



ONTAP tools for VMware vSphereのドキュメント

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

目次

ONTAP tools for VMware vSphereのドキュメント	1
リリース ノート	2
ONTAP toolsのリリースノート	2
ONTAP tools for VMware vSphere 10.5 の新機能	2
サポート対象の ONTAP プラットフォームとvCenter サーバーバージョン	3
ONTAP tools for VMware vSphere 9 と 10 の機能比較	3
概念	5
ONTAP toolsについて学ぶ	5
ONTAP toolsの主要な概念と用語	5
役割ベースアクセス制御 (RBAC)	8
ONTAP tools RBACについて学ぶ	9
VMware vSphere を使用した RBAC	10
ONTAP を使用した RBAC	17
ONTAP tools for VMware vSphere の導入	21
ONTAP tools for VMware vSphere のクイックスタート	21
ONTAP toolsの高可用性導入ワークフロー	23
ONTAP tools for VMware vSphere の要件と構成制限	24
システム要件	24
ストレージとアプリケーションの最小要件	24
ポートの要件	25
ONTAP tools for VMware vSphere を vVols データストアに導入する際の構成上の制限	27
VMFS および NFS データストア用の ONTAP tools for VMware vSphere を導入するための構成制限	27
ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA)	28
ONTAP toolsの導入前要件	29
展開ワークシート	29
ネットワークファイアウォールの設定	31
ONTAPストレージ設定	31
ONTAP Toolsの導入	31
ONTAP toolsの導入エラーのトラブルシューティング	37
ログ ファイルの収集	37
展開エラーコード	38
ONTAP Tools for VMware vSphereの設定	41
vCenter Server インスタンスを ONTAP tools に追加する	41
ONTAP tools で VASA Provider を vCenter Server インスタンスに登録する	42
ONTAP tools を使用して NFS VAAI プラグイン をインストールする	43
ONTAP toolsでESXiホストの設定を構成する	44
ESXiサーバーのマルチパスとタイムアウト設定を構成する	44
ESXiホストの値を設定する	45
ONTAP tools用のONTAPユーザーロールと権限を設定する	45

SVMアグリゲートマッピング要件	47
ONTAP ユーザーとロールを手動で作成する	47
ONTAP tools for VMware vSphere 10.1ユーザーから10.3ユーザーへのアップグレード	55
ONTAP tools for VMware vSphere 10.3ユーザーから10.4ユーザーへのアップグレード	57
ONTAP toolsにストレージバックエンドを追加する	58
ONTAP tools でvCenter Server インスタンスにストレージバックエンドを関連付ける	60
ONTAP tools でネットワーク アクセスを設定する	60
ONTAP toolsでデータストアを作成する	61
データストアと仮想マシンの保護	66
ONTAP toolsでホストクラスタを保護する	66
SRA保護を使用して保護する	67
データストアを保護するために ONTAP tools で SRA を設定する	67
SAN および NAS 環境向けの ONTAP tools で SRA を構成する	68
大規模環境向けに ONTAP tools で SRA を構成する	69
ONTAP tools を使用して VMware Live Site Recovery アプライアンスで SRA を構成する	70
ONTAP toolsでSRA認証情報を更新する	71
ONTAP toolsで保護サイトとリカバリサイトを構成する	72
保護対象サイトとリカバリ サイトのリソースの設定	74
ONTAP toolsで複製されたストレージシステムを検証する	78
ONTAP toolsのファンアウト保護	78
ONTAP tools for VMware vSphereの管理	82
ONTAP toolsダッシュボードについて学ぶ	82
ONTAP toolsがigroupとエクスポートポリシーを管理する方法	83
エクスポート ポリシー	87
ONTAP toolsによるigroupの管理方法	88
簡単な動作概要	88
igroupコンテキスト	89
命名の動作	90
シナリオ別の動作	90
カスタムigroupの再利用とAPIの動作	91
ネイティブからマネージドへの変換ビュー	91
検出されたネイティブigroupの再利用	92
ONTAP toolsマネージャのユーザーインターフェイスについて学ぶ	92
ONTAP tools Manager の設定を管理する	94
ONTAP toolsのAutoSupport設定を編集する	94
ONTAP toolsにNTPサーバーを追加する	95
ONTAP toolsでVASA ProviderとSRAの認証情報をリセットする	95
ONTAPツールのバックアップ設定を編集する	96
ONTAP toolsサービスを有効にする	96
ONTAP toolsアプライアンスの設定を変更する	97
VMware vSphereホストをONTAPツールに追加する	98

データストアの管理	99
ONTAP toolsでNFSおよびVMFSデータストアをマウントする	99
ONTAP toolsでNFSおよびVMFSデータストアをアンマウントする	99
ONTAP tools で vVols データストアをマウントする	100
ONTAP toolsでNFSおよびVMFSデータストアのサイズを変更する	101
ONTAP tools で vVols データストアを拡張する	101
ONTAP tools で vVols データストアを縮小する	101
ONTAP toolsでデータストアを削除する	102
ONTAP tools のデータストアの ONTAP ストレージ ビュー	103
ONTAP toolsの仮想マシンストレージビュー	104
ONTAP toolsでストレージしきい値を管理する	104
ONTAP toolsでストレージバックエンドを管理する	104
ストレージを検出する	104
ストレージバックエンドを変更する	105
ストレージバックエンドを削除する	105
ストレージバックエンドの詳細ビュー	106
ONTAP tools で vCenter Server インスタンスを管理する	107
ストレージバックエンドとvCenter Serverインスタンスの関連付けを解除する	107
vCenter Server インスタンスを変更する	107
vCenter Server インスタンスを削除する	107
vCenter Server 証明書の更新	108
ONTAP tools証明書の管理	110
ONTAP tools for VMware vSphere メンテナンスコンソールへのアクセス	112
ONTAP toolsのメンテナンスコンソールについて学ぶ	112
ONTAP toolsのリモート診断アクセスを設定する	113
他のONTAP toolsノードでSSHを起動します	114
ONTAP toolsでvCenter Serverのクレデンシャルを更新	114
ONTAP toolsで証明書検証フラグを変更する	114
ONTAP tools レポート	116
仮想マシンの管理	117
ONTAP toolsにおける仮想マシンの移行とクローン作成に関する考慮事項	117
ONTAP tools で仮想マシンを vVols データストアに移行する	118
ONTAP toolsでVASA構成をクリーンアップする	119
ONTAP toolsでVMにデータディスクを接続または切断する	119
ONTAP toolsでストレージシステムとホストを検出する	120
ONTAP Toolsを使用したESXiホストの設定の変更	121
パスワードの管理	121
ONTAP tools Manager パスワードの変更	121
ONTAP tools Manager のパスワードをリセット	122
ONTAP toolsでアプリケーションユーザーのパスワードをリセットする	122
ONTAP toolsのメンテナンスコンソールのパスワードをリセットする	122

ホストクラスタ保護の管理	124
ONTAP toolsで保護されたホストクラスタを変更する	124
ONTAP toolsでホストクラスタ保護を削除する	126
ONTAP tools のセットアップを復元する	127
ONTAP toolsをアンインストールする	128
ONTAP toolsをアンインストールした後、FlexVolボリュームを削除する	129
VMware vSphere 向け ONTAP tools のアップグレード	130
ONTAP tools for VMware vSphere 10.x から 10.5 へのアップグレード	130
ONTAP toolsのアップグレードエラーコード	132
ONTAP tools for VMware vSphere 9.xx から 10.5 への移行	138
ONTAP tools for VMware vSphere 9.xx から 10.5 への移行	138
VASA プロバイダーを移行し、ONTAP ツールで SRA を更新する	138
VASAプロバイダーを移行する手順	138
ストレージレプリケーションアダプタ (SRA) を更新する手順	143
REST API を使用した自動化	145
ONTAP tools REST APIについて学ぶ	145
基盤としてのREST Webサービス	145
ONTAP tools Manager環境	146
ONTAP tools REST API実装の詳細	146
REST API へのアクセス方法	146
HTTP の詳細	147
認証	148
同期リクエストと非同期リクエスト	148
最初のONTAP tools REST API呼び出しを実行する	149
開始する前に	149
ステップ1：アクセストークンを取得する	149
ステップ2：REST API呼び出しを発行する	150
ONTAP tools REST APIリファレンス	150
法律上の表示	151
著作権	151
商標	151
特許	151
プライバシー ポリシー	151
オープンソース	151

ONTAP tools for VMware vSphereのドキュメント

リリース ノート

ONTAP toolsのリリースノート

ONTAP tools for VMware vSphere 10.5で利用可能な新機能および強化された機能について説明します。

新機能と機能強化の完全なリストについては、[ONTAP tools for VMware vSphere 10.5 の新機能](#)を参照してください。

最新の互換性情報については、["NetApp Interoperability Matrix Tool"](#)を参照してください。

ONTAP tools for VMware vSphere 9.12D1、9.13D2、および 9.13P2 リリースから ONTAP tools for VMware vSphere 10.5 への移行がサポートされています。

詳細については、["ONTAP tools for VMware vSphere 10.5 リリースノート"](#)を参照してください。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 10.5 の新機能

ONTAP tools for VMware vSphere 10.5で利用可能な新機能について説明します。

- プラットフォーム資格

ONTAP tools for VMware vSphere 10.5では、ASA r2システムのサポートが追加され、最新のハードウェアおよびソフトウェア構成との互換性が提供されます。このリリースには、ONTAP 9.16.1および9.17.1との統合も含まれており、サポートされる環境が拡張されます。

- **VMware**の資格と認定

ONTAP tools for VMware vSphere 10.5 は、現在の VMware 相互運用性認証基準に準拠しており、ESXi ホストとvCenter Server の両方をサポートしています。

- **MetroCluster**サポート

今回のリリースでは、MetroCluster構成のサポートが導入され、高可用性とディザスタリカバリ機能が強化されました。

- セキュリティと証明書の管理

今回のリリースでは、自己署名証明書の管理が簡素化され、ユーザーエクスペリエンスとセキュリティ標準への準拠の両方が向上します。証明書検証ワークフローが改善され、ONTAP および ONTAP tools for VMware vSphere の通信が保護されます。

- レプリケーション機能の強化

このリリースでは、SRA および SnapMirror アクティブ同期を含む階層的整合性グループによる VMFS レプリケーションが ASA r2 システムでサポートされています。データ保護と復旧を向上させるため、RPO ゼロのバックアップをサポートしています。

- アップグレードと移行

以前のバージョンのONTAP tools for VMware vSphereからONTAP tools for VMware vSphere 10.5へのアップグレードおよび移行プロセスは、シームレスかつ効率的に動作するように設計されており、ダウンタイムを最小限に抑え、スムーズな移行を実現します。

サポート対象の **ONTAP** プラットフォームと**vCenter** サーバーバージョン

ONTAP tools for VMware vSphere 10.5 P1は、SRAおよびSnapMirror active syncコンポーネントのvCenter高可用性（HA）構成をサポートします。この構成ではvVolsはサポートされていません。HAフェイルオーバー中、vCenterが数分間利用できない場合があります。大規模な環境やエラーが発生した場合、フェイルオーバー時間が15分を超えることがあります。

詳細については、"[vCenter High Availabilityドキュメント](#)"を参照してください。vCenter HAに関するご質問は、"[Broadcomサポート](#)"までお問い合わせください。

バージョン互換性に関する最新情報については、"[NetApp Interoperability Matrix Tool](#)"を参照してください。

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

ONTAP tools for VMware vSphere 9 から ONTAP tools for VMware vSphere 10.2 以降のバージョンへの移行が適切かどうかをご確認ください。



最新の互換性情報については、"[NetApp Interoperability Matrix Tool](#)"を参照してください。

機能	ONTAP tools 9.13	ONTAP tools 10.2以降
主な価値提案	強化されたセキュリティ、コンプライアンス、自動化機能により、Day 0からDay 2の運用を合理化および簡素化します。	VMFS向けにFCのサポートを拡張し、VMFSのみにNVMe-oFのサポートを追加しました。NetApp SnapMirrorの使いやすさ、vSphereメトロストレージクラスタの簡単なセットアップ、および3サイトVMware Live Site Recoveryのサポート
ONTAPリリースの認定	ONTAP 9.9.1からONTAP 9.16.1	ONTAP tools 10.2 の場合は ONTAP 9.12.1 ~ 9.15.1。ONTAP tools 10.3 の場合は ONTAP 9.14.1、9.15.1、9.16.0、および 9.16.1。ONTAP tools 10.4 の場合は ONTAP 9.14.1、9.15.1、9.16.0、および 9.16.1。ASA r2 システムを使用する場合、ONTAP tools 10.4 には ONTAP 9.16.1P3 以降が必要です。ONTAP tools 10.5の場合、ONTAP 9.15.1、9.16.1、および9.17.0
VMware リリースサポート	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 から VMware Live Site Recovery 9.0	vSphere 7.x-8.x vSphere 9.0（ONTAP tools 10.5以降） VMware Site Recovery Manager (SRM) 8.7からVMware Live Site Recovery 9.0 注： ONTAP tools 10.xでは、SRMは共有サイトをサポートし、拡張性とパフォーマンスの向上を実現しています。

機能	ONTAP tools 9.13	ONTAP tools 10.2以降
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）	NFS および VMFS データストア: NFS （v3 および v4.1）、VMFS （iSCSI/FCP/NVMe-oF）
拡張性	ホストとVM：ホスト300台、VM最大10K台 データストア：NFS 600個、VMFS最大50個	ホストとVM：600ホスト
可観測性	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、動的なVMおよびデータストアレポート	パフォーマンス、容量、ホストコンプライアンスのダッシュボードを更新 動的なVMおよびデータストアレポート
データ保護	VMFSおよびNFS向けのSRAレプリケーション。SCVとの統合およびバックアップのための相互運用性。	iSCSI VMFSおよびNFS v3データストア向けのSRAレプリケーション、SMASとVMware Live Site Recoveryを組み合わせた3サイト保護。VMFSを使用したFCPのSRAサポート。
VASAプロバイダーサポート	VASA 4.0	VASA 3.0

概念

ONTAP toolsについて学ぶ

ONTAP tools for VMware vSphereは、仮想マシンのライフサイクル管理のためのツールセットです。VMware エコシステムと統合することで、データストアのプロビジョニングを簡素化し、仮想マシンに基本的な保護機能を提供します。これは、水平方向にスケラブルなイベント駆動型マイクロサービスの集合体であり、Open Virtual Appliance (OVA) としてデプロイされます。

ONTAP tools for VMware vSphere のサポート対象：

- 保護やディザスタリカバリなどのコア仮想マシン (VM) 機能
- ストレージのポリシーベース管理のためのVASAプロバイダー
- ストレージポリシーベースの管理
- Storage Replication Adapter (SRA)

VMware 向け ONTAP tools の高可用性

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

HAソリューションは、以下の種類の障害から迅速に復旧するのに役立ちます。

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

ONTAP tools for VMware vSphere の HA を有効にするために、追加の設定を行う必要はありません。



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

HA機能を使用するには、導入時またはVM設定でCPUホット アドとメモリ ホットプラグが有効になっていることを確認してください。

ONTAP toolsの主要な概念と用語

以下のセクションでは、この文書で使用されている主要な概念と用語について説明します。

認証局 (CA)

CAとは、Secure Sockets Layer (SSL) 証明書を発行する信頼できる機関のことです。

整合性グループ

整合性グループとは、単一の単位として管理されるボリュームの集合体です。整合性グループは、ストレージユニットおよびボリューム間でデータの一貫性を確保するために同期されます。ONTAPでは、複数のボリュームにまたがるアプリケーション ワークロードの管理と保護を容易に行うことができます。詳細はこちらをご覧ください ["整合性グループ"](#)。

デュアルスタック

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

高可用性 (HA)

クラスタノードは、無停止運用を実現するためにHA（高可用性）ペアで構成されます。

論理ユニット番号 (LUN)

