
3. サイドバーの*[設定]*をクリックします。
4. 画面で、[パスワードのリセット]*を選択します。
5. ユーザ名と新しいパスワードを入力し、新しいパスワードの入力を確認します。
6. [リセット (Reset)]*をクリックして変更を適用します。

メンテナンスコンソールのユーザパスワードのリセット

ゲストOSの再起動処理中に、grubメニューにメンテナンスコンソールのユーザ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に存在するメンテナンスコンソールのユーザパスワードを更新する場合に使用します。パスワードのリセットが完了すると、VMが再起動して新しいパスワードを設定します。HA導入シナリオでは、VMの再起動後、他の2つのVMでパスワードが自動的に更新されます。

• 手順 *

1. vCenter Serverにログインする
2. VMを右クリックし、* Power > Restart Guest OS *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。



5秒でオプションを選択できます。いずれかのキーを押して進行状況を停止し、グラブメニューをフリーズします。

3. [メンテナンスユーザ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機会は3回あります。新しいパスワードの入力が完了すると、システムが再起動します。
5. Enter キーを押して続行します。VM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]*オプションを指定した場合にのみ使用してください。

ボリュームをクリーンアップ

ONTAP tools for VMware vSphereの導入環境を削除したら、導入時に作成されたFlexVolをクリーンアップする必要があります。導入に専用のONTAPクラスタを使用していた場合は、FlexVolをクリーンアップする必要があります。導入によって大量のFlexVolが作成され、使用されないためパフォーマンスが低下します。

次のガイドラインに従って、ONTAP tools for VMware vSphere環境の削除後にFlexVolをクリーンアップします。

手順

1. ONTAP tools for VMware vSphereのプライマリノードVMで、次のコマンドを実行して導入タイプを特定します。

```
cat /opt/netapp/meta/ansible vars.yaml | grep -i protocol
```

iSCSI環境の場合は、igroupも削除する必要があります。

2. 次のコマンドを使用して、導入時にONTAPで作成されたFlexVolのリストを取得します。

```
kubectl describe persistentvolumes | grep internalName | awk -F=' ' '{print $2}'
```

3. vCenter ServerからのVMの削除（を参照） ["vCenter ServerまたはデータストアからのVMまたはVMテンプレートの削除"](#)
4. ONTAP System Managerからボリュームを削除します。を参照してください。 ["FlexVol volumeの削除"](#) ボリュームを削除するには、CLIコマンドでFlexVolの正確な名前を指定します。
5. iSCSIを導入する場合は、ONTAPからSAN igroupを削除します。を参照してください。 ["SANイニシエータとigroupの表示と管理"](#)

HA構成では4つのigroupが作成され、非HA構成では2つのigroupが作成されます。次のコマンドを実行して、最初のigroup名を確認します。

```
kubectl -n trident get tbc trident-backend -o yaml | grep igroupName : | awk -F' : ' '{print $2}'
```

その他のigroup名は、VMのホスト名から始まります。

ONTAPツールのアップグレード

ONTAP toolsの最新リリースへのアップグレード

ONTAP tools for VMware vSphere 10.0および10.1から10.1にアップグレードすると、リカバリボリュームが作成され、必要なすべての詳細がリカバリボリュームに反映されます。構成のリカバリが必要な場合は、リカバリボリュームを使用してONTAP tools for VMware vSphereのセットアップをリカバリできます。ONTAP tools for VMware vSphere 10.1のパッチレベルアップグレードを実行する場合は、同じリカバリボリュームが使用され、詳細が更新されます。アップグレードは、HA構成と非HA構成の両方でサポートされます。

- 始める前に *

アップグレードタスクを開始する前に、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で、ONTAP toolsへのコンソールを開きます。
2. maintenanceユーザとしてログインします。
3. 「* 4 *」と入力して[Support and Diagnostics]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. 「* y *」と入力して、任意のパスワードを設定します。
6. ターミナル/puttyから、前の手順で設定した「diag」とパスワードで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*

次のコマンドを実行して、MongoDBのバックアップを作成します。

- `kn exec-it ntv-MongoDB-0 sh-kN`は`kubectl -n ntv-system`の別名である。
- `env | grep MongoDB_root_password` -ポッド内でこのコマンドを実行します。
- 'exit'-これを実行してポッドから出ます。
- `KN exec NTV-MongoDB-0—mongodump -u root -p MongoDB_root_password --archive=/tmp/ mongodb-backup.gz --gzip` -この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` -このコマンドを実行して、上記のコマンドを使用して作成した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スナップショットを作成する

- 「`kN get pvc`」 コマンドを実行し、コマンドの出力を保存します。
- 次のいずれかの方法で、すべてのボリュームのSnapshotを1つずつ作成します。
 - CLIから次のコマンドを実行します。 `volume snapshot create -vserver <vserver_name>-volume <volume_name>-snapshot <snapshot_name>`

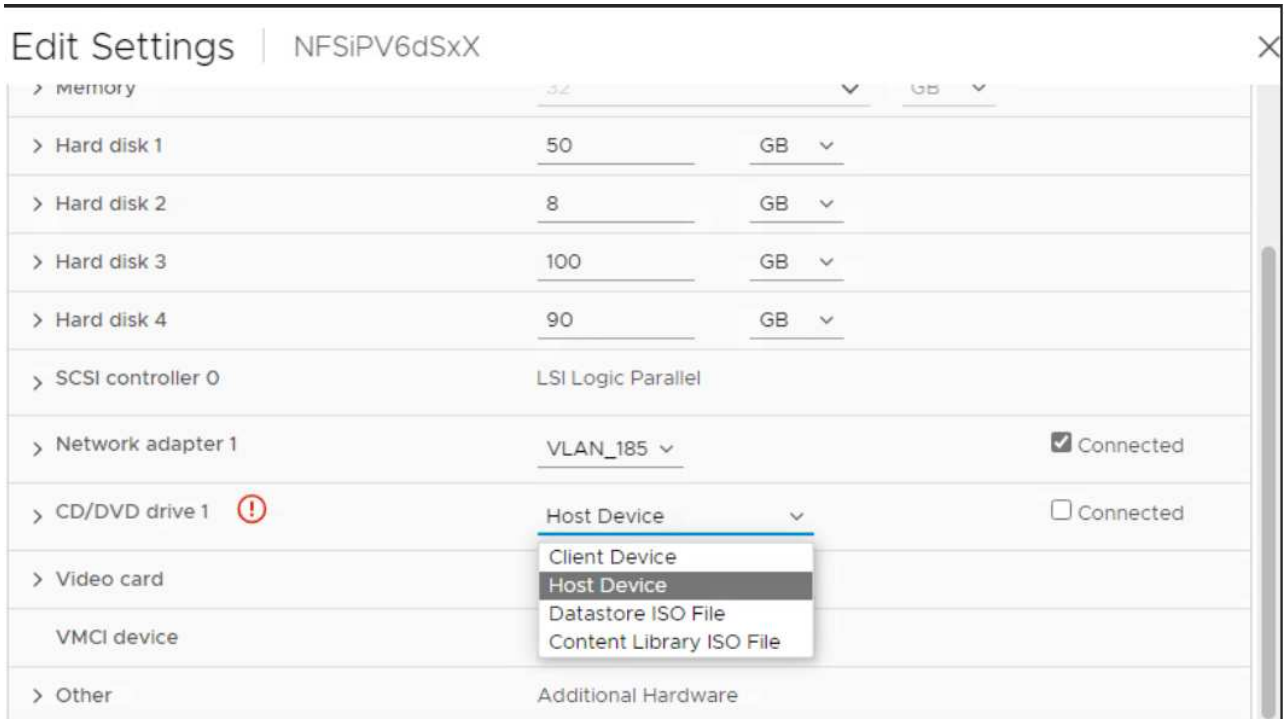
- ONTAP System Managerのユーザインターフェイスで、検索バーの名前でボリュームを検索し、名前をクリックしてボリュームを開きます。[Snapshot]に移動し、そのボリュームのSnapshotを追加します。

- vCenterでVMware vSphere VM用のONTAPツールのスナップショットを作成します（HA導入の場合は3 VM、非HA導入の場合は1 VM）*
- vSphere Clientユーザインターフェイスで、VMを選択します。
- [Snapshots]タブに移動し、*[Take Snapshot]*ボタンをクリックします。