LUNとは、ストレージエリアネットワーク (SAN) 内の論理単位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、Small Computer System Interface (SCSI) プロトコルまたはそのカプセル化された派生プロトコルを介してアクセスされる論理ディスクです。

NVMe名前空間およびサブシステム

NVMe ネームスペースとは、論理ブロックにフォーマット可能な不揮発性メモリの量のことです。ネームスペースは FC および iSCSI プロトコルにおける LUN に相当し、NVMe サブシステムは igroup に類似しています。NVMe サブシステムはイニシエータと関連付けることができ、関連付けられたイニシエータはサブシステム内のネームスペースにアクセスできるようになります。

ONTAP tools Manager

ONTAP tools ManagerはONTAP tools for VMware vSphere管理者に、管理対象のvCenter Serverインスタンスとオンボード済みストレージバックエンドに対するより高度な制御を提供します。vCenter Serverインスタンス、ストレージバックエンド、証明書、パスワード、ログバンドルの管理に役立ちます。

オープン仮想アプライアンス (OVA)

OVAは、仮想マシン上で実行する必要がある仮想アプライアンスまたはソフトウェアのパッケージ化および配布のためのオープン スタンドードです。

復旧目標時点 (RPO)

RPOは、データのバックアップまたは複製をどのくらいの頻度で行うかを示す指標です。これは、業務を再開するために、障害発生後にデータを復元する必要がある正確な時点を指定するものです。例えば、組織のRPO（目標復旧時点）が4時間であれば、災害発生時に最大4時間分のデータが失われても許容できるということになります。

SnapMirrorアクティブ同期

SnapMirror active sync により、完全なサイト障害が発生してもビジネスサービスが継続して動作できるようになり、セカンダリコピーを使用してアプリケーションを透過的にフェイルオーバーすることができま
す。SnapMirror active sync でフェイルオーバーをトリガーするために、手動介入やカスタムスクリプトは必

要ありません。詳細はこちらをご覧ください ["SnapMirrorアクティブ同期"](#)。

ストレージバックエンド

ストレージバックエンドとは、ESXiホストが仮想マシンファイル、データ、その他のリソースを保存するために使用する基盤となるストレージインフラストラクチャのことです。これらにより、ESXiホストは永続データにアクセスして管理できるようになり、仮想化環境に必要なストレージ機能とパフォーマンスが提供されます。

グローバルクラスター（ストレージバックエンド）

グローバルストレージバックエンドは、ONTAPクラスター認証情報でのみ使用可能で、ONTAP tools Managerインターフェースからオンボーディングされます。これらは最小限の権限で追加でき、vVols管理に必要な重要なクラスターリソースの検出を可能にします。vVols管理に必要な重要なクラスターリソースの検出を可能にします。グローバルクラスターは、SVMユーザーがvVols管理のためにローカルに追加されるマルチテナントシナリオに最適です。

ローカルストレージバックエンド

クラスターまたはSVM認証情報を持つローカルストレージバックエンドは、ONTAP toolsのユーザーインターフェースを通じて追加され、vCenterに限定されます。ローカルでクラスター認証情報を使用する場合、関連付けられたSVMは自動的にvCenterにマッピングされ、vVolsまたはVMFSを管理します。SRAを含むVMFS管理については、ONTAP toolsはグローバルクラスターを必要とせずにSVM認証情報をサポートします。

Storage Replication Adapter（SRA）

SRAは、VMware Live Site Recoveryアプライアンス内にインストールされている、ストレージベンダー固有のソフトウェアです。このアダプタは、Site Recovery Managerとストレージコントローラ間の通信を、Storage Virtual Machine（SVM）レベルおよびクラスターレベルの構成において可能にします。

ストレージ仮想マシン（SVM）

SVMは、ONTAPにおけるマルチテナンシーの単位です。ハイパーバイザー上で実行される仮想マシンと同様に、SVMは物理リソースを抽象化する論理エンティティです。SVMには、データボリュームと、クライアントにデータを提供する1つ以上のLIFが含まれています。

均一な構成と非均一な構成

- ***均一ホストアクセス***とは、2つのサイトのホストが、両サイトのストレージクラスターへのすべてのパスに接続されていることを意味します。サイト間パスは、距離をまたいで延伸されています。
- ***非均一ホストアクセス***とは、各サイトのホストが同じサイト内のクラスターにのみ接続されることを意味します。サイト間パスとストレッチパスは接続されていません。



均一なホストアクセスは、すべてのSnapMirrorアクティブ同期構成でサポートされます。不均一なホストアクセスは、対称アクティブ/アクティブ構成でのみサポートされます。詳細はこちらをご覧ください ["SnapMirror active sync の ONTAP における概要"](#)。

Virtual Machine File System（VMFS）

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

仮想ボリューム（vVols）

vVolsは、仮想マシンが使用するストレージに対して、ボリュームレベルの抽象化を提供します。これにはいくつかの利点があり、従来のLUNを使用する代替手段となります。vVolデータストアは通常、vVolsのコンテナとして機能する単一のLUNに関連付けられています。

VMストレージポリシー

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

VMware Live Site Recovery

VMware Live Site Recovery（旧称：Site Recovery Manager（SRM））は、VMware仮想環境向けに、事業継続性、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、管理および運用のためにストレージアレイをvCenter Serverと統合する一連の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プロバイダを含む、いくつか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APIセットです。APIには、ホストがストレージ操作をアレイにオフロードするために使用する一連の基本操作が含まれています。VAAIは、ストレージを大量に消費するタスクにおいて、大幅なパフォーマンス向上をもたらすことができます。

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster（vMSC）は、ストレッチ クラスター展開で vSphere を有効化およびサポートするアーキテクチャです。vMSC ソリューションは、NetApp MetroCluster および SnapMirror アクティブ同期（旧称 SMBC）でサポートされています。これらのソリューションは、ドメイン障害が発生した場合のビジネス継続性を強化します。回復力モデルは、お客様による具体的な構成選択に基づいて決定されます。詳細はこちらをご覧ください ["VMware vSphere メトロストレージクラスター"](#)。

vVolsデータストア

vVolsデータストアは、VASAプロバイダーによって作成および保守されるvVolsコンテナの論理的な表現です。

RPOゼロ

RPOとはリカバリーポイント目標の略で、一定期間内に許容できるとみなされるデータ損失量のことを指します。RPOゼロとは、データ損失が一切許容されないことを意味します。

役割ベースアクセス制御（RBAC）

ONTAP tools RBACについて学ぶ

ロールベースアクセス制御（RBAC）は、組織内のリソースへのアクセスを制御するためのセキュリティフレームワークです。RBACは、個々のユーザーに権限を割り当てるのではなく、アクションを実行するための特定の権限レベルを持つロールを定義することで、管理を簡素化します。定義されたロールはユーザーに割り当てられるため、エラーのリスクを軽減し、組織全体のアクセス制御の管理を簡素化するのに役立ちます。

RBAC標準モデルは、複雑さが増していく複数の実装技術またはフェーズで構成されています。その結果、実際のRBACの導入は、ソフトウェアベンダーとその顧客のニーズに基づいて異なり、比較的単純なものから非常に複雑なものまで多岐にわたる可能性があります。

RBACコンポーネント

大まかに言うと、RBACの実装には一般的にいくつかの構成要素が含まれています。これらの構成要素は、認可プロセスを定義する一環として、さまざまな方法で結び付けられています。

権限

特権とは、許可または拒否できるアクションまたは機能のことです。ファイルの読み取り機能のような単純なものである場合もあれば、特定のソフトウェア システムに固有のより抽象的な操作である場合もあります。Privilegesを定義して、REST APIエンドポイントおよびCLIコマンドへのアクセスを制限することもできます。すべてのRBAC実装には事前定義された特権が含まれており、管理者がカスタム特権を作成できる場合もあります。

ロール

ロールとは、1つ以上の権限を含むコンテナです。ロールは一般的に、特定の業務や職務内容に基づいて定義されます。ユーザーにロールが割り当てられると、そのユーザーにはそのロールに含まれるすべての権限が付与されます。権限と同様に、実装には事前定義されたロールが含まれており、一般的にはカスタムロールの作成も可能です。

オブジェクト

オブジェクトとは、RBAC環境内で識別される、現実のリソースまたは抽象的なリソースを表します。権限によって定義されたアクションは、関連付けられたオブジェクトに対して、または関連付けられたオブジェクトを使用して実行されます。実装方法によっては、オブジェクトタイプ全体または特定のオブジェクトインスタンスに対して権限を付与することができます。

ユーザとグループ

認証後、ユーザーには役割が割り当てられるか、役割に関連付けられます。RBACの実装によっては、ユーザーに割り当てられる役割が1つだけの場合もあれば、ユーザーごとに複数の役割を割り当てられるものの、同時にアクティブにできる役割は1つだけという場合もあります。グループに役割を割り当てることで、セキュリティ管理をさらに簡素化できます。

権限

権限とは、ユーザーまたはグループと役割をオブジェクトに関連付ける定義のことです。権限は、階層構造を持つオブジェクトモデルにおいて、階層内の子オブジェクトにオプションで継承させることができるため、非常に役立ちます。

2つのRBAC環境

ONTAP tools for VMware vSphere 10を使用する際には、考慮すべき2つの異なるRBAC環境がありま

す。ONTAP tools for VMware vSphere 10では、操作を実行するためにvCenterとONTAPの両方で特定の権限が必要です。ONTAP toolsはストレージ管理タスクを自動化しますが、vCenterまたはONTAPのいずれにもユーザーアカウントを作成しません。サービスアカウントは、必要に応じてvSphere管理者が作成する必要があります。このドキュメントでは、管理者が効果的なONTAP tools管理のために必要なロールと権限を割り当てるためのガイダンスを提供します。

VMware vCenter Server

VMware vCenter Server におけるRBACの実装は、vSphere Client ユーザーインターフェースを通じて公開されているオブジェクトへのアクセスを制限するために使用されます。ONTAP tools for VMware vSphere 10 のインストールの一環として、RBAC環境はONTAP toolsの機能を表す追加のオブジェクトを含むように拡張されます。これらのオブジェクトへのアクセスはリモートプラグインを通じて提供されます。詳細については、"[vCenter Server RBAC環境](#)"を参照してください。

ONTAP クラスター

ONTAP tools for VMware vSphere 10は、ONTAP REST APIを通じてONTAPクラスターに接続し、ストレージ関連の操作を実行します。ストレージリソースへのアクセスは、認証時に提供されたONTAPユーザーに関連付けられたONTAPロールによって制御されます。詳細については、"[ONTAP RBAC環境](#)"を参照してください。

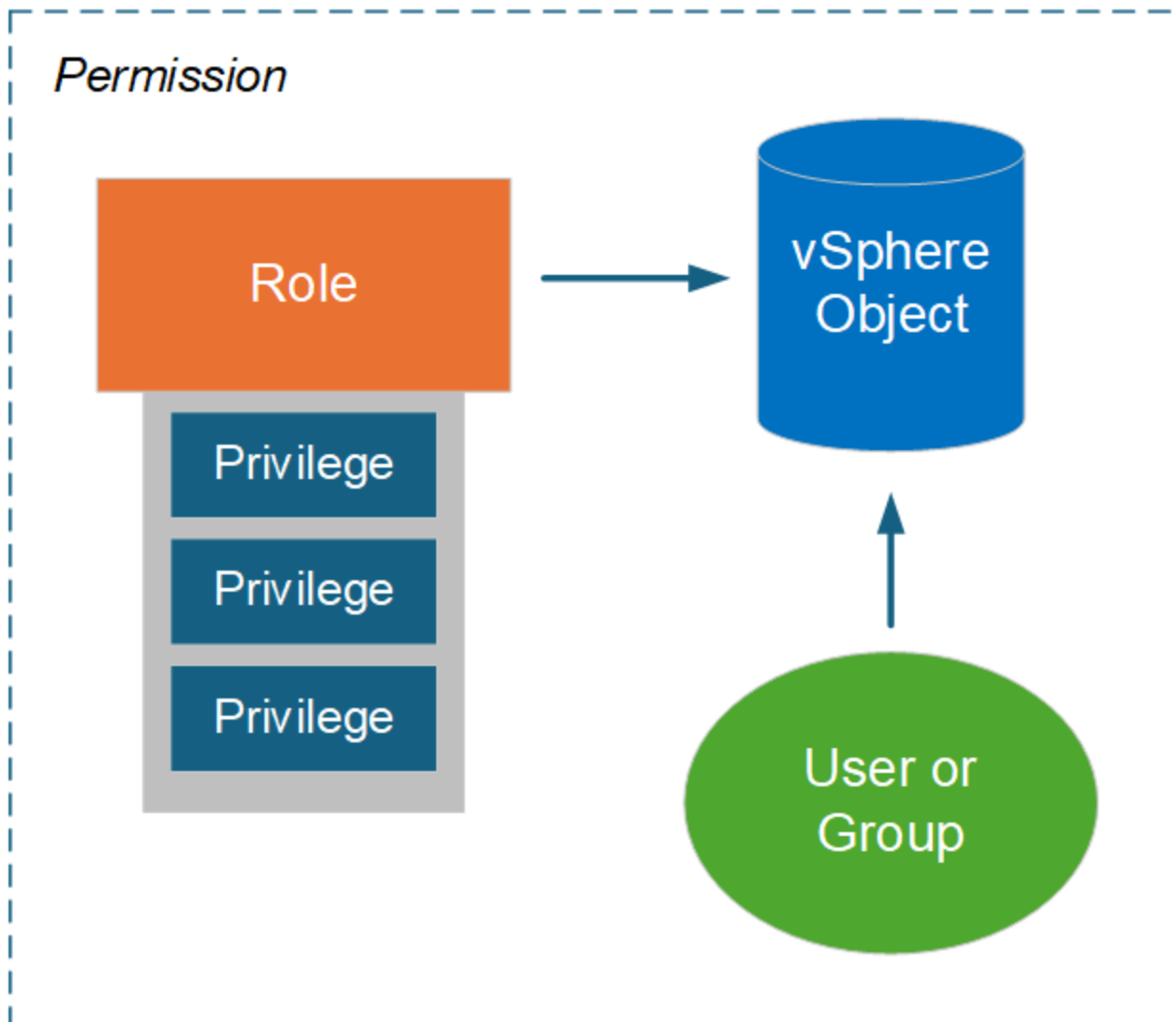
VMware vSphere を使用した RBAC

vCenter Server RBAC と ONTAP tools の連携

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

vCenter Server 権限のイラスト

許可は、vCenter Server 環境でアクセス制御を適用するための基盤です。許可定義にユーザーまたはグループを含む vSphere オブジェクトに適用されます。vCenter 許可の概要を示す図を以下に示します。



vCenter Server 権限の構成要素

vCenter Server 権限は、権限が作成される際に結合される複数のコンポーネントのパッケージです。

vSphereオブジェクト

権限は、vSphere オブジェクト（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）に関連付けられています。オブジェクトに割り当てられた権限に基づいて、vCenter Server は、各ユーザーまたはグループがオブジェクトに対して実行できるアクションまたはタスクを決定します。ONTAP tools for VMware vSphere に固有のタスクについては、すべての権限が vCenter Server のルートまたはルートフォルダレベルで割り当てられ、検証されます。詳細については、["RBACを使用するvCenter サーバ"](#) を参照してください。

Privileges とロール

ONTAP tools for VMware vSphere 10 で使用される vSphere の権限には、2 種類あります。この環境での RBAC の操作を簡素化するために、ONTAP tools は、必要なネイティブ権限とカスタム権限を含むロールを提供します。権限には以下が含まれます：

- vCenter Server標準の権限

これらは、vCenter Server が提供する Privileges です。

- ONTAP Tools固有の権限

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

ユーザとグループ

Active Directory またはローカルの vCenter Server インスタンスを使用してユーザーとグループを定義できます。ロールと組み合わせることで、vSphere オブジェクト階層内のオブジェクトに対する権限を作成できます。この権限は、関連付けられたロールにおける権限に基づいてアクセスを許可します。ロールはユーザーに単独で直接割り当てられるものではないことに注意してください。代わりに、ユーザーとグループは、より大きな vCenter Server 権限の一部として、ロール権限を通じてオブジェクトへのアクセス権を取得します。