「generate-support-bundle-job」というプレフィックスが付いた完了したポッドをログバンドルから削除してから、アップグレードを実行します。サポートバンドルの生成を実行中の場合は、完了してからポッドを削除します。

• 手順 *

1. ONTAP tools for VMware vSphereアップグレードISO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、[Actions]>*[Edit Settings]*を選択します。
3. [Edit settings]ウィンドウの[CD/DVD drive]フィールドで、[content library ISO file]を選択します。
4. ISOファイルを選択し、* OK *をクリックします。[CD/DVDドライブ]フィールドで[接続済み]チェックボックスを選択します。



5. vCenter Serverで、ONTAP toolsへのコンソールを開きます。
6. maintenanceユーザとしてログインします。
7. 「* 3 *」と入力して、[システム設定]メニューを選択します。
8. 「* 7 *」と入力して、アップグレードオプションを選択します。
9. をアップグレードすると、次の処理が自動的に実行されます。
 - a. 証明書のアップグレード

アップグレードのエラーコード

ONTAP tools for VMware vSphereのアップグレード処理中にエラーコードが発生することがあります。エラーコードは5桁で、最初の2桁は問題に遭遇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。

問題の追跡と解決を容易にするために、すべてのエラーログがansible-perl-errors.logファイルに記録されます。このログファイルには、エラーコードと失敗したAnsibleタスクが記録されます。



このページに記載されているエラーコードは参照用です。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、モードアップグレード
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl、導入、HA
04	firstboot-deploy-otv-ng.pl、デプロイ、非HA
05	firstboot-deploy-otv-ng.pl、リブート
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

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 *	解像度
063	リカバリボリュームへのコンテンツのコピーに失敗しました	Snapshotベースのリカバリを実行
068	Debianパッケージのロールバックに失敗しました	Snapshotベースのリカバリを実行
069	ファイルノリストアニシツハイ	Snapshotベースのリカバリを実行
070	バックアップの削除に失敗	Snapshotベースのリカバリを実行
071	Kubernetesクラスタが健全な状態でない	Snapshotベースのリカバリを実行
072	CRファイルがjailディスクに存在しません	Snapshotベースのリカバリを実行

073	強制調整フラグをfalseに設定中にCRの適用に失敗しました	Snapshotベースのリカバリを実行
074	ISOのマウントに失敗しました	アップグレードを再試行します。
075	アップグレードの事前確認に失敗しました	アップグレードを再試行します。
076	レジストリのアップグレードに失敗しました	Snapshotベースのリカバリを実行
077	レジストリのロールバックに失敗しました	Snapshotベースのリカバリを実行
078	オペレータのアップグレードに失敗しました	Snapshotベースのリカバリを実行
079	オペレータロールバックに失敗しました	Snapshotベースのリカバリを実行
080	サービスのアップグレードに失敗しました	Snapshotベースのリカバリを実行
081	サービスのロールバックに失敗しました	Snapshotベースのリカバリを実行
082	コンテナからの古いイメージの削除に失敗しました	Snapshotベースのリカバリを実行
083	バックアップの削除に失敗しました	Snapshotベースのリカバリを実行
084	JobManagerを本番環境に戻すことができませんでした	Snapshotベースのリカバリを実行
085	CA証明書秘密を作成できませんでした	Snapshotベースのリカバリを実行
086	サーバ/秘密鍵証明書のシークレットを作成できませんでした	Snapshotベースのリカバリを実行
087	失敗しました。10.0から10.1へのアップグレード後の手順を完了できませんでした	アップグレード後の手順に失敗しました。
088	journaldのログローテーションの設定に失敗しました	アップグレードを再試行します。

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が失敗した場合にONTAP tools for VMware vSphereをリストアする方法"](#)

ONTAPツールの移行

最新リリースのONTAP toolsに移行する

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



ONTAP tools for VMware vSphere 9.xxのセットアップは、VASA Provider機能のみを実行する場合にのみ移行することを推奨します。NVMeデータストアとVVolレプリケーションがある場合は、ONTAP tools for VMware vSphere 10.1にセットアップを移行することは推奨されません。

- このタスクについて *

ONTAP tools for VMware vSphere 9.10D2、9.11D4、9.12、9.13リリースから10.1リリースへの移行がサポートされます。