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

ONTAP tools for VMware vSphere 10 の RBAC 実装には、vCenter Server を本番環境で使用する前に考慮すべきいくつかの側面があります。

vCenter のロールと管理者アカウント

カスタム vCenter Server ロールを定義して使用する必要があるのは、vSphere オブジェクトおよび関連する管理タスクへのアクセスを制限する場合のみです。アクセスを制限する必要がない場合は、代わりに管理者アカウントを使用できます。各管理者アカウントは、オブジェクト階層の最上位レベルで管理者ロールが定義されています。これにより、ONTAP tools for VMware vSphere 10 によって追加されたオブジェクトを含む、vSphere オブジェクトへのフルアクセスが提供されます。

vSphereオブジェクト階層

vSphereオブジェクトインベントリは階層構造で整理されています。例えば、以下のように階層を下っていくことができます。

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

すべての権限は、VAAI プラグイン操作を除く vSphere オブジェクト階層で検証されます。VAAI プラグイン操作は、対象の ESXi ホストに対して検証されます。

ONTAP tools for VMware vSphere 10 に含まれるロール

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



必要に応じて、新しいカスタムロールを作成できます。そのためには、既存のONTAP toolsロールの1つをクローニングし、必要に応じて編集します。構成変更後、影響を受けるvSphereクライアントユーザーは、変更を有効にするために一度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 のロールを表示するには、vSphere Client の上部にある **Menu** を選択し、**Administration** をクリックしてから、左側の **Roles** をクリックします。以下の権限は、vCenter Server

の導入またはオンボーディングを担当する vCenter ユーザに割り当てられたロールに含める必要があります。これらの権限が、導入またはオンボーディング プロセスの前提条件として設定されていることを確認してください。

- アラーム
 - 警報を確認する
- コンテンツライブラリ
 - ライブラリアイテムを追加
 - テンプレートでチェックイン
 - テンプレートを確認する
 - ファイルをダウンロード
 - ストレージのインポート
 - ストレージを読み取る
 - ライブラリアイテムを同期する
 - 購読ライブラリを同期する
 - 設定を表示する
- データストア
 - Allocate space
 - Browse datastore
 - Low level file operations
 - Remove file
 - Update virtual machine files
 - 仮想マシンのメタデータを更新する
- ESX Agent Manager
 - View
- フォルダ
 - フォルダを作成
- ホスト
 - 構成
 - 詳細設定
 - 設定の変更
 - ネットワーク設定
 - System resources
 - 仮想マシンの自動起動構成
 - ローカル操作
 - Create virtual machine

- Delete virtual machine
 - Reconfigure virtual machine
- Network
 - Assign network
 - 設定
- OvfManager
 - OvfConsumer アクセス
- ホストプロファイル
 - View
- リソース
 - Assign virtual machine to resource pool
- スケジュールされたタスク
 - タスクを作成する
 - タスクの変更
 - タスクを実行する
- タスク
 - タスクを作成する
 - タスクの更新
- vApp
 - 仮想マシンを追加する
 - リソース プールの割り当て
 - vApp の割り当て
 - 作成
 - インポート
 - Move
 - Power off
 - Power on
 - URLから取得
 - OVF環境の表示
- 仮想マシン
 - 構成の変更
 - Add existing disk
 - Add new disk
 - Add or remove device
 - 高度な設定

- Change CPU count
- メモリの変更
- Change Settings
- Change resource
- Extend virtual disk
- Modify device settings
- Remove disk
- ゲスト情報をリセットする
- Upgrade virtual machine compatibility
- 在庫を編集
 - Create from existing
 - Create new
 - Move
 - 登録
 - 削除
 - 登録解除
- インタラクション
 - 仮想マシン上でのバックアップ操作
 - Configure CD media
 - Configure floppy media
 - デバイスを接続する
 - コンソール操作
 - VIX API によるゲストオペレーティングシステム管理
 - Power off
 - Power on
 - リセット
 - 中断
- プロビジョニング
 - Allow disk access
 - Clone template
 - ゲストをカスタマイズ
 - Deploy template
 - カスタマイズ仕様の変更
 - Read customization specifications
- Snapshotの管理
 - Snapshot の作成

- Remove snapshot
- スナップショットの名前を変更する
- Revert to snapshot

以下に説明するように、あらかじめ定義された3つのロールがあります。

NetApp ONTAP tools for VMware vSphere 管理者

すべてのネイティブ vCenter Server の Privileges と、VMware vSphere 管理者タスクのコア ONTAP tools for VMware を実行するために必要な ONTAP tools 固有の Privileges を提供します。

NetApp ONTAP tools for VMware vSphere 読み取り専用

ONTAP tools への読み取り専用アクセスを提供します。これらのユーザーは、アクセス制御された ONTAP tools for VMware vSphere の操作を実行できません。

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ネイティブの vCenter Server Privileges の一部と ONTAP tools 固有の Privileges を提供します。以下のタスクを実行できます：

- 新しいデータストアの作成
- データストアの管理

vSphereオブジェクトとONTAPストレージバックエンド

これら2つのRBAC環境は連携して動作します。vSphereクライアントインターフェースでタスクを実行する際、vCenter Serverに定義されたONTAPツールのロールが最初にチェックされます。操作がvSphereによって許可されている場合、ONTAPロールの権限が確認されます。この2番目のステップは、ストレージバックエンドの作成および構成時にユーザーに割り当てられたONTAPロールに基づいて実行されます。

vCenter Server RBAC の操作

vCenter Server の権限とアクセス許可を使用する際には、いくつか考慮すべき点があります。

必要な権限

ONTAP tools for VMware vSphere 10 のユーザーインターフェースにアクセスするには、ONTAPツール固有の「表示」権限が必要です。vSphere にこの権限なしでサインインして NetApp アイコンをクリックすると、ONTAP tools for VMware vSphere はエラーメッセージを表示し、ユーザーインターフェースへのアクセスを禁止します。

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

代わりに、別の下位の vSphere オブジェクトレベルに「表示」権限を割り当てることができます。ただし、これにより、アクセスして使用できる ONTAP tools for VMware vSphere のメニューが制限されます。

アクセス許可の割り当て

vSphereオブジェクトおよびタスクへのアクセスを制限する場合は、vCenter Serverの権限を使用する必要があります。vSphereオブジェクト階層のどの位置に権限を割り当てるかによって、ユーザーが実行でき

るONTAP tools for VMware vSphere 10のタスクが決まります。



より制限的なアクセス権限を定義する必要がない限り、一般的にはルートオブジェクトまたはルートフォルダのレベルで権限を割り当てておくことをお勧めします。

ONTAP tools for VMware vSphere 10 で使用可能な権限は、ストレージシステムなどのカスタム非 vSphere オブジェクトに適用されます。可能であれば、割り当て先となる vSphere オブジェクトが存在しないため、これらの権限は ONTAP tools for VMware vSphere のルートオブジェクトに割り当てておくことをお勧めします。たとえば、ONTAP tools for VMware vSphere の「ストレージシステムの追加/変更/削除」権限を含む権限は、ルートオブジェクトレベルで割り当てておく必要があります。

オブジェクト階層の上位レベルで権限を定義する場合、その権限が下位レベルに渡され、子オブジェクトに継承されるように構成できます。必要に応じて、子オブジェクトに追加の権限を割り当てて、親オブジェクトから継承された権限を上書きすることができます。

権限はいつでも変更できます。権限内の Privileges を変更すると、その権限に関連付けられているユーザーは vSphere からログアウトし、変更を有効にするために再度ログインする必要があります。

ONTAP を使用した RBAC

ONTAP RBAC が ONTAP tools と連携する仕組み

ONTAPは、堅牢で拡張性の高いRBAC環境を提供します。RBAC機能を使用して、REST APIおよびCLIを通じて公開されるストレージおよびシステム操作へのアクセスを制御できます。ONTAP tools for VMware vSphere 10の展開で使用する前に、この環境に慣れておくことをお勧めします。

管理オプションの概要

環境と目標に応じて、ONTAP RBAC を使用する際に利用できるオプションがいくつかあります。以下に、主要な管理上の決定事項の概要を示します。詳細については、["ONTAP Automation：RBACセキュリティの概要"](#)も参照してください。



ONTAP RBACはストレージ環境に合わせて調整されており、vCenter Serverに付属のRBAC実装よりもシンプルです。ONTAPでは、ユーザーに役割を直接割り当てます。vCenter Serverで使用されるような明示的な権限の設定は、ONTAP RBACでは不要です。

役割と権限の種類

ONTAPユーザーを定義する際には、ONTAPロールが必要です。ONTAPロールには2種類あります：

- REST

REST ロールは ONTAP 9.6 で導入され、REST API を通じて ONTAP にアクセスするユーザーに一般的に適用されます。これらのロールに含まれる権限は、ONTAP REST API エンドポイントおよび関連するアクションへのアクセスという観点から定義されます。

- 従来型

これらは、ONTAP 9.6 より前に存在していたレガシーロールです。これらは RBAC の根幹を成す要素であり続けています。権限は、ONTAP CLI コマンドへのアクセスに関して定義されます。

RESTロールは比較的最近導入されたものですが、従来のロールにもいくつかの利点があります。たとえば、追加のクエリパラメータを含めることで、権限が適用されるオブジェクトをより正確に定義できるようになります。

Scope

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

役割の定義

ONTAPは、クラスターレベルとSVMレベルの両方で、事前定義された一連のロールを提供します。カスタムロールを定義することもできます。

ONTAP REST ロールの操作

ONTAP tools for VMware vSphere 10 に含まれる ONTAP REST ロールを使用する際には、いくつかの考慮事項があります。

役割マッピング

従来型ロールでもRESTロールでも、すべてのONTAPアクセス権限の決定は、基となるCLIコマンドに基づいて行われます。ただし、RESTロールの権限はREST APIエンドポイントの観点で定義されているため、ONTAPは各RESTロールに対してマッピングされた従来のロールを作成する必要があります。したがって、各RESTロールは基盤となる従来のロールに対応付けられます。これにより、ONTAPはロールの種類に関係なく、一貫した方法でアクセス制御の決定を行うことができます。並列マッピングされたロールは変更できません。

CLI権限を使用してRESTロールを定義する

ONTAPは常にCLIコマンドを使用して基本レベルでのアクセスを決定するため、RESTエンドポイントの代わりにCLIコマンドの権限を使用してRESTロールを表現することが可能です。このアプローチの利点の1つは、従来のロールで利用できる詳細な設定が可能になることです。

ONTAPロールを定義する際の管理インターフェース

ユーザーとロールは、ONTAP CLI と REST API を使用して作成できます。ただし、ONTAP tools Manager から入手できる JSON ファイルとともに System Manager インターフェースを使用する方が便利です。詳細については、["ONTAP tools for VMware vSphere 10 で ONTAP RBAC を使用する"](#)を参照してください。

ONTAP tools に関する ONTAP RBAC の考慮事項

ONTAP tools for VMware vSphere 10 の ONTAP との RBAC 実装には、本番環境で使用する前に考慮すべきいくつかの側面があります。

設定プロセスの概要

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

主な設定手順の概要を以下に説明します。詳細については、["ONTAP ユーザーロールと権限の設定"](#)を参照してください。

1. 準備

ONTAP tools Manager と ONTAP クラスターの両方に管理者資格情報が必要です。

2.JSON定義ファイルをダウンロードする

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

3.ロールを持つ ONTAP ユーザーを作成する

システムマネージャーにサインインした後、ユーザーとロールを作成できます。

1. 左側の「クラスター」を選択し、次に「設定」を選択します。
2. 「ユーザーとロール」までスクロールダウンして「→」をクリックします。
3. 「ユーザー」の下にある「追加」を選択し、「仮想化製品」を選択します。
4. ローカルワークステーション上のJSONファイルを選択してアップロードしてください。

4.役割を設定する

役割を定義する過程で、いくつかの管理上の決定を下す必要があります。詳細については、[\[システムマネージャーを使用してロールを設定する\]](#)を参照してください。

システムマネージャーを使用してロールを設定する

システムマネージャーを使用して新しいユーザーとロールの作成を開始し、JSONファイルをアップロードした後、環境とニーズに基づいてロールをカスタマイズできます。

コアユーザーとロールの設定

RBACの定義は、VSC、VASAプロバイダー、SRAの組み合わせなど、いくつかの製品機能としてパッケージ化されています。RBACサポートが必要な環境を選択してください。例えば、リモートプラグイン機能をサポートするロールが必要な場合は、VSCを選択します。ユーザー名とそれに関連付けられたパスワードも選択する必要があります。

権限

ロール権限は、ONTAP ストレージに必要なアクセス レベルに基づいて 4 つのセットに分けられています。ロールの基となる権限には次のものがあります：

- Discovery

ストレージ システムを追加できます。

- ストレージの作成

このロールにより、ストレージを作成できます。また、検出ロールに関連付けられたすべての権限も含まれます。

- ストレージを変更する

この役割により、ストレージを変更できます。また、ストレージロールの検出および作成に関連するすべての権限も含まれます。

- ストレージを削除する

このロールを使用すると、ストレージを削除できます。また、ストレージの検出、作成、および変更とい

ったロールに関連するすべての権限も含まれます。

役割を持つユーザーを生成する

環境の構成オプションを選択したら、「追加」をクリックすると、ONTAPによってユーザーとロールが作成されます。生成されるロールの名前は、以下の値を連結したものです。

- JSONファイルで定義された定数プレフィックス値（例：「OTV_10」）
- 選択した製品機能
- 権限セットの一覧。

例

OTV_10_VSC_Discovery_Create

新しいユーザーは、「ユーザーと役割」ページの一覧に追加されます。HTTPとONTAPIの両方のユーザーログイン方法がサポートされていることに注意してください。

ONTAP tools for VMware vSphere の導入

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

このクイックスタートセクションを参照して、VMware vSphere 向け ONTAP tools for VMware vSphere をセットアップしてください。

まずこれらのコアタスクを完了して、ONTAP tools を Day-0 の管理およびプロビジョニングに対応できる状態にしてください。次に、環境および保護要件に基づいて、オプションのタスクを完了してください。

最初に、NFS および VMFS データストアをサポートするコアサービスを提供する小規模なシングルノード構成として、ONTAP tools for VMware vSphere を導入します。サービスごとのコンテナを追加したり、回復性を強化したり、vVols データストアと高可用性（HA）を使用したりするために構成を拡張するには、まずこのワークフローを完了してから、拡張手順に進んでください。詳細については、["HA展開ワークフロー"](#)を参照してください。

1

デプロイメントの計画

お使いの環境が、サポートされているデプロイメントに対応できる状態であることを確認してください。vSphere、ONTAP、および ESXi ホストのバージョンが ONTAP tools のバージョンと互換性があることを確認してください。十分な CPU、メモリ、およびディスク容量を確保してください。セキュリティルールによっては、ファイアウォールやその他のセキュリティツールを設定して、ネットワークトラフィックを許可する必要がある場合があります。

vCenter Server がインストールされており、アクセス可能であることを確認してください。

- ["Interoperability Matrix Tool"](#)
- ["ONTAP tools for VMware vSphere の要件と構成制限"](#)
- ["始める前に"](#)

2

ONTAP tools for VMware vSphere を導入する

NFS および VMFS データストアの基本サービスを確立するために ONTAP tools アプライアンスを導入します。

最初に、ONTAP tools for VMware vSphere を小規模なシングルノード構成としてデプロイします。構成を拡張して vVols データストアと高可用性（HA）を使用する予定がある場合は、このワークフローを完了した後に行います。HA 構成に拡張するには、CPU ホットアドとメモリのホットプラグが有効になっていることを確認してください。