既存のユーザは、パッチリリースにアップグレードする前に、現在のリリースからOVAバックアップを作成する必要があります。

一般的な移行手順

1. ONTAP tools for VMware vSphere 10.1リリース向けOVAを導入します。
2. ONTAP tools for VMware vSphere 10.1リリースに移行するvCenter Serverインスタンスを追加します。を参照し ["vCenter Serverインスタンスの追加と管理"](#)
3. ONTAP Tools for VMware vSphereプラグインvCenter APIを使用して、ストレージバックエンドをローカルでオンボードします。移行用に、ローカルスコープのストレージとしてストレージを追加します。
4. ONTAP tools for VMware vSphere 9.xxから移行されたNFSデータストアとVMFSデータストアがONTAP tools for VMware vSphere 10.1に表示されるのは、データストアの検出ジョブがトリガーされたあとだけです。トリガーされるまでに最大30分かかることがあります。ONTAP tools for VMware vSphere Plugin UIページの[Overview]ページにデータストアが表示されるかどうかを確認します。

SRAの移行手順

- 始める前に *

移行の前に、一方のサイトが保護状態で、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。



フェイルオーバーが完了して再保護が保留になっている場合は、移行しないでください。再保護を完了してから移行を実行します。同じ環境でリカバリプランをテストリカバリプランのテストが完了したら、テストリカバリをクリーンアップし、移行を開始します。

1. SRM UIでONTAP tools for VMware vSphere 9.xxリリースのSRAアダプタを削除するには、次の手順を実行します。
 - a. SRM Configuration Managementページに移動します。

- b. [Storage Replication Adapter]セクションに移動
- c. Kebabメニューをクリックし、* Reset configuration *をクリックします。
- d. ケバブメニューをクリックし、*削除*を選択します。

これらの手順は、保護サイトとリカバリサイトの両方で実行します。

- 2. の手順に従って、保護サイトとリカバリサイトの両方にONTAP Tools for VMware vSphere 10.1 SRAアダプタをインストールします。 ["SRMアプライアンスでSRAを設定する"](#)
- 3. SRM UIページで、[アレイの検出]*処理と[デバイスの検出]*処理を実行し、デバイスが移行前の状態になっていることを確認します。

VASA Providerの移行手順

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

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

- 2. ONTAP tools for VMware vSphere 10.1リリース向けOVAを導入します。
- 3. ONTAP tools for VMware vSphere 10.1リリースに移行するvCenter Serverインスタンスを追加します。を参照して ["vCenter Serverインスタンスを追加する"](#)
- 4. リモートのプラグインvCenter APIからローカルでストレージバックエンドをオンボードする。移行対象としてローカルスコープのストレージを追加します。
- 5. 移行する次のAPI呼び出しを問題します。

◦ 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 *
投稿	/api/v1

処理タイプ

非同期

カールの例

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

◦ JSON入力例* 9.12および9.13からの移行のリクエスト本文：

```
{"otv_ip": "10.12.13.45", "vasa_provider_credentials": {"username": "vasauser", "password":  
"****"} "database_password": "****"}
```

他のリリース移行のリクエスト本文：

```
{"otv_ip": "10.12.13.45", "vasa_provider_credentials": {"username": "vasauser", "password":  
"****"} }
```

◦ JSON出力例*

ジョブオブジェクトが返されます。次の手順で使用するには、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": "running"}
```

6. 次のURIを使用してステータスを確認します。

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

ジョブが完了したら、移行レポートを検証します。job-responseからレポートをJobDataの一部として表示できます。

7. ONTAP tools for VMware vSphereストレージプロバイダをvCenter Serverおよびに追加します ["VASA ProviderをvCenter Serverに登録"](#)。
8. ONTAP Tools for VMware vSphereストレージプロバイダ9.10 / 9.11 / 9.12 / 9.13 VASA Providerサービスをメンテナンスコンソールから停止します。

VASA Providerは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VMにアクセスし、ONTAP Tools for VMware vSphereからアクセス

できます。

9. 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 *
パッチ	/api/v1

処理タイプ

非同期

カールの例

パッチ 「/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43

◦ JSON入力例*

```
{"id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "running"}
```

◦ JSON出力例*

ジョブオブジェクトが返されます。次の手順で使用するには、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": "running"}
```

PATCH処理の要求の本文が空です。



UUIDは、移行後のAPIの応答で返された移行UUIDです。

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

10. 移行用の削除APIは次のとおりです。

* HTTP メソッド *	* パス *
削除	/api/v1

処理タイプ

非同期

カールの例

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

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

移行が完了したら、ONTAP tools 10.1をvCenter Serverに登録したら、次の手順を実行します。

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

REST APIによる自動化

REST APIの概要

REST APIを使用して、VMware vSphereの管理処理用のONTAPツールをいくつか実行できます。REST APIはSwagger Webページから利用できます。

APIドキュメントを表示したり、呼び出しを手動で問題したりするには、`_https://loadbalancerIP:8443/_`にあるSwagger Webページにアクセスします。



すべてのAPIには、要求の本文と、swaggerページに記載されている例があります。このセクションに記載されているワークフローと例は、参照のみを目的としています。

ONTAP tools for VMware vSphere REST APIにアクセスする方法

ONTAP REST API には、いくつかの方法でアクセスできます。

ネットワークに関する考慮事項

REST API には、次のインターフェイスを通じて接続できます。

- クラスタ管理LIF
- ノード管理LIF
- SVM 管理 LIF

使用するLIFは、HTTPS管理プロトコルをサポートするように設定する必要があります。また、ネットワークのファイアウォール設定でHTTPSトラフィックを許可する必要があります。



必ずクラスタ管理LIFを使用してください。これにより、API要求の負荷がすべてのノードに分散され、オフラインになっているノードや接続の問題が発生しているノードを回避できます。複数のクラスタ管理LIFが設定されている場合は、REST APIへのアクセスに関してすべて同じです。

ONTAP Tools for VMware vSphere APIオンラインドキュメントページ

Swaggerには、NetApp ONTAP tools for VMware vSphereプラグインのサポートページにあるハイパーリンクからアクセスできます。

最新バージョンのAPIのドキュメントページにアクセスするためのURLの形式は次のとおりです。

`'https://<loadbalancer_ip_address>/docs/api'`

カスタムのソフトウェアとツール

ONTAP Tools for VMware vSphere APIには、さまざまなプログラミング言語やツールを使用してアクセスで

きます。代表的なものとしては、Python、Java、Curl、PowerShell などがあります。API を使用するプログラム、スクリプト、またはツールは、REST Web サービスのクライアントとして機能します。プログラミング言語を使用すると、API についての理解が深まり、ONTAP Tools for VMware vSphere の管理を自動化することができます。

最新バージョンの API に直接アクセスするためのベース URL の形式は次のとおりです。

```
'https://<loadbalancer_ip_address>/api'
```

複数のバージョンがサポートされている場合に特定のバージョンの API にアクセスするには、次の形式の URL を使用します。

```
'https://<loadbalancer_ip_address>/api/v1'
```

API 要求を制御する入力変数

API 呼び出しの処理方法は、HTTP 要求で設定されたパラメータと変数を使用して制御できます。

HTTP メソッド

ONTAP tools for VMware vSphere REST API でサポートされる HTTP メソッドを次の表に示します。



REST エンドポイントごとにすべての HTTP メソッドを使用できるわけではありません。

HTTP メソッド	製品説明
取得	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。
投稿	指定した入力に基づいて新しいリソースインスタンスを作成します。
削除	既存のリソースインスタンスを削除します。
PUT	既存のリソースインスタンスを変更します。

要求ヘッダー

HTTP 要求には複数のヘッダーを含める必要があります。

コンテンツタイプ

要求の本文に JSON が含まれている場合は、このヘッダーを *application/json* に設定する必要があります。

同意する

このヘッダーは、*application/json* に設定してください。

許可

base64文字列としてエンコードされたユーザ名とパスワードを使用してベーシック認証を設定する必要があります。

リクエストの本文

要求の本文の内容は、それぞれの呼び出しに応じて異なります。HTTP要求の本文は、次のいずれかで構成されます。

- JSONオブジェクトと入力変数
- 空

オブジェクトのフィルタリング

GETを使用するAPI呼び出しを実行するときに、返されるオブジェクトを任意の属性に基づいて制限またはフィルタリングできます。たとえば、次のように完全に一致する値を指定できます。