デプロイ中は、カスタマイズ テンプレート フィールド、特にホスト名、ONTAP tools の IP アドレスの使用状況、および DNS 要件を注意深く確認してください。

- ["ONTAP tools for VMware vSphere の導入"](#)

3

vCenter クライアント プラグイン の登録とインストール

vCenter クライアント プラグインを登録し、必要な権限とロールを適用するには、vCenter Server インスタンスを追加します。vCenter Server インスタンスを追加すると、ONTAP tools はリモート プラグインを登録し、カスタム プラグインおよび API 権限を適用し、カスタムロールを作成して、vSphere ユーザーインターフェイスにプラグインのショートカットを追加します。

- ["vCenter Server インスタンスを ONTAP tools に追加する"](#)

4

ストレージバックエンドを設定する

ONTAP ストレージリソースを接続して、ONTAP tools がデータストアをプロビジョニングおよび管理できるようにします。ストレージバックエンドを ONTAP クラスタに追加します。マルチテナント環境で vCenter Server がテナント SVM に関連付けられている場合は、ONTAP tools Manager を使用してクラスタを追加します。次に、ストレージバックエンドを vCenter Server に関連付けて、その vCenter インスタンスのグローバルマッピングを作成します。

ONTAP tools のユーザーインターフェースを使用して、クラスターまたは SVM の認証情報でローカルストレージバックエンドを追加します。これらのストレージバックエンドは、単一の vCenter に限定されます。ローカルでクラスター認証情報を使用する場合、関連付けられた SVM は自動的に vCenter にマッピングされ、vVols または VMFS を管理します。SRA を含む VMFS 管理については、ONTAP tools はグローバルクラスターを必要とせずに SVM 認証情報をサポートします。

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

オプションの次のタスク

1

ONTAP ユーザーロールと権限の設定

デフォルトの管理者アカウントではなく、最小権限アクセスのためのカスタム ONTAP ロールを設定します。

- ["ONTAP ユーザーロールと権限の設定"](#)

2

複数の vCenter Server インスタンスの証明書をアップグレードする

複数の vCenter Server インスタンス間で信頼できる証明書ベースの通信を使用するために証明書をアップグレードします。

- ["証明書の管理"](#)

3

SRA保護の設定

SRA機能を有効にして、NFSおよびVMFSデータストアのディザスタリカバリ保護を設定します。

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

4

SnapMirror アクティブ同期保護を有効にする

VMFSデータストアを保護するために、SnapMirror active syncを使用してホストクラスター保護をセットアップします。ONTAPシステムで、必要なクラスターとSVMをピアリングし、ONTAP tools for VMware vSphereでホストクラスター保護を構成します。このオプションはVMFSデータストアにのみ適用されます。

- ["ホストクラスター保護を使用して保護する"](#)

5

ONTAP tools の導入環境のバックアップとリカバリを設定する

バックアップとリカバリを設定して ONTAP tools の構成を保護し、障害発生時に迅速に復旧できるようにします。

バックアップはONTAP tools for VMware vSphere 10.5でデフォルトで有効になっており、10分ごとに実行されます。障害発生時にセットアップを復元するために使用できる、ONTAP tools for VMware vSphereのセットアップのバックアップをスケジュールします。

- ["バックアップ設定を編集する"](#)
- ["ONTAP tools のセットアップを復元する"](#)

ONTAP toolsの高可用性導入ワークフロー

回復力を高め、サービスごとにサポートするコンテナ数を増やすには、初期の ONTAP tools デプロイメントを高可用性（HA）構成に拡張してください。HA セットアップの vVols データストアには、VASA Provider サービスを有効にする必要があります。

1

展開規模を拡大する

ONTAP tools for VMware vSphere の設定をスケールアップして、デプロイメント内のノード数を増やし、構成を HA セットアップに変更できます。

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

2

サービスを有効にする

vVolsデータストアを設定するには、VASAプロバイダーサービスを有効にする必要があります。VASAプロバイダーをvCenterに登録し、適切なネットワーク構成とストレージ構成を含め、ストレージポリシーがHAの要件を満たしていることを確認してください。

SRAサービスを有効にして、VMware Site Recovery Manager（SRM）またはVMware Live Site Recovery（VLSR）向けのONTAP tools Storage Replication Adapter（SRA）を使用します。

- ["VASAプロバイダーおよびSRAサービスを有効にする"](#)

3

証明書をアップグレードする

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

ONTAP tools for VMware vSphere の要件と構成制限

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

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ホストを含むサポートされているvSphere環境に導入する必要があります。

システム要件

- ノードごとのインストールパッケージの必要容量
 - 15GB - シンプロビジョニングの場合
 - 348GB - シックプロビジョニングの場合
- ホストシステムのサイジング要件 下の表は、各デプロイメントサイズに推奨されるメモリ容量を示しています。高可用性 (HA) 構成の場合、記載されているアプライアンスサイズの3倍の容量が必要です。

展開の種類	ノードあたりのCPU数	ノードあたりのメモリ容量 (GB)	ノードごとにシックプロビジョニングされるディスク容量 (GB)
小規模	9	18	350
中	13	26	350
Large NOTE：大規模展開はHA構成のみを対象としています。	17	34	350



バックアップが有効になっている場合、各 ONTAP tools クラスターには、VM がデプロイされるデータストア上にさらに 50 GB の空き容量が必要です。したがって、非 HA 構成では 400 GB、HA 構成では合計 1100 GB の容量が必要となります。

ストレージとアプリケーションの最小要件

ストレージ、ホスト、およびアプリケーション	バージョン要件
ONTAP	9.15.1、9.16.1、および9.17.0
ONTAP tools でサポートされている ESXi ホスト	7.0.3以降
ONTAP tools がサポートする vCenter Server	7.0U3以降
VASA Provider	3.0
OVAアプリケーション	10.5
ONTAP tools 仮想マシンをデプロイする ESXi ホスト	7.0U3と8.0U3
vCenter Server：ONTAP tools 仮想マシンのデプロイ先	7.0 と 8.0



ONTAP tools for VMware vSphere 10.4 以降、仮想マシンのハードウェアはバージョン 10 から 17 に変更されました。

相互運用性マトリックスツール（IMT）には、サポートされているバージョンのONTAP、vCenter Server、ESXiホスト、およびプラグイン アプリケーションに関する最新情報が含まれています。

["Interoperability Matrix Tool"](#)

ポートの要件

次の表は、NetApp が使用するネットワークポートとその目的の概要を示しています。ポートには3つの異なる種類があります。

- 外部ポート：これらのポートは、Kubernetesクラスタまたはノードの外部からアクセスできます。これらにより、サービスが外部ネットワークやユーザーと通信できるようになり、クラスタ環境外のシステムとの統合が可能になります。
- ノード間ポート：これらのポートは、Kubernetesクラスタ内のノード間の通信を可能にします。これらは、データの共有や共同作業といったクラスタタスクに必要です。シングルノード構成の場合、ノード間ポートはノード内部でのみ使用され、外部アクセスは不要です。ノード間ポートは、クラスタ外部からのトラフィックを受け入れることができます。ファイアウォールルールを使用して、ノード間ポートへのインターネットアクセスをブロックします。
- 内部ポート：これらのポートは、ClusterIP アドレスを使用して Kubernetes クラスタ内で通信します。これらは外部に公開されておらず、ファイアウォールルールに追加する必要はありません。



すべての ONTAP tools ノードが同じサブネット上に配置されていることを確認し、相互に途切れることのない通信を維持してください。

クリックすると、ポート要件表が展開または折りたたまれます。

サービス/コンポーネント名	ポート	プロトコル	ポートタイプ	概要
ntv-gateway-svc (LB)	443つまたは8443つ	TCP	外部	VASA Provider サービスへの着信通信のパススルーポート。VASA Provider の自己署名証明書とカスタム CA 証明書は、このポートでホストされています。
SSH	22	TCP	外部	リモート サーバへのログインとコマンド実行のための Secure Shell。
rke2 server	9345	TCP	ノード間	RKE2スーパーバイザーAPI（信頼できるネットワークに制限）。
kube-apiserver	6443	TCP	ノード間	Kubernetes API サーバーポート（信頼できるネットワークに制限）。
rpcbind/portmapper	111	TCP/UDP	ノード間	サービス間のRPC通信に使用されます。
coredns (DNS)	53	TCP/UDP	ノード間	クラスタ内での名前解決のためのドメインネームシステム (DNS) サービス。
NTP	123	UDP	ノード間	時刻同期のための Network Time Protocol (NTP) 。
etcd	2379、2380、2381	TCP	ノード間	クラスタデータ用のキーバリューストア。
kube-vip	2112	TCP	ノード間	Kubernetes API サーバーポート。
kubelet	10248つまたは10250つ	TCP	ノード間	Kubernetesコンポーネント
kube-controller	10257	TCP	ノード間	Kubernetesコンポーネント
クラウドコントローラー	10258	TCP	ノード間	Kubernetesコンポーネント

サービス/コンポーネント名	ポート	プロトコル	ポートタイプ	概要
kube-scheduler	10259	TCP	ノード間	Kubernetesコンポーネント
kube-proxy	10249つまたは10256つ	TCP	ノード間	Kubernetesコンポーネント
calico-node	9091つまたは9099つ	TCP	ノード間	Calicoネットワークコンポーネント。
containerd	10010	TCP	ノード間	コンテナデーモンサービス。
VXLAN (Flannel)	8472	UDP	ノード間	ポッド間の通信のためのオーバーレイネットワーク。



HA構成の場合、すべてのノード間でUDPポート8472が開いていることを確認してください。このポートは、ノード間のポッド間通信を可能にするものであり、これをブロックするとノード間のネットワーク接続が中断されます。

ONTAP tools for VMware vSphere を vVols データストアに導入する際の構成上の制限

次の表は、VMware vSphere用のONTAP toolsを構成するためのガイドとして使用できます。

デプロイ	タイプ	vVolsの数	ホスト数
HA 認定外	スモール (S)	最大12K	32
HA 認定外	中 (M)	最大24K	64
高可用性	スモール (S)	最大24K	64
高可用性	中 (M)	最大50k	128
高可用性	ラージ (L)	最大10万	256



表内のホスト数は、接続されているすべてのvCentersの合計を表します。

VMFS および NFS データストア用の ONTAP tools for VMware vSphere を導入するための構成制限

このセクションに記載されている構成制限は、NetAppによって検証およびサポートされています。実際の制限は、環境やワークロードによって異なる場合があります。これらの制限を超えると、パフォーマンスやサポート性に影響が出る可能性があるため、推奨されません。表を確認する際は、以下の点にご留意ください：

- 仮想マシンのディザスタリカバリ (DR) は、同期、非同期、または厳密な同期ポリシーを使用して構成されます。DRはNVMeプロトコルではサポートされていません。
- ESXi ホスト クラスタ保護ではSnapMirror Active Sync が使用されますが、これは複数のvCenter展開をサポートしていません。
- ONTAP tools は、導入規模に基づいて ESXi ホストとデータストアの数のみを制限します。ONTAP tools

に接続できる vCenter Server の数には制限はありません。

- ONTAP toolsは、すべてのストレージオブジェクトを並列検出します。ONTAPストレージオブジェクトの設定制限は、アクティブに使用されているオブジェクトの数に関係なく適用されます。
- ONTAP toolsでは、オンボード可能なvCenterサーバ数に制限はありません。構成の制限は、サポートされるホストとデータストアの数によって決まります。詳細は次の表をご覧ください。

導入	VMFSおよびNFSデータストアの数	DR対応VMFSデータストアの数	ホスト数
非HA Small	200	80	32
非HA Medium	250	100	32
HA Small	350	200	64
HA Medium	600	200	128
HA Large	1024	250	256

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

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

vCenter 展開サイズ	小	中
アレイベースのレプリケーションを使用して保護するように構成された仮想マシンの総数	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
リカバリ計画ごとの保護グループの総数	50	50
複製されたデータストアの数	255	255
VM 数	4000	7000

次の表は、VMware Live Site Recovery インスタンスの数とそれに対応する ONTAP tools for VMware vSphere の導入サイズを示しています。

VMware Live Site Recoveryインスタンスの数	ONTAP toolsのデプロイメント サイズ
最大4	小規模
4～8	中
8より大きい	大規模

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

ONTAP toolsの導入前要件

展開を進める前に、以下の要件が満たされていることを確認してください。

要件	あなたのステータス
vSphereバージョン、ONTAPバージョン、および ESXi ホスト バージョンは、ONTAP toolsバージョンと互換性があります。	☐ はい ☐ いいえ
vCenter Server環境がセットアップおよび構成されています。	☐ はい ☐ いいえ
ブラウザのキャッシュが削除されました	☐ はい ☐ いいえ
親のvCenter Server 認証情報を持っている	☐ はい ☐ いいえ
vCenter Server インスタンスのログイン資格情報を持っている必要があります。このインスタンスには、ONTAP tools for VMware vSphere がデプロイ後に登録のために接続します	☐ はい ☐ いいえ
証明書が発行されるドメイン名は、カスタムCA証明書が必須となるマルチvCenterデプロイメントの仮想IPアドレスにマッピングされます。	☐ はい ☐ いいえ
ドメイン名に対してnslookupチェックを実行し、ドメインが意図したIPアドレスに解決されているかどうかを確認しました。	☐ はい ☐ いいえ
証明書は、ドメイン名と ONTAP tools の IP アドレスを使用して作成されます。	☐ はい ☐ いいえ
ONTAP tools アプリケーションと内部サービスには、vCenter Server からアクセスできます。	☐ はい ☐ いいえ
マルチテナント SVM を使用する場合、各 SVM に SVM 管理 LIF があります。	☐ はい ☐ いいえ

展開ワークシート

シングルノード展開の場合

以下のワークシートを使用して、ONTAP tools for VMware vSphere の初期導入に必要な情報を収集してください：

要件	あなたの価値
ONTAP ツールアプリケーションの IP アドレス。これは、`https://<ip>:8443/virtualization/ui/` で ONTAP ツールマネージャの Web インターフェイス（ロードバランサ）にアクセスするための IP アドレスです。	

要件	あなたの価値
内部通信用のONTAP tools仮想IPアドレス。このIPアドレスは、複数のONTAP toolsインスタンスを使用するセットアップでの内部通信に使用されます。このIPアドレスは、ONTAP toolsアプリケーションのIPアドレスと同じにしないでください。（Kubernetesコントロールプレーン）	
ONTAP tools 管理ノードの DNS ホスト名	
プライマリ DNS サーバー	
セカンダリDNSサーバー	
DNS検索ドメイン	
ONTAP tools 管理ノードの IPv4 アドレス。管理ネットワーク上のノード管理インターフェイスの一意のIPv4アドレスです。これは、SSH経由のリモート診断アクセスのためにONTAP toolsアプライアンスに接続するために使用されます。	
IPv4アドレスのサブネットマスク	
IPv4アドレスのデフォルトゲートウェイ	
IPv6アドレス（オプション）	
IPv6プレフィックス長（オプション）	
IPv6アドレスのゲートウェイ（オプション）	



上記すべてのIPアドレスに対してDNSレコードを作成してください。ホスト名を割り当てる前に、DNSでそれらを空いているIPアドレスにマッピングしてください。すべてのIPアドレスは、導入用に選択された同じVLAN上にある必要があります。

高可用性（HA）展開の場合

シングルノード展開の要件に加えて、HA展開には以下の情報が必要です：

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

ネットワークファイアウォールの設定

必要なファイアウォールポートが、関連するすべてのIPアドレスに対して開いていることを確認してください。ONTAP tools はポート 443 経由で LIF にアクセスする必要があります。必要なポートの完全なリストについては、["ONTAP tools for VMware vSphere の要件と構成制限"](#) のポート要件のセクションを参照してください。