<field>=<query value>

完全一致に加えて、値の範囲内の一連のオブジェクトを返すための他の演算子も使用できます。ONTAP Tools for VMware vSphere REST APIでは、次の表に示すフィルタ演算子がサポートされます。

運用者	製品説明
=	等しい
<	より小さい
>	次の値より大きい
≤	以下
≥	以上
更新	または
なんだ	等しくない
*	すべてに一致するワイルドカード

また、クエリの一部として **null** キーワードまたはその negation*!null* を使用して、特定のフィールドが設定されているかどうかに基づいてオブジェクトのコレクションを返すこともできます。



通常、設定されていないフィールドはクエリの照合から除外されます。

特定のオブジェクトフィールドの要求

デフォルトでは、GETを使用してAPI呼び出しを実行すると、オブジェクトを一意に識別する属性のみが返されます。このフィールドの最小セットは、各オブジェクトのキーとして機能し、オブジェクトタイプによって異なります。クエリパラメータを使用すると、次の方法で追加のオブジェクトプロパティを選択でき `fields` ます。

共通または標準のフィールド

fields=* を指定すると、最もよく使用されるオブジェクトフィールドが取得されます。これらのフィールドは通常、ローカルサーバメモリに保持されるか、アクセスするための処理をほとんど必要としません。これらは、URLパスキー（UUID）を指定してGETを使用したあとにオブジェクトに対して返されるプロパティと同じです。

すべてのフィールド

fields=** を指定すると 'アクセスするために追加のサーバ処理が必要なフィールドも含め' すべてのオブジェクトフィールドが取得されます

カスタムフィールドの選択

fields=<field_name> を使用すると、必要なフィールドを正確に指定できます。複数のフィールドを要求する場合は、値をカンマで区切ってスペースなしで指定する必要があります。



ベストプラクティスとして、必要なフィールドを常に個別に指定することを推奨します。一連の共通フィールドまたはすべてのフィールドは、必要に応じて取得する必要があります。共通として分類されるフィールドで、**fields=*** を使用して返されるフィールドは、ネットアップの内部パフォーマンス分析に基づいて決定されます。フィールドの分類は、今後のリリースで変更される可能性があります。

出力セット内のオブジェクトのソート

リソースコレクション内のレコードは、オブジェクトによって定義されたデフォルトの順序で返されます。次のように、フィールド名とソート方向を指定したクエリパラメータを使用して順序を変更できます `order_by`。

```
order_by=<field name> asc|desc
```

たとえば、`type` フィールドを降順に並べ替え、`id` を昇順に並べ替えることができます。

```
order_by=type desc, id asc
```

- ソートフィールドを指定しても方向を指定しない場合、値は昇順でソートされます。
- 複数のパラメータを指定する場合は、各フィールドをカンマで区切ります。

コレクション内のオブジェクトを取得するときのページネーション

GETを使用してAPI呼び出しを発行し、同じタイプのオブジェクトのコレクションにアクセスすると、ONTAP tools for VMware vSphereでは、2つの制約に基づいてできるだけ多くのオブジェクトが返されます。これらの各制約は、リクエストの追加のクエリパラメータを使用して制御できます。特定のGET要求に対して最初に到達した制約によって要求が終了するため、返されるレコード数が制限されます。



すべてのオブジェクトについての処理が完了する前に要求が終了した場合、次のレコードのバッチを取得するために必要なリンクが応答に含まれます。

オブジェクト数の制限

デフォルトでは、ONTAP tools for VMware vSphereはGET要求に対して最大10、000個のオブジェクトを返します。この制限は、`_max_records_query` パラメータを使用して変更できます。例：

```
max_records=20
```

返されるオブジェクトの数は、関連する時間制約およびシステム内のオブジェクトの総数に基づいて、有効な最大数よりも少なくなることがあります。

オブジェクトの読み出しに使用する時間の制限

デフォルトでは、ONTAP tools for VMware vSphereは、GET要求で許可された時間内にできるだけ多くのオブジェクトを返します。デフォルトのタイムアウトは15秒です。この制限は、`_return_timeout_query` パラメータを使用して変更できます。例：

```
return_timeout=5
```

返されるオブジェクトの数は、システム内のオブジェクトの総数だけでなく、関連するオブジェクト数の制約に基づいて、有効な最大数よりも少なくなることがあります。

結果セットの絞り込み

必要に応じて、これらの2つのパラメータを追加のクエリパラメータと組み合わせて、結果セットを絞り込むことができます。たとえば、次の例では、指定した時間が経過すると生成されたEMSイベントが最大10個返されます。

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

複数の要求を発行してオブジェクトをページングすることができます。以降の各API呼び出しでは、最後の結果セットの最新のイベントに基づいて新しい時間値を使用する必要があります。

サイズのプロパティ

一部のAPI呼び出しおよび特定のクエリパラメータで使用する入力値は数値です。バイト単位で整数を指定する代わりに、必要に応じて次の表に示すサフィックスを使用できます。

サフィックス	製品説明
KB	KBキロバイト（1024バイト）またはキビバイト
MB	MBメガバイト（KB x 1024バイト）またはメビバイト
GB	GBギガバイト（MB x 1024バイト）またはギビバイト
TB	テラバイト（GB x 1024バイト）またはテビバイト
PB	ペタバイト（TB x 1024バイト）またはペビバイト

Swagger UIからONTAP Tools for VMware vSphere APIのリファレンスドキュメントにアクセス

ONTAP REST APIのドキュメントには、ローカルのONTAPシステムのSwagger UIからアクセスできます。

- 始める前に *

次の情報が必要です。

- ONTAP クラスタ管理 LIF の IP アドレスまたはホスト名
- ONTAP REST APIにアクセスする権限を持つアカウントのユーザ名とパスワード

手順

1. ブラウザにURLを入力し、* Enter *: `_https://<ip_address>/docs/api_`を押します。
2. ONTAPアカウントを使用してサインイン

ONTAP API ドキュメントページが表示され、主要なリソースカテゴリ別に分類された API 呼び出しが下部に表示されます。

3. 個々の API 呼び出しの例として、* cluster * カテゴリまでスクロールし、* get/cluster * をクリックします。

REST APIの使用を開始する

ONTAP Tools for VMware vSphere REST APIはすぐに使用を開始できます。APIにアクセスすると、ライブセットアップの複雑なワークフロープロセスでAPIを使用する前に、ある程度の情報を確認できます。

Hello world

システムで簡単なコマンドを実行して、ONTAP tools for VMware vSphere REST APIの使用を開始し、使用可能かどうかを確認できます。

開始する前に

- システムでCurlユーティリティが使用可能であることを確認します。
- ONTAP tools for VMware vSphereサーバのIPアドレスまたはホスト名
- ONTAP tools for VMware vSphere REST APIにアクセスする権限を持つアカウントのユーザ名とパスワード。



クレデンシャルに特殊文字が含まれている場合は、使用しているシェルに基づいてCurlが許容できる形式にする必要があります。たとえば、各特殊文字の前にバックスラッシュを挿入したり、文字列全体を一重引用符で囲むことができます `username:password`。

ステップ

コマンドラインインターフェイスで、次のコマンドを実行してプラグイン情報を取得します。

```
curl -X GET -u username:password -k  
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

例：

```
curl -X GET -u admin:password -k  
"https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

ワークフロー

ストレージ検出

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

次のAPIを使用して検出を実行します。

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



オンボードストレージバックエンド（SVMまたはクラスタ）のワークフローを参照し、ストレージバックエンドAPIの応答からIDを取得してください。

このAPIエンドポイントからの検出は、ローカルを対象としたストレージバックエンドでのみサポートされ、グローバルを対象としたストレージバックエンドではサポートされません。ストレージバックエンドのタイプがclusterの場合は、子SVMに対して暗黙的に検出が実行されます。ストレージバックエンドのタイプがSVMの場合、選択したSVMに対してのみ検出が実行されます。

例：

IDで指定したストレージバックエンドで検出を実行するには

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

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

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

SVMアグリゲートのマッピングの要件

データストアのプロビジョニングにSVMのユーザクレデンシャルを使用するため、ONTAP tools for VMware vSphereは、データストアのPOST APIで指定されたアグリゲートにボリュームを作成します。ONTAPでは、SVMユーザクレデンシャルを使用して、マッピングされていないアグリゲートにボリュームを作成することはできません。この問題を解決するには、ここで説明するONTAP REST APIまたはCLIを使用してSVMとアグリゲートをマッピングします。