ONTAP ストレージ設定

ONTAP ストレージと ONTAP tools for VMware vSphere のシームレスな統合を確保するために、以下の設定を検討してください：

- ストレージ接続にファイバーチャネル（FC）を使用している場合は、FCスイッチのゾーニングを設定して、ESXiホストをSVMのFC LIFに接続してください。["ONTAPシステムによるFCおよびFCoEゾーニングについて学習します"](#)
- ONTAP tools で管理される SnapMirror レプリケーションを使用するには、ONTAP ストレージ管理者が SnapMirror を使用する前に ONTAP で ["ONTAP クラスターのピア関係"](#) および ["ONTAP クラスター間 SVM ピア関係"](#) を作成する必要があります。

ONTAP Toolsの導入

ONTAP tools for VMware vSphere アプライアンスは、NFS および VMFS データストアをサポートするコアサービスを備えた小型の単一ノードとしてデプロイされます。ONTAP tools のデプロイプロセスには最大 45 分かかる場合があります。

開始する前に

小規模な単一ノードをデプロイする場合は、コンテンツライブラリはオプションです。マルチノード構成または高可用性構成の場合、コンテンツライブラリが必要です。VMwareでは、コンテンツライブラリにはVMテンプレート、vAppテンプレート、およびその他のファイルが格納されます。コンテンツライブラリを使用してデプロイすると、ネットワーク接続に依存しないため、シームレスなエクスペリエンスが実現します。

コンテンツライブラリを作成する前に、以下の点を考慮してください。

- クラスター内のすべてのホストがアクセスできるように、共有データストア上にコンテンツライブラリを作成します。
- ONTAP tools for VMware vSphere OVA をデプロイする前に、コンテンツライブラリを設定してください。
- アプライアンスをHA構成にする前に、コンテンツライブラリが作成されていることを確認してください。



デプロイ後、コンテンツライブラリ内のOVAテンプレートを削除しないでください。



将来的に HA 展開を有効にするには、ONTAP tools 仮想マシンを ESXi ホスト上に直接展開しないでください。代わりに、ESXi ホスト クラスターまたはリソース プール内に展開してください。

コンテンツライブラリを作成するには、以下の手順に従ってください。

1. 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を "[NetAppサポート サイト](#)"からダウンロードします。
2. vSphere クライアントにログインします
3. vSphere クライアントメニューを選択し、「コンテンツライブラリ」を選択します。
4. ページ右側の **Create** を選択します。
5. ライブラリに名前を付けて、コンテンツライブラリを作成します。
6. 作成したコンテンツライブラリにアクセスしてください。
7. ページ右側の*Actions*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。



詳細については、"[コンテンツライブラリの作成と使用](#)"ブログを参照してください。



デプロイを進める前に、クラスタの分散リソース スケジューラ (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 が移行されないことが保証されます。

ONTAP tools for VMware vSphere vSphereは、最初は非HA構成で展開されます。HA展開に拡張するには、CPUホット アドとメモリ ホットプラグを有効にする必要があります。この手順は、デプロイプロセスの一部として実行することも、デプロイ後にVMの設定を編集することもできます。

手順

1. ONTAP tools for VMware vSphere のバイナリ (.ova) と署名済み証明書を含むファイルを "[NetAppサポート サイト](#)"からダウンロードしてください。OVA をコンテンツライブラリにインポート済みの場合は、この手順をスキップして次の手順に進んでください。
2. vSphere サーバにログインします。
3. OVA をデプロイするリソース プール、クラスター、またはホストに移動します。



自身が管理するvVolsデータストアにONTAP tools for VMware vSphere仮想マシンを絶対に保存しないでください。

4. OVAファイルは、コンテンツライブラリまたはローカルシステムからデプロイできます。

ローカルシステムから	コンテンツライブラリより
a. 右クリックして「OVF テンプレートの展開...」を選択します。 b. URL から OVA ファイルを選択するか、ファイルの場所を参照して選択し、「次へ」を選択します。	a. コンテンツライブラリに移動し、デプロイするライブラリアイテムを選択します。 b. 「アクション」 > 「このテンプレートから新しいVMを作成する」を選択します。

5. **Select a name and folder** フィールドに、仮想マシンの名前を入力し、その場所を選択します。
 - vCenter Server 8.0.3 バージョンを使用している場合は、*この仮想マシンのハードウェアをカスタマイズする*オプションを選択します。これにより、*完了の準備ができました*ウィンドウに進む前に*ハードウェアのカスタマイズ*という追加の手順が有効になります。
 - vCenter Server 7.0.3を使用している場合は、導入の最後にある*次の手順*セクションの手順に従ってください。

netapp-ontap-tools-for-vmware-vsphere-10.5-1740090540 - New Virtual Machine from Content Library

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

Select a name and folder

Specify a unique name and target location

Virtual machine name: demooty

Select a location for the virtual machine.

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

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

CANCEL

BACK

NEXT

6. コンピュータリソースを選択し、*次へ*を選択します。必要に応じて、*デプロイされたVMを自動的に電源オンにする*のチェックボックスをオンにします。
7. テンプレートの詳細を確認し、*次へ*を選択します。
8. 使用許諾契約書を読んで同意し、**Next** を選択してください。
9. 構成に使用するストレージとディスクフォーマットを選択し、*次へ*をクリックします。
10. 各送信元ネットワークの送信先ネットワークを選択し、*次へ*を選択します。
11. *テンプレートのカスタマイズ*ウィンドウで、必要な項目を入力してください。

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

1 Select a name and folder

2 Select a compute resource

3 Review details

4 License agreements

5 Select storage

6 Select networks

7 Customize template

8 Customize hardware

9 Ready to complete

Customize template

ONTAP tools IP address

ONTAP tools virtual IP address*

vCenter Server configuration for ONTAP tools deployment

3 settings

vCenter Server hostname*

Enter the hostname of the target vCenter Server for ONTAP tools deployment.

vCenter Server username (user@domain.com)*

Enter the user principal name of the vCenter Server account (for example, username@vsphere.local).
backup@vsphere.local|

vCenter Server password*

Enter the vCenter Server password to authenticate your login.

Password

Confirm Password

CANCEL

BACK

NEXT

「テンプレートのカスタマイズ」ページの値は、正常にデプロイするために必須です。

特に以下のフィールドに注意してください：



- ホスト名：ONTAP tools VM のホスト名を入力してください。有効なホスト名形式を使用してください。
- **ONTAP tools** の IP アドレス：これは、ONTAP tools へのアクセスに使用するプライマリ管理インターフェイスです。
- **IPv4**アドレス：これは、トラブルシューティングとメンテナンスのための診断シェルとSSHアクセスに使用されるノードのIPアドレスです。

ホストまたはvCenterに DNS 名を使用する場合は、それらの名前が DNS で正しく解決されることを確認してください。



vCenter のホスト名は、ONTAP tools アプライアンスがデプロイされている vCenter Server インスタンスの名前です。

2つのvCenter Server構成でONTAP toolsを導入する場合（アプライアンスが1つのvCenterインスタンスでホストされ、別のインスタンスを管理する場合）、ONTAP toolsをホストしているvCenterインスタンスに制限付きロールを割り当てることができます。OVFテンプレートのデプロイに必要な権限のみを持つ専用のvCenterユーザーとロールを作成できます。詳細については、["ONTAP tools for VMware vSphere 10 に含まれるロール"](#)に記載されているロールを参照してください。

ONTAP tools で管理される vCenter インスタンスについて、vCenter ユーザーアカウントに管理者権限があることを確認してください。

- ホスト名には、文字（A-Z、a-z）、数字（0-9）、ハイフン（-）を含める必要があります。デュアル

スタックを設定するには、IPv6アドレスにマッピングされるホスト名を指定します。



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

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

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

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template
- Customize hardware**
- Ready to complete

Customize hardware

Configure the virtual machine hardware

Virtual Hardware VM Options Advanced Parameters

[ADD NEW DEVICE](#)

▼ CPU * 9 ⓘ

Cores per Socket 1 ▼
Sockets: 9

CPU Hot Plug ☒ Enable CPU Hot Add

Reservation 10305 ▼ MHz ▼

Limit Unlimited ▼ MHz ▼

Shares Normal ▼ 1000 ▼

Hardware virtualization ☐ Expose hardware assisted virtualization to the guest OS

Performance Counters ☐ Enable virtualized CPU performance counters

Scheduling Affinity ⓘ

CANCEL BACK NEXT

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

1 Select a name and folder

2 Select a compute resource

3 Review details

4 License agreements

5 Select storage

6 Select networks

7 Customize template

8 Customize hardware

9 Ready to complete

Customize hardware

Limit

Unlimited

MIN

Shares

Normal

1000

Hardware virtualization

Expose hardware assisted virtualization to the guest OS

Performance Counters

Enable virtualized CPU performance counters

Scheduling Affinity

I/O MMU

Enabled

Memory *

18

GB

Reservation

9

GB

Reserve all guest memory (All locked)

Limit

Unlimited

MB

Shares

Normal

368640

Memory Hot Plug

Enable

Hard disks *

5 total | 348 GB

CANCEL

BACK

NEXT

13. 「完了の準備」ウィンドウで詳細を確認し、「完了」を選択します。

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

14. 仮想マシンの自動起動オプションが選択されていない場合は、タスク完了後に仮想マシンを起動してください。

仮想マシンのWebコンソール内でインストールの進行状況を確認できます。

OVFフォームに不一致がある場合は、修正措置を促すダイアログボックスが表示されます。タブキーを使って移動し、必要な変更を行い、**OK** を選択してください。問題解決のための試行回数は3回です。3回試行しても問題が解決しない場合は、インストールプロセスが停止します。その場合は、新しい仮想マシンでインストールを再試行することをお勧めします。

次は？

ONTAP tools for VMware vSphere を vCenter Server 7.0.3 とともに導入済みの場合は、導入後に以下の手順に従ってください。

1. vCenterクライアントにログインします。
2. ONTAP tools ノードの電源をオフにします。
3. *インベントリ*にあるONTAP tools for VMware vSphereの仮想マシンに移動し、*設定の編集*オプションを選択します。
4. 「CPU」オプションで、「CPU ホット アドを有効にする」チェックボックスをオンにします
5. 「メモリ」オプションで、「メモリ ホット アド」の横にある「有効にする」チェックボックスをオンにします。

ONTAP toolsの導入エラーのトラブルシューティング

デプロイメントで問題が発生した場合は、ログとエラーコードを確認して問題を診断し、解決してください。ONTAP tools for VMware vSphere 10.5以降、ポッドから収集されるログバンドルには、MongoDB、RabbitMQ、Vaultのログに加え、すべてのポッドのステータスと説明が含まれます。これらは既存のONTAP toolsサービスログに加えて提供され、サポート性とトラブルシューティング性が向上します。

ログ ファイルの収集

ONTAP tools for VMware vSphere のログファイルは、ONTAP tools Manager ユーザーインターフェイスで使用可能なオプションから収集できます。テクニカルサポート担当者から、問題解決のためにログファイルの収集を依頼される場合があります。



ONTAP tools Managerからログを生成すると、すべてのvCenter Serverインスタンスのすべてのログが含まれます。vCenter Clientユーザーインターフェイスからログを生成すると、選択したvCenter Serverに対してスコープされます。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから **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. ログファイルを生成するには、*生成*を選択してください。
5. ログバンドルのラベルを入力し、**Generate** を選択します。

tar.gzファイルをダウンロードして、テクニカルサポートに送信してください。

vCenter クライアントユーザーインターフェイスを使用してログバンドルを生成するには、以下の手順に従ってください：

手順

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



生成されたログバンドルは、過去3日間または72時間以内に生成されたログバンドルを置き換えます。

展開エラーコード

ONTAP tools for VMware vSphere の導入、再起動、およびリカバリ操作中にエラーコードが表示される場合があります。エラーコードは5桁で、最初の2桁は問題が発生したスクリプトを表し、最後の3桁はそのスクリプト内の特定のワークフローを表します。

すべてのエラーログは、問題の追跡と解決を容易にするため、/var/log ディレクトリ内の 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 タスクが含まれています。



このページに記載されているエラーコードは参考情報としてのみご利用ください。エラーが解消されない場合、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。

以下の表は、エラーコードとそれに対応するファイル名を示しています。

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

エラーコードの最後の3桁は、スクリプト内の具体的なワークフローエラーを示します。

デプロイメントエラーコード	ワークフロー	解決
049	ネットワークと検証用の Perl スクリプトも間もなくそれらを割り当てます。	-
050	SSHキーの生成に失敗しました	プライマリ仮想マシン（VM）を再起動します。
053	RKE2のインストールに失敗しました	以下のコマンドを実行してプライマリ VM を再起動するか、再デプロイしてください：sudo rke2-killall.sh (すべての VM) sudo rke2-uninstall.sh (すべての VM)。
054	kubeconfigの設定に失敗しました	再導入

055	レジストリのデプロイに失敗しました	レジストリポッドが存在する場合は、ポッドの準備が整うまで待ってから、プライマリ VM を再起動するか、再デプロイしてください。
059	KubeVip のデプロイに失敗しました	Kubernetes コントロール プレーンの仮想 IP アドレスと、導入時に指定した ONTAP tools の IP アドレスが同じ VLAN に属し、使用可能な IP アドレスであることを確認します。前述の項目がすべて正しければ、再起動してください。そうでない場合は、再導入してください。
060	オペレーターの展開に失敗しました	再起動
061	サービスのデプロイに失敗しました	Kubernetes の基本的なデバッグ（get pods、get rs、get svc など）を ntv-system 名前空間で実行し、詳細とエラーログを /var/log/ansible-perl-errors.log および /var/log/ansible-run.log で確認してから再デプロイしてください。
062	ONTAP tools サービスのデプロイに失敗しました	詳細については、/var/log/ansible-perl-errors.log にあるエラーログを参照し、再デプロイしてください。
065	SwaggerページのURLにアクセスできません	再導入
066	ゲートウェイ証明書のデプロイ後の手順が失敗しました	アップグレードを復旧／完了するには、次の手順を実行します。 • 診断シェルを有効にします。 • 「sudo perl /home/maint/scripts/post-deploy-upgrade.pl -- postDeploy」 コマンドを実行します。 • /var/log/post-deploy-upgrade.log のログを確認してください。
088	journald のログローテーションの設定に失敗しました	VMがホストされているホストと互換性のあるVMネットワーク設定を確認してください。別のホストに移行して、VMを再起動してみてください。

089	サマリーログローテーション設定ファイルの所有権変更に失敗しました	プライマリVMを再起動します。
096	動的ストレージプロビジョナーをインストールする	-
108	シードスクリプトが失敗しました	-
114	MongoDBコレクションの内部証明書更新が失敗しました	デプロイがエラーコード114で失敗した場合は、以下の手順を実行してください： • 診断シェルを有効にします。 • 次のコマンドを実行します。 <pre>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --internal_cert_update_collection</pre> • でログを確認します <pre>/var/log/otvng/post-deploy-upgrade.log</pre>

再起動エラーコード	ワークフロー	解決
067	rke2-serverの待機がタイムアウトしました。	-
101	メンテナンス/コンソールユーザーのパスワードのリセットに失敗しました。	-
102	メンテナンス/コンソールユーザーのパスワードリセット中に、パスワードファイルの削除に失敗しました。	-
103	保管庫内の新しいメンテナンス/コンソールユーザーのパスワードの更新に失敗しました。	-
088	journald のログローテーションの設定に失敗しました。	VMがホストされているホストと互換性のあるVMネットワーク設定を確認してください。別のホストに移行して、VMを再起動してみてください。
089	サマリーログローテーション設定ファイルの所有権変更に失敗しました。	仮想マシンを再起動してください。

ONTAP Tools for VMware vSphereの設定

vCenter Server インスタンスを ONTAP tools に追加する

vCenter Server インスタンスを ONTAP tools for VMware vSphere に追加して、vCenter Server 環境の仮想データストアを設定、管理、保護します。複数の vCenter Server インスタンスを追加する場合、ONTAP tools と各 vCenter Server 間のセキュアな通信にはカスタム CA 証明書が必要です。

タスク概要

ONTAP ツールは vCenter Server と統合されており、vSphere クライアントから直接、プロビジョニング、Snapshot、データ保護などのストレージタスクを実行できます。

vCenter Server インスタンスを ONTAP tools に追加すると、以下のアクションが自動的にトリガーされます：

- ONTAP tools は、vCenter クライアント プラグイン をリモート プラグイン として登録します。
- プラグインと API のカスタム Privileges は、vCenter Server インスタンスに適用されます。
- ユーザーを管理するために、カスタムロールが作成されます。
- プラグインはvSphereユーザーインターフェースのショートカットとして表示されます。

開始する前に

- vCenter Server 証明書に、DNS と IP アドレスの両方のエントリを含む有効なサブジェクト代替名 (SAN) 拡張が含まれていることを確認してください。次に例を示します。

```
X509v3 extensions:  
    X509v3 Subject Alternative Name:  
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

証明書に SAN 拡張が含まれていない場合、または SAN 拡張に正しい DNS または IP アドレス値が含まれていない場合、証明書検証エラーのため、ONTAP tools for VMware vSphere の操作が失敗する可能性があります。

- vCenter Server のプライマリネットワーク識別子 (PNID) を SAN の詳細に含める必要があります。PNID と DNS 名は同一であり、DNS で解決可能である必要があります。
- vCenter Server は完全修飾ドメイン名 (FQDN) を使用して導入することを推奨します。証明書の SAN に DNS Name=machine_FQDN が含まれるようにすることで、最適な互換性とサポートを実現します。
- 詳細については、VMware のドキュメントを参照してください：
 - ["異なる解決策パスのvSphere証明書の要件"](#)
 - ["vCenter マシン SSL 証明書をカスタム認証局署名証明書に置き換える"](#)
 - ["エラー：Subject Alternate Name \(SAN\) フィールドにPNIDが含まれていません。有効な証明書を提供してください"](#)



FQDN が使用できない場合は、PNID を IP アドレスに設定し、IP アドレスを SAN に含めることができます。ただし、これは VMware では推奨されていません。

手順

1. ウェブブラウザを開き、次のURLにアクセスしてください：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. **vCenters** > 追加 を選択して、vCenter サーバーインスタンスをオンボードします。vCenter の IP アドレスまたはホスト名、ユーザー名、パスワード、およびポートの詳細を入力してください。
4. 詳細オプションで、vCenter Server 証明書を自動的に取得（承認）するか、手動でアップロードします。



vCenter インスタンスを ONTAP tools に追加するために管理者アカウントは必要ありません。管理者アカウントがなくても、権限を制限したカスタムロールを作成できます。詳細については、"[vCenter Server RBAC と ONTAP tools for VMware vSphere 10 を使用](#)" を参照してください。

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

ONTAP tools for VMware vSphere を使用して、VASA プロバイダーを vCenter Server インスタンスに登録します。これにより、ONTAP システムでのストレージ ポリシーベース管理、vVols サポート、および VMware Live Site Recovery アプライアンスとの統合が可能になります。

VASA プロバイダー設定には、選択した vCenter Server の登録ステータスが表示されます。

手順

1. vSphere クライアントにログインします。
2. プラグイン セクションの「ショートカット」>「**NetApp ONTAP tools**」を選択します。
3. 設定 > **VASA Provider**設定 を選択します。ONTAP toolsは、VASA Providerの登録ステータスを「未登録」と表示します。
4. VASAプロバイダーを登録するには、*Register*ボタンを選択してください。
5. VASA Providerの名前とクレデンシャルを入力します。ユーザ名には、英字、数字、アンダースコアのみを使用できます。パスワードは8~256文字にする必要があります。
6. 「登録」を選択します。
7. 登録とページ更新が成功すると、ONTAP tools には、登録済みの VASA Provider のステータス、名前、およびバージョンが表示されます。

次の手順

オンボーディングされた VASA プロバイダーが、vCenter クライアントの VASA プロバイダーの下に表示されていることを確認してください：

手順

1. vCenter Server インスタンスに移動します。
2. 管理者の資格情報でログインしてください。
3. **Storage Providers > Configure** を選択します。登録済みの VASA プロバイダーが正しくリストされていることを確認してください。

ONTAP tools を使用して NFS VAAI プラグイン をインストールする

NFS vStorage Array Integration用API (NFS VAAI) プラグインは、VMware vSphere をNFSストレージアレイに接続します。ONTAP tools for VMware vSphereを使用してVAAIプラグインをインストールします。これにより、ESXiホストの代わりにNFSストレージアレイが特定のストレージ操作を処理できるようになります。

開始する前に

- ["NetApp NFS Plug-in for VMware VAAI"](#)インストールパッケージをダウンロードします。
- ESXi ホストがvSphere 7.0 U3（最新パッチ以降）および ONTAP 9.14.1 以降であることを確認してください。
- NFSデータストアをマウントします。

手順

1. vSphere クライアントにログインします。
2. プラグイン セクションの「ショートカット」>「**NetApp ONTAP tools**」を選択します。
3. 設定 > **NFS VAAI Tools** を選択します。
4. VAAI プラグインをすでに vCenter Server にアップロード済みの場合は、「既存バージョン」の「変更」を選択してください。まだアップロードしていない場合は、「アップロード」を選択してください。
5. ファイルを参照して選択し、`.vib`ファイルを選択して、*アップロード*を選択してファイルをONTAP toolsにアップロードします。
6. 「ESXi ホストにインストール」を選択し、NFS VAAI プラグインをインストールする ESXi ホストを選択して、「インストール」を選択します。

vSphere Web クライアントには、プラグインをインストールできる ESXi ホストのみが表示されます。インストールの進行状況は、最近のタスクセクションで確認できます。

7. インストール後、ESXiホストを手動で再起動してください。

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

次の手順

NFS VAAI プラグインをインストールしてESXiホストを再起動した後、VAAI コピー オフロード用のNFSエクスポートポリシーを設定します。エクスポートポリシールールが以下の要件を満たしていることを確認してください：

- 関連する ONTAP ボリュームは NFSv4 呼び出しを許可します。

- rootユーザーはrootのままであり、すべてのジャンクション親ボリュームでNFSv4が許可されます。
- VAAI サポートのオプションは、関連する NFS サーバで設定されます。

詳細については、"[VAAI コピー オフロードに適切な NFS エクスポート ポリシーを設定する](#)" KBの記事を参照してください。

関連情報

["VMware vStorage over NFSのサポート"](#)

["NFSv4.0の有効化または無効化"](#)

["ONTAPでのNFSv4.2のサポート"](#)

ONTAP toolsでESXiホストの設定を構成する

ESXi サーバーのマルチパス設定とタイムアウト設定を構成することで、データの可用性と整合性を維持するのに役立ちます。プライマリパスが利用できなくなった場合に、バックアップストレージパスへの自動フェイルオーバーが可能になります。

ESXiサーバーのマルチパスとタイムアウト設定を構成する

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

タスク概要

この処理には、お使いのシステム構成や負荷状況によっては時間がかかる場合があります。最近のタスクパネルで進捗状況を確認できます。

手順

1. VMware vSphere Web クライアントのホームページで、「ホストとクラスタ」を選択します。
2. VMware vSphere Web クライアントのショートカットページで、プラグイン セクションの **NetApp ONTAP tools** を選択します。
3. ONTAP tools for VMware vSphere プラグインの概要（ダッシュボード）にある **ESXi** ホスト準拠 カードに移動します。
4. 「推奨設定を適用」リンクを選択します。
5. 「推奨ホスト設定の適用」ウィンドウで、NetApp推奨設定を使用するように更新するホストを選択し、「次へ」を選択します。



ESXiホストを展開すると、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てください。
7. 概要ペインで値を確認し、*完了*を選択します。最近のタスクパネルで進捗状況を確認できます。

ESXiホストの値を設定する

ONTAP tools for VMware vSphereを使用して、ESXiホスト上でタイムアウト値やその他の値を設定し、最適なパフォーマンスとフェイルオーバーを実現します。これらの値はNetAppのテストに基づいて設定されます。

次に示すESXiホストの値を設定できます。

HBA / CNA アダプタ設定

以下のパラメータをデフォルト値に設定します：

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

MPIO 設定

MPIO設定は、NetAppストレージシステムに最適なパスを選択します。MPIO設定は最適なパスを選択して使用します。

ハイパフォーマンス環境の場合、または単一の LUN データストアでテストする場合は、ラウンドロビン (VMW_PSP_RR) パス選択ポリシー (PSP) の負荷分散設定を調整してパフォーマンスを向上させます。デフォルトの IOPS 値を 1000 から 1 に変更します。



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

NFS設定

パラメータ	この値を...に設定してください。
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumesを使用したチャンク アップロード署名要求がサポートされるようになりました。	256
NFS.MaxQueueDepth	128以上
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

ONTAP tools用のONTAPユーザーロールと権限を設定する

このセクションでは、ONTAP tools for VMware vSphere および ONTAP System Manager を使用して、ストレージバックエンドの ONTAP ユーザーロールと Privileges

を設定します。提供されている JSON ファイルを使用してロールを割り当てたり、ユーザーとロールを手動で作成したり、管理者以外のアカウントに必要な最小限の Privileges を適用したりできます。

開始する前に

- ONTAP tools for VMware vSphere から ONTAP Privileges ファイルを https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip を使用してダウンロードします。zip ファイルをダウンロードすると、2 つの JSON ファイルが見つかります。ASA r2 システムを設定する際は、ASA r2 固有の JSON ファイルを使用してください。



ユーザーは、クラスタレベルまたはストレージ仮想マシン (SVM) レベルで直接作成できません。user_roles.json ファイルを使用しない場合は、ユーザーが最低限必要な SVM 権限を持っていることを確認してください。

- ストレージバックエンドの管理者権限でログインしてください。

手順

1. ダウンロードした https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip ファイルを展開します。
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. 管理者権限でクラスターにログインしてください。ユーザーを設定するには：
 - a. クラスター ONTAP tools ユーザーを設定するには、クラスター > 設定 > ユーザーと役割 ペインを選択します。
 - b. SVM ONTAP tools ユーザーを設定するには、ストレージ **SVM** > 設定 > ユーザーと役割 ペインを選択します。
 - c. 「Users」の下にある「Add」を選択します。
 - d. 「ユーザーの追加」ダイアログ ボックスで、「仮想化製品」を選択します。
 - e. *参照*して ONTAP Privileges JSON ファイルを選択してアップロードします。ASA r2 以外のシステムの場合は users_roles.json ファイルを選択し、ASA r2 システムの場合は users_roles_ASAr2.json ファイルを選択します。

ONTAP tools は製品フィールドに自動的に入力します。

- f. ドロップダウンから、製品機能として「VSC、VASA Provider、SRA」を選択してください。

ONTAP tools は、選択した製品機能に基づいて「役割」フィールドを自動的に設定します。

- g. 必要なユーザ名とパスワードを入力します。
- h. ユーザーに必要な Privileges (Discovery、Create Storage、Modify Storage、Destroy Storage、NAS/SAN Role) を選択し、**Add** を選択します。

ONTAP tools は新しいロールとユーザーを追加します。設定したロールに付与されている Privileges を確認できます。

SVMアグリゲートマッピング要件

SVM ユーザー認証情報を使用してデータストアをプロビジョニングする場合、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上にボリュームを作成します。ONTAP は、SVM にマッピングされていないアグリゲート上に SVM ユーザーがボリュームを作成することを防止します。ボリュームを作成する前に、ONTAP REST API または CLI を使用して、SVM を必要なアグリゲートにマッピングしてください。

REST API :

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

ONTAP CLI :

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

ONTAP ユーザーとロールを手動で作成する

JSONファイルを使わずに、ユーザー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. 管理者権限でクラスターにログインします。
 - a. クラスター ONTAP tools のロールを設定するには、クラスター > 設定 > *ユーザーとロール*を選択します。
 - b. クラスター SVM の ONTAP tools ロールを設定するには、ストレージ **SVM** > 設定 > *ユーザーとロール*を選択します。
3. 役割を作成する：
 - a. **Roles** テーブルの **Add** を選択します。
 - b. *役割名*と*役割属性*の詳細を入力してください。

*RESTAPI パス*を追加し、ドロップダウンリストからアクセスを選択してください。
 - c. 必要なAPIをすべて追加し、変更を保存します。
4. ユーザーを作成する：
 - a. ユーザー テーブルの下にある **追加** を選択します。
 - b. 「ユーザーの追加」ダイアログボックスで、「System Manager」を選択します。
 - c. *ユーザー名*を入力してください。

- d. 上記の「ロールの作成」手順で作成したオプションから「ロール」を選択してください。
- e. アクセスを許可するアプリケーションと認証方法を入力します。ONTAPI と HTTP は必須のアプリケーションで、認証タイプは * Password * です。
- f. ユーザーのパスワードを設定し、ユーザーを保存します。

管理者権限を持たないグローバルスコープのクラスタユーザーに必要な最小限の **Privileges** の一覧

このページでは、JSON ファイルを持たない非管理者グローバルスコープのクラスタユーザーに必要な最小限の Privileges を一覧表示します。クラスタがローカルスコープにある場合は、JSON ファイルを使用してユーザーを作成してください。これは、ONTAP tools for VMware vSphere が ONTAP 上でプロビジョニングを行うために、読み取り Privileges 以上の権限を必要とするためです。

APIを使用して機能にアクセスできます：

API	アクセス レベル	使用目的
/api/cluster	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/cluster/nodes	読み取り専用	プラットフォームタイプの検出
/api/security/accounts	読み取り専用	特権の検出
/api/security/roles	読み取り専用	特権の検出
/api/storage/aggregates	読み取り専用	データストア/ボリュームのプロビジョニング中のアグリゲートスペースチェック
/api/storage/cluster	読み取り専用	クラスタレベルのスペースと効率データを取得するには
/api/storage/disks	読み取り専用	集約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およびVMポリシー管理
/api/svm/svms	読み取り専用	クラスタをローカルで追加した際に、SVM構成を取得するため。
/api/network/ip/interfaces	読み取り専用	ストレージバックエンドの追加 - 管理LIFスコープがクラスタ/SVMであることを識別する
/api/storage/availability-zones	読み取り専用	SAZ ディスカバリ。ONTAP 9.16.1 リリース以降および ASA r2 システムに適用されます。
/api/cluster/metrocluster	読み取り専用	MetroCluster のステータスと設定の詳細を取得します。

VMware vSphere 向け ONTAP tools の ONTAP API ベースのクラスタスコープユーザーを作成する



データストアに対するPATCH操作および自動ロールバックには、検出、作成、変更、および破棄の権限が必要です。権限が不足していると、ワークフローやクリーンアップに問題が発生する可能性があります。

検出、作成、変更、削除の権限を持つ ONTAP API ベースのユーザーは、ONTAP tools のワークフローを管理できます。

上記で述べたすべての権限を持つクラスタスコープのユーザーを作成するには、次のコマンドを実行します：

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

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

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

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

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

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

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

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

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

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

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

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

security login rest-role create -role <role-name> -api
```

```

/api/storage/namespaces -access all

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```



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

さらに、ONTAPバージョン9.16.0以降では、以下のコマンドを実行してください：

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

ONTAP バージョン 9.16.1 以降の ASA r2 システムの場合は、次のコマンドを実行します。

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

VMware vSphere 向け ONTAP tools の ONTAP API ベースの SVM スコープユーザーを作成する

以下のコマンドを実行して、すべての権限を持つSVMスコープのユーザーを作成します。

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