ONTAP 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
```

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

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

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

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



上記のAPI応答のIDは検出で 사용됩니다。

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

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

vVolデータストアの作成

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



ルートアグリゲートがSVMにマッピングされていないことを確認します。

データストアを作成する前にJWTトークンを生成するか、vCenterで[Maximum Bearer Token Lifetime]を60mに設定してSAMLトークンの有効期限を延長します。

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

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

1. 新しいボリュームでvVolデータストアを作成する。

ONTAP REST APIを使用して、アグリゲートIDとストレージID（SVM UUID）を取得します。/virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vVols/datastores以降

次のURIを使用してステータスを確認します。

+

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

+ NFSデータストアのリクエスト本文

```
{"name": "nfsds1", "protocol": "nfs" AFF, "platform_type": "smolef": "domain-c8", "volumes": [
{"is_existing": false, "name": "vol_nfs_pvt", "size_in_mb": 2048000, "space_efficiency
```

iSCSIデータストアの要求本文: {"name": "iscsi_custom", "protocol" AFF: "iscsi", "platform_type": "domain-c8", "volumes": [{"is_existing": false, "name": "iscsi_custom": 8034, "space_efficiency": "thin", "-custom"- b-b"-b": "-feid": {""-b""": 5eid": 5ee": {""-feid": 5eid": {""-bree": {""-feid": {""-feid": {""-feid": {""-breeid": {""-breeid"} 既存のボリュームを使用してvVolデータストアを作成する。

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

```
POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores
リクエスト本文
```

```

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

```

vVolデータストアのマウントとアンマウント

VMware Virtual Volumes (vVol) データストアを1つ以上の追加ホストにマウントして、追加のホストにストレージアクセスを提供することができます。APIを使用してvVolデータストアをアンマウントできます。

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

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

```

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

```

vCenterからVVolデータストアMORefを取得します。

リクエスト本文

```

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

```

例：*追加ホストへのマウント

追加のホストにマウントするには、次のAPIを使用します。

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

Request Body

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

- 追加ホストでアンマウント

追加のホストでアンマウントするには、次のAPIを使用します。

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

Request Body

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

VVolデータストアのストレージの拡張または縮小

使用可能なストレージを増減するAPIが用意されています。

- 手順 *

vVolデータストアを拡張または縮小するには、次のAPIを使用します。

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

例

- 新しいボリュームを追加するためにvVolデータストアを変更する

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

Request Body

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

- 既存のボリュームを追加するためにvVolデータストアを変更する

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

Request Body

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

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

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

Request Body

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

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

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

Request Body

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

vVolデータストアの削除

vVolデータストアは、データストアで使用可能なFlexVol volumeが少なくとも1つ存在していれば削除されません。HAクラスタでvVolデータストアを削除する場合は、まずHAクラスタ内のすべてのホストからデータストアをアンマウントしてから、vCenterサーバのユーザインターフェイスを使用して_.vsphere-ha_folderを手動で削除します。

- 手順 *

vVolデータストアを削除するには、次のAPIを使用します。

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

例

- vVolデータストアの削除とストレージからのボリュームの削除

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



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

- vVolデータストアを削除し、ストレージからボリュームは削除しない

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

応答：

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

ストレージしきい値の管理

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

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

例：vCenter GUIDによるvCenter Serverインスタンスごとのストレージしきい値の取得

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

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

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

例：vCenter GUIDを使用してvCenterごとのストレージしきい値を更新します。デフォルトの制限は、「ほぼフル」が80%、「フル」が90%です。すべてのしきい値設定の変更

```

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

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

```

ネットワークアクセスの管理

次のAPIを使用して、ホワイトリストに追加するIPアドレスを指定します。

```

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

{
    value: string
}

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

{
    value: string
}

```

法的通知

法的通知では、著作権に関する声明、商標、特許などにアクセスできます。

著作権

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

商標

NetApp、NetAppのロゴ、およびNetAppの商標ページに記載されているマークは、NetApp、Inc.の商標です。その他の会社名および製品名は、それ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

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

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

プライバシーポリシー

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

オープンソース

通知ファイルには、ネットアップソフトウェアで使用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記載されています。

["ONTAP tools for VMware vSphere 10.1に関する注意事項"](#)

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。