```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

さらに、ONTAPバージョン9.16.0以降では、以下のコマンドを実行してください：

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

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

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

例：

```
security login create -user-or-group-name testvpsraall -application http  
-authentication-method password -role  
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

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

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

例：

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

ONTAP tools for VMware vSphere 10.1ユーザーから10.3ユーザーへのアップグレード

JSONファイルを使用して作成されたクラスタスコープのユーザーを持つONTAP tools for VMware vSphere 10.1ユーザーは、以下のONTAP CLIコマンドを管理者権限で使用して、10.3リリースにアップグレードしてください。

製品の機能について：

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

クラスタ権限：

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all

ONTAP tools for VMware vSphere 10.1 で json ファイルを使用して作成された SVM スコープのユーザーを使用している場合は、管理者権限を持つ ONTAP CLI コマンドを使用して 10.3 リリースにアップグレードしてください。

SVM権限：

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>
```

```
security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>
```

以下のコマンドを有効にするには、既存のロールに `vserver nvme namespace show` および `vserver nvme subsystem show` コマンドを追加します。

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

ONTAP tools for VMware vSphere 10.3ユーザーから10.4ユーザーへのアップグレード

ONTAP 9.16.1 以降、ONTAP tools for VMware vSphere 10.3 ユーザーを 10.4 ユーザーにアップグレードします。

JSON ファイルを使用して作成されたクラスタスコープユーザーおよび ONTAP バージョン 9.16.1 以降を使用している ONTAP tools for VMware vSphere 10.3 のユーザーは、管理者権限を持つ ONTAP CLI コマンドを使用して 10.4 リリースにアップグレードしてください。

製品の機能について：

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

クラスタ権限：

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

ONTAP toolsにストレージバックエンドを追加する

ONTAP tools for VMware vSphere を使用して、ESXi ホストのストレージバックエンドを追加および管理します。クラスターや SVM をオンボーディングし、MetroCluster サポートを有効にして、セキュアな接続のために証明書を検証できます。ストレージバックエンドは、ONTAP tools Manager または vSphere クライアントを使用して構成し、証明書のステータスを監視したり、クラスターの変更後にリソースを手動で再検出したりできます。

ストレージ バックエンドをローカルに追加するには、ONTAP toolsのインターフェイスでクラスターまたはSVMの資格情報を使用します。ローカル ストレージ バックエンドは、選択したvCenter Serverでのみ使用できます。ONTAP toolsは、vVolsまたはVMFSデータストア管理のためにSVMをvCenter Serverにマッピングします。VMFSデータストアおよびSRAのワークフローでは、クラスターをグローバルにマッピングすることなくSVMの資格情報を使用できます。

グローバルストレージバックエンドを追加するには、ONTAP tools Manager で ONTAP クラスターの認証情報を使用します。グローバルストレージバックエンドにより、検出ワークフローが vVol 管理に必要なクラスターリソースを特定できるようになります。マルチテナント環境では、SVM ユーザーをローカルに追加してvVols データストアを管理できます。

グローバルおよびローカルストレージバックエンドの詳細については、KB記事 ["OTV 10：ストレージバックエンドのグローバルスコープとローカルスコープとは"](#)を参照してください。

MetroClusterサポートが ONTAP で有効になっている場合は、ソースクラスターとデスティネーションクラスターの両方を、ローカルまたはグローバルストレージバックエンドとしてオンボードします。

開始する前に

証明書に有効なサブジェクト代替名 (SAN) フィールドが含まれていることを確認してください。ONTAP システムはSANフィールドを使用して、クラスターおよびSVM管理LIFを識別します。

ONTAP tools Manager の使用



マルチテナントのセットアップでは、ストレージバックエンドクラスタをグローバルに追加し、SVMをローカルに追加して、SVMユーザーの認証情報を使用できます。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから「ストレージバックエンド」を選択します。
4. ストレージバックエンドを追加し、サーバーのIPアドレスまたはFQDN、ユーザー名、パスワードの詳細を指定してください。



IPv4およびIPv6アドレス管理LIFがサポートされています。

5. ONTAPクラスタ証明書を自動的に取得して認証するか、証明書の場合を参照して手動でアップロードします。



必要に応じて、メンテナンスコンソールからサブジェクト代替名 (SAN) の検証を無効にすることができます。手順については、["証明書検証フラグを変更する"](#)を参照してください。

6. 追加するストレージバックエンドがMetroCluster構成の一部である場合、ONTAP tools Managerはピアクラスターを追加するためのポップアップメッセージを表示します。「追加」を選択し、MetroClusterピアストレージバックエンドの詳細を入力してください。



ONTAPシステムがスイッチオーバーとスイッチバックを実行した後、ONTAP tools の検出を手動で実行してください。

vSphere クライアントユーザーインターフェースの使用



vVolsデータストアは、vSphereクライアントユーザーインターフェースを通じたSVMユーザーの直接追加をサポートしていません。

1. vSphere クライアントにログインします。
2. ショートカットページで、プラグインセクションにある **NetApp ONTAP tools** を選択します。
3. サイドバーから「ストレージバックエンド」を選択します。
4. ストレージバックエンドを追加し、サーバーの IP アドレス、ユーザー名、パスワード、ポートの詳細を入力してください。



IPv4またはIPv6の管理LIFのいずれかを使用して、クラスタベースの認証情報でストレージバックエンドを追加できます。SVMユーザーを直接追加するには、SVMベースの認証情報とSVM管理LIFを指定してください。クラスターがすでにオンボーディングされている場合、そのクラスターからSVMユーザーを再度オンボーディングすることはできません。

5. ONTAPクラスタ証明書を自動的に取得して認証するか、証明書の場合を参照して手動でアップロードします。
6. 追加されたストレージバックエンドが MetroCluster 構成の一部である場合、ONTAP tools は **Add MetroCluster peer** 画面を表示します。**Add peer** を選択して、ピアストレージバックエンドを追加します。



ONTAPシステムがスイッチオーバーとスイッチバックを実行した後、ONTAP tools の検出を手動で実行してください。

ONTAP tools は、*ストレージバックエンド*ページに新しく追加されたストレージバックエンドを一覧表示します。証明書の有効期限が30日以内の場合、ONTAP tools は証明書の有効期限列に警告を表示します。有効期限が切れると、ONTAP tools はストレージシステムに接続できないため、ストレージバックエンドを不明としてマークします。

関連情報

["OTV 10：ストレージバックエンドのグローバルスコープとローカルスコープとは"](#)

["クラスタをMetroCluster構成に設定"](#)

ONTAP tools でvCenter Server インスタンスにストレージバックエンドを関連付ける

ストレージバックエンドを vCenter Server インスタンスに関連付けて、すべての vCenter Server インスタンスへのアクセスを有効にします。MetroCluster 構成では、ストレージバックエンドクラスタを関連付ける場合、ピアクラスタも vCenter Server に関連付けてください。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから vCenter を選択します。
4. ストレージバックエンドに接続する vCenter Server インスタンスの横にある縦の省略記号を選択します。
5. ドロップダウンメニューから、選択したvCenter Serverインスタンスに関連付けるストレージバックエンドを選択します。

ONTAP tools でネットワーク アクセスを設定する

デフォルトでは、ESXi ホストから検出されたすべての IP アドレスは、ネットワーク アクセスを設定しない限り、エクスポート ポリシーに自動的に追加されます。エクスポート ポリシーを変更することで、特定の IP アドレスからのアクセスのみを許可できます。除外された ESXi ホストがマウント操作を試みた場合、その操作は失敗します。

手順

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

複数のIPアドレスを追加するには、リストをカンマ、範囲、Classless Inter-Domain Routing (CIDR) 、またはこれら3つの組み合わせで区切ります。

4. 「保存」を選択します。

ONTAP toolsでデータストアを作成する

ホストクラスタレベルでデータストアを作成すると、ONTAP tools はすべての宛先ホストにマウントし、必要な権限がある場合にのみアクションを有効にします。

vCenter Server のネイティブデータストアと **ONTAP tools** が管理するデータストア間の相互運用性

ONTAP tools for VMware vSphere 10.4 以降、ONTAP tools はデータストア用にネストされた igroup を作成します。親 igroup はデータストア固有のもので、子 igroup はホストにマッピングされます。ONTAP System Manager からフラットな igroup を作成し、ONTAP tools を使用せずに VMFS データストアの作成に使用できます。詳細については、"[SANイニシエータとigroupを管理する](#)"を参照してください。

ストレージをオンボーディングしてデータストア検出を実行した後、ONTAP tools はVMFSデータストア内のフラットなigroupをネストされたigroupに変更します。以前のフラットなigroupを使用して新しいデータストアを作成することはできません。ネストされたigroupを再利用するには、ONTAP tools の管理インターフェイスまたはREST APIを使用してください。

vVols データストアを作成する

ONTAP tools for VMware vSphere 10.3以降では、スペース効率をthinとして、ASA r2システム上にvVols データストアを作成できます。vVol。VASA Providerは、vVolデータストアの作成時にコンテナと必要なプロトコルエンドポイントを作成します。VASA Providerは、このコンテナにバックアップボリュームを割り当てません。

開始する前に

- 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てください。
- VASAプロバイダーが選択したvCenterに登録されていることを確認してください。
- ASA r2ストレージシステムでは、SVMはSVMユーザーのアグリゲートにマッピングされる必要があります。

手順

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



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

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



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

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

新しいボリュームを作成する際に、データストアでQoSを有効にすることができます。デフォルトでは、LUN作成要求ごとに1つのボリュームが作成されます。ASA r2ストレージシステムのvVolsデータストアについては、この手順をスキップしてください。

8. *概要*ペインで選択内容を確認し、*完了*を選択してください。

NFSデータストアを作成する

NFSデータストアは、NFSプロトコルを使用してESXiホストを共有ストレージに接続します。これらはシンプルで柔軟性があり、VMware vSphere環境で使用されています。

手順

1. vSphere クライアントにログインします。
2. ホストシステム、ホストクラスタ、またはデータセンターを右クリックして、* NetApp ONTAP tools* > *データストアの作成*を選択します。
3. *データストアの種類*フィールドで「NFS」を選択してください。
4. 「名前とプロトコル」ペインに、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。詳細オプションで「データストアクラスタ」と「Kerberos認証」を選択します。



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

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



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

- 詳細オプションでは、プラットフォームのドロップダウンメニューで「パフォーマンス」または「容量」が選択されている場合にのみ、「非対称」切り替えボタンが表示されます。
 - プラットフォームのドロップダウンで **Any** オプションを選択すると、vCenter 内のすべての SVM を表示できます。プラットフォームと非対称フラグは表示には影響しません。
7. 「ストレージ属性」ペインで、ボリューム作成に使用するアグリゲートを選択します。詳細設定で、必要に応じて「スペース予約」と「QoSを有効にする」を選択します。
 8. 「概要」ペインで選択内容を確認し、「完了」を選択してください。

ONTAP tools はNFSデータストアを作成し、すべてのホストにマウントします。

VMFSデータストアを作成する

VMFSは、仮想マシンファイルを保存するためのクラスタ型ファイルシステムです。複数のESXiホストが同じVMファイルに同時にアクセスでき、vMotionおよび高可用性機能をサポートします。

保護されたクラスターの場合：

- VMFSデータストアのみ作成可能です。保護されたクラスタにVMFSデータストアを追加すると、自動的にそのデータストアが保護されます。
- 保護されたホストクラスタが1つ以上存在するデータセンターには、データストアを作成することはできません。
- 親ホストクラスタが「自動フェイルオーバーデュプレックスポリシー」（均一構成または非均一構成）によって保護されている場合、ESXi ホスト上にデータストアを作成することはできません。
- VMFSデータストアは、非同期関係によって保護されているESXiホスト上でのみ作成できます。「Automated Failover Duplex」ポリシーによって保護されているホストクラスタの一部であるESXiホスト上に、データストアを作成してマウントすることはできません。

開始する前に

- ONTAP ストレージ側で、各プロトコルのサービスと LIF を有効にします。
- ASA r2 ストレージシステムで SVM ユーザーの集約に SVM をマッピングします。

- NVMe/TCPプロトコルを使用する場合は、ESXiホストを設定します。

- a. 確認する ["VMware互換性ガイド"](#)



VMware vSphere 7.0 U3以降のバージョンはNVMe/TCPプロトコルをサポートしています。ただし、VMware vSphere 8.0以降のバージョンを推奨します。

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

FC プロトコル用に ONTAP SVM を設定するには、["FC用のSVMの設定"](#)を参照してください。

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

VMware vSphere 7.0でNVMe/FCを使用する方法の詳細については、["ONTAP NVMe/FC ホスト構成ガイド"](#)および ["TR-4684を使用したチャック アップロード署名要求がサポートされるようになりました。"](#)を参照してください。

手順

1. vSphere クライアントにログインします。
2. ホストシステム、ホストクラスタ、またはデータセンターを右クリックして、**NetApp ONTAP tools** > *データストアの作成*を選択します。
3. VMFS データストアのタイプを選択します。
4. 「名前とプロトコル」ペインに、データストア名、サイズ、およびプロトコル情報を入力します。既存のVMFSクラスタに新しいデータストアを追加するには、「詳細オプション」でデータストアクラスタを選択します。
5. **Storage***ペインでストレージVMを選択します。必要に応じて、*詳細オプション セクションで カス

タムイニシエータグループ名を入力してください。データストアには、既存の igroup を選択するか、カスタム名で新しい igroup を作成できます。

NVMe/FCまたはNVMe/TCPプロトコルが選択されると、新しい名前空間サブシステムが作成され、名前空間マッピングに使用されます。ONTAP toolsは、データストア名を含む自動生成された名前を使用して、名前空間サブシステムを作成します。*Storage*ペインの詳細オプションにある*custom namespace subsystem name*フィールドで、名前空間サブシステムの名前を変更できます。

6. 「ストレージ属性」 ペインから：

- a. ドロップダウンオプションから「Aggregate」を選択します。



ASA r2ストレージシステムでは、ストレージが分離されているため、*アグリゲート*オプションは表示されません。ASA r2ストレージシステムタイプのSVMを選択すると、ストレージ属性ページにQoSを有効にするためのオプションが表示されます。

- b. ONTAP toolsは、選択したプロトコルに基づいて、シン スペース リザーブを持つストレージ ユニット（LUN/Namespace）を作成します。



ONTAP 9.16.1以降、ASA r2ストレージシステムはクラスターあたり最大12ノードをサポートします。

- c. 12ノードSVMを搭載したASA r2ストレージシステム（異種クラスタ）の*パフォーマンスサービスレベル*を選択してください。選択したSVMが同種クラスタである場合、またはSVMユーザーを使用している場合は、このオプションは使用できません。

「Any」は、デフォルトのパフォーマンスサービスレベル（PSL）値です。この設定では、ONTAPのバランスの取れた配置アルゴリズムを使用してストレージユニットを作成します。ただし、必要に応じてパフォーマンスオプションまたはエクストリームオプションを選択できます。

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



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



既存のボリュームを使用して、NVMe/FCまたはNVMe/TCPプロトコルによるVMFSデータストアを作成することはできません。VMFSデータストア用の新しいボリュームを作成します。

7. 「概要」 ペインでデータストアの詳細を確認し、「完了」を選択します。



保護されたクラスター上にデータストアを作成すると、「The datastore is being mounted on a protected Cluster.」という読み取り専用のメッセージが表示されます。

結果

ONTAP tools はVMFSデータストアを作成し、すべてのホストにマウントします。

データストアと仮想マシンの保護

ONTAP toolsでホストクラスタを保護する

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

開始する前に

ホストクラスタを保護する前に、以下の要件を満たしていることを確認してください。

- ホストクラスタには、単一のSVMからのデータストアのみが含まれています。
- ホストクラスタ上のデータストアは、クラスタ外のホストにはマウントされません。
- ホストクラスタにマウントされるデータストアは、iSCSIまたはFCプロトコルを使用するVMFSデータストアです。vVols、NFS、またはNVMe/FCおよびNVMe/TCPプロトコルを使用したVMFSデータストアは使用できません。
- ホスト上にマウントされたFlexVol/LUN ボリュームに基づくデータストアは、いずれの整合性グループにも属しません。
- ホストにマウントされたFlexVol/LUN ボリュームに基づくデータストアは、SnapMirror関係の一部ではありません。
- ホストクラスタには、少なくとも1つのデータストアが含まれています。

手順

1. vSphere クライアントにログインします。
2. ホストクラスタを右クリックして、* NetApp ONTAP tools* > *クラスタの保護*を選択します。
3. クラスタ保護ウィンドウでは、システムが自動的にデータストアの種類とソースストレージ仮想マシン (VM) の詳細を入力します。保護されているデータストアを表示するには、「データストア」リンクを選択してください。
4. 「関係を追加」を選択します。
5. 「**SnapMirror** 関係の追加」*ウィンドウで、「ターゲットストレージVM」と「ポリシー」*タイプを選択します。

ポリシータイプは非同期または AutomatedFailOverDuplex です。

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

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

6. ホスト構成を統一しない場合は、そのクラスタ内の各ホストに対してホストアクセス（送信元/宛先）を選択してください。

7. *追加*を選択します。
8. **Modify host cluster protection** 操作を使用して、ホストクラスタ保護を編集できます。省略記号メニューオプションを使用して、関係を編集または削除できます。
9. 「保護」ボタンを選択します。

システムはジョブID詳細を含むvCenterタスクを作成し、最近のタスクパネルにその進捗状況を表示します。これは非同期タスクです。ユーザーインターフェースにはリクエストの送信状況のみが表示され、タスクの完了を待つことはありません。

10. 保護対象のホストクラスタを表示するには、* NetApp ONTAP tools* > 保護 > *ホストクラスタ関係*に移動します。整合性グループを選択すると、その容量、関連するデータストア、および子整合性グループが表示されます。



作成後1時間以内に保護を解除する必要がある場合は、まずストレージ検出を実行してください。

関連情報

"VMware vSphere メトロストレージクラスター (vMSC) "

SRA保護を使用して保護する

データストアを保護するために **ONTAP tools** で **SRA** を設定する

ONTAP tools for VMware vSphereは、ディザスタリカバリを設定するためのSRA機能を有効にするオプションを提供します。

開始する前に

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

手順

1. URL : `https://<srm\_ip>:5480` を使用してVMware Live Site Recoveryアプライアンス管理インターフェースにログインし、VMware Live Site Recoveryアプライアンス管理インターフェースでStorage Replication Adaptersに移動します。
2. 「新しいアダプター」を選択します。
3. SRA プラグイン用の .tar.gz インストーラーを VMware Live Site Recovery にアップロードします。
4. VMware Live Site Recovery のストレージレプリケーションアダプタページで詳細が更新されていることを確認するために、アダプタを再スキャンしてください。



フェイルオーバー後、データストアに対して拡張、マウント、削除などの操作が利用できなくなる場合があります。データストアの検出を実行して、適切なコンテキストメニューアクションを更新および表示します。



各再保護操作の後には、両方のサイトでストレージ検出を実行する必要があります。

SRA保護機能を備えた新しいシステムでは、必ずテストフェイルオーバーを実行してください。テストフェイルオーバーをスキップすると、再保護操作が失敗する可能性があります。

ファンアウト構成において、自動フェイルオーバーデュープレックスおよび非同期 SnapMirror の SnapMirror ソースがサイト B に変更される SnapMirror Active Sync フェイルオーバーの後、サイト B とサイト C の間でテストフェイルオーバーを実行してください。この手順を省略すると、再保護操作が失敗する可能性があります。

関連情報

["VMware Site Recovery Managerを使用してNFSデータストアの災害復旧を構成する"](#)

SAN および NAS 環境向けの ONTAP tools で SRA を構成する

VMware Live Site Recovery 用の 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環境向けにSRAを構成する



SRAワークフローの整合性グループは、UnifiedとASA r2ストレージシステムの両方で、SANプロトコル (iSCSIとファイバーチャネル) でのみサポートされています。

開始する前に

保護サイトと復旧サイトには、以下のプログラムをインストールしておく必要があります。

- VMware Live Site Recovery : VMware のサイトには、VMware Live Site Recovery のインストールドキュメントが掲載されています。

["VMware Live Site Recoveryについて"](#)

- SRA : VMware Live Site Recovery にアダプタをインストールします。

iSCSIプロトコル構成については、SRAワークフローを実行する前に以下の点に注意してください：

- 保護されたサイト：iSCSI ストレージアダプタとデータ LIF の詳細は、データストアをプロビジョニングする際に自動的に構成されます。手動設定は不要です。
- リカバリサイト：iSCSIストレージアダプタは、ディザスタリカバリのリソースマッピングに含まれる各ESXiホストで手動で設定する必要があります。各ホストでアダプタを個別に設定しないようにするには、SRAワークフローが設定されているSVMを使用して、リカバリサイトにiSCSIタイプのプレースホルダデータストアを作成します。これにより、iSCSIアダプタと必要なデータLIF IPアドレスがマッピングされたすべてのESXiホストに自動的に追加されます。詳細については、["ONTAP toolsでプレースホルダデータストアを設定する"](#)を参照してください。

手順

1. 保護対象サイトで、プライマリESXiホストがプライマリ ストレージ システムのLUNに接続されていることを確認します。
2. プライマリ ストレージ システムで、LUN が `ostype` オプションを `_VMware_` に設定した igroup に属していることを確認してください。
3. 復旧サイトのESXiホストが、ストレージ仮想マシン（SVM）に対して適切なiSCSIおよびファイバーチャネル接続を確立していることを確認してください。セカンダリサイトのESXiホストはセカンダリサイトのストレージにアクセスできる必要があります、プライマリサイトのESXiホストはプライマリサイトのストレージにアクセスできる必要があります。

これは、ESXi ホストに SVM 上にローカル LUN が接続されていることを確認するか、SVM に対して `iscsi show initiators` コマンドを使用することで実行できます。ESXi ホストでマッピングされた LUN への LUN アクセスを確認し、iSCSI 接続を検証してください。

NAS環境向けにSRAを設定する



SRAワークフローでは、NFSの整合性グループはサポートされていません。NFSデータストアボリュームが整合性グループの下に配置され、保護されている場合、デバイスの検出操作は失敗します。SRAを使用してNFSデータストアを保護する場合、整合性グループを使用しないでください。

開始する前に

保護サイトと復旧サイトには、以下のプログラムをインストールしておく必要があります。

- VMware Live Site Recovery : VMware Live Site Recovery のインストール手順書は、VMware サイトで入手できます - ["VMware Live Site Recoveryについて"](#)
- SRA : VMware Live Site Recovery と SRA サーバー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に登録された仮想マシンがあることを確認します。
2. 保護対象サイトのESXiホストが、Storage Virtual Machine（SVM）からのNFSエクスポートボリュームをマウントしていることを確認してください。
3. VMware Live Site Recoveryにアレイを追加するためにArray Managerウィザードを使用する場合、NFSエクスポートが存在する有効なIPアドレスが*NFSアドレス*フィールドに指定されていることを確認してください。*NFSアドレス*フィールドには、NFSホスト名またはFQDNを使用しないでください。
4. 復旧サイトにある各ESXiホストで `ping` コマンドを使用して、ホストにSVMからNFSエクスポートを提供するために使用されるIPアドレスにアクセスできるVMkernelポートがあることを確認します。

大規模環境向けに ONTAP tools で SRA を構成する

大規模環境で最適なパフォーマンスを発揮させるには、ストレージレプリケーションアダプタ（SRA）の推奨設定に従って、ストレージ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

大規模環境向けのVMware Live Site Recoveryでは、以下のタイムアウト値を設定する必要があります。

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

また、`StorageProvider.autoResignatureMode` オプションも有効にしてください。

ストレージプロバイダーの設定変更に関する詳細については、"[Change Storage Provider Settings](#)"を参照してください。

ストレージ設定

タイムアウトが発生した場合は、`storage.commandTimeout` および `storage.maxConcurrentCommandCnt` の値をより大きな値に増やしてください。



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

SAN プロバイダの設定を変更するには、"[Change Storage Settings](#)"を参照してください。

ONTAP tools を使用して VMware Live Site Recovery アプライアンスで SRA を構成する

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

VMware Live Site Recovery アプライアンスで SRA を設定すると、ONTAP tools for VMware vSphere の認証情報がアプライアンス内に保存され、VMware Live Site Recovery と SRA 間の通信が可能になります。

開始する前に

- `.tar.gz` ファイルを "[NetApp サポート サイト](#)" からダウンロードしてください。
- ONTAP tools Manager で SRA サービスを有効にします。詳細については、"[サービスを有効にする](#)" セクションを参照してください。
- vCenter Server を ONTAP tools for VMware vSphere アプライアンスに追加します。詳細については、"[vCenter サーバーの追加](#)" セクションを参照してください。
- ONTAP tools for VMware vSphere にストレージバックエンドを追加します。詳細については、"[ストレージバックエンドを追加する](#)" セクションを参照してください。



ONTAP tools から vCenter 証明書パッチを適用した場合は、(:5480) ポートを使用して VMware Live Site Recovery アプライアンスの vCenter 構成を更新してください。手順については、"[Site Recovery Manager アプライアンスを再構成する](#)" を参照してください。

手順

1. VMware Live Site Recovery アプライアンスの画面で、**Storage Replication Adapter > New Adapter** を選択します。
2. `.tar.gz` ファイルを VMware Live Site Recovery にアップロードします。
3. PuTTYなどのSSHクライアントを使用して、管理者アカウントでVMware Live Site Recoveryアプライアンスにログインします。
4. 以下のコマンドを使用してrootユーザーに切り替えます：`su root`
5. コマンド `'cd /var/log/vmware/srm'` を実行して、ログディレクトリに移動します。
6. ログの保存場所で、SRAが使用するDocker IDを取得するコマンドを入力します：`docker ps -l`
7. コンテナIDにログインするには、次のコマンドを入力してください：`docker exec -it -u srm <container id> sh`
8. 以下のコマンドを使用して、ONTAP tools for VMware vSphere の IP アドレスとパスワードで VMware Live Site Recovery を構成します：`perl command.pl -I --otv-ip <OTV_IP>:8443 --otv -username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Perlスクリプトが特殊文字を区切り文字としてではなくパスワードの一部として扱うように、パスワードをシングルクォーテーションで囲ってください。
 - アプリケーション（VASA Provider/SRA）のユーザー名とパスワードは、これらのサービスを初めて有効にする際に ONTAP tools Manager で設定できます。これらの認証情報を使用して、SRA を VMware Live Site Recovery に登録してください。
 - vCenter の GUID を確認するには、vCenter インスタンスを追加した後、ONTAP tools Manager の vCenter Server ページに移動してください。["vCenter サーバーの追加"](#) セクションを参照してください。
9. アダプタを再スキャンして、更新された詳細情報がVMware Live Site Recovery Storage Replication Adaptersページに表示されていることを確認してください。

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

ONTAP toolsでSRA認証情報を更新する

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

開始する前に

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

手順

1. VMware Live Site Recovery マシンからキャッシュされた ONTAP tools のクレデンシャルを削除するには、次のコマンドを実行します：
 - a. `sudo su <enter root password>`
 - b. `docker ps`

- c. `docker exec -it <container_id> sh`
- d. `cd conf/`
- e. `rm -rf *`

2. Perlコマンドを実行して、新しい認証情報でSRA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>`` パスワードの値はシングルクォーテーション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、および認証情報を使用してSRAサーバーと通信できます。

証明書の変更後に**VMware Live Site Recovery** アプライアンスで**vCenter**を再構成する

vCenter証明書が変更された場合（たとえば、vCenterのアップグレード後）、Site Recovery拡張機能でサムプリントの不一致エラーが発生する可能性があります。この問題を解決するには、次の手順を実行します。

手順

1. VMware Live Site Recovery アプライアンスで vCenter を再構成

- a. ブラウザでVMware Live Site Recoveryアプライアンスの管理インターフェイスを開きます：
`https://<SRM_IP>:5480`
- b. *** Summary *** タブを選択します。
- c. vCenter Server 接続の **Reconfigure** を選択します。

これにより、vCenterから最新の証明書のサムプリントが取得され、受け入れられます。

2. サイトペアリングを再接続してください（エラーが続く場合）

再設定後も指紋不一致エラーが解消されない場合：

- a. vCenterユーザーインターフェイスにログインします。
- b. **Site Recovery** 拡張機能に移動します。
- c. **Site Pairing** セクションを探してください。
- d. ***再接続***を選択して、更新された証明書でサイトペアリングを再確立します。

ONTAP toolsで保護サイトとリカバリサイトを構成する

保護対象サイト上の仮想マシン群を保護するには、保護グループを作成する必要があります。

新しいデータストアを追加する場合、既存のデータストアグループに含めることも、新しいデータストアを追加して保護用の新しいボリュームまたは整合性グループを作成することもできます。保護された整合性グループまたはボリュームに新しいデータストアを追加した後、SnapMirror を更新し、保護サイトとリカバリサイトの両方でストレージ検出を実行します。新しいデータストアが確実に検出され、保護されるように、検出を手動で実行することも、スケジュールに基づいて実行することもできます。

保護対象サイトとリカバリ サイトのペアリング

vSphere Client を使用して作成した保護サイトとリカバリサイトをペアリングすることで、Storage Replication Adapter (SRA) がストレージシステムを検出できるようにする必要があります。



Storage Replication Adapter (SRA) は、Automated Failover Duplexタイプの同期関係が1つと、整合性グループ上の非同期SnapMirror関係が1つのファンアウトをサポートします。ただし、整合性グループ上の2つの非同期SnapMirror関係によるファンアウト、またはボリューム上のSnapMirror関係によるファンアウトはサポートされていません。VaultタイプのSnapMirror関係は、これらのファンアウト制限の対象外です。SRAでの整合性グループのサポートは、UnifiedおよびASA r2ストレージシステムのSANプロトコル (iSCSIおよびファイバーチャネル) に限定されています。NFSでは整合性グループはサポートされていません。NFSデータストアボリュームが整合性グループ下に配置されている場合、デバイス検出操作は失敗します。

開始する前に

- 保護対象サイトと復旧対象サイトの両方に、VMware Live Site Recoveryをインストールしておく必要があります。
- 保護サイトと復旧サイトの両方にSRAをインストールする必要があります。

手順

- vSphere Client のホームページで、**Site Recovery** アイコンをダブルクリックし、**Sites** を選択します。
- オブジェクト > アクション > サイトのペアリング を選択します。
- 「Pair Site Recovery Manager Servers」ダイアログボックスで、保護対象サイトのPlatform Services Controllerのアドレスを入力し、「Next」を選択します。
- [Select vCenter Server]セクションで、次の手順を実行します。
 - 保護対象サイトのvCenter Serverが対応するペア候補として表示されていることを確認します。
 - SSO管理者認証情報を入力し、*完了*を選択します。
- プロンプトが表示されたら、[はい] を選択してセキュリティ証明書を承認してください。

結果

「オブジェクト」ダイアログボックスには、保護サイトと回復サイトの両方が表示されます。

保護グループの設定

開始する前に

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

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

手順

- vCenter Server にログインし、「Site Recovery」>「Protection Groups」を選択します。

2. 「Protection Groups」 ペインで、「New」を選択します。
3. 保護グループの名前と説明、方向を指定し、*次へ*を選択します。
4. *Type*フィールドで、NFSおよびVMFSデータストアの*Type field option...*としてデータストア グループ（アレイ ベースのレプリケーション）を選択します。障害領域は、レプリケーションが有効になっているSVMで構成されます。ピアリングのみが実装されており、問題のないSVMが表示されます。
5. 「Replication groups」 タブで、有効になっているアレイペア、または構成した仮想マシンを含むレプリケーショングループのいずれかを選択し、*Next*を選択します。

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

6. 既存の復旧プランを選択するか、新しい復旧プランに追加 を選択して新しい復旧プランを作成できます。
7. 「完了の準備」 タブで、作成した保護グループの詳細を確認し、**Finish** を選択します。

保護対象サイトとリカバリ サイトのリソースの設定

ONTAP toolsでネットワーク マッピングを設定する

保護サイトから復旧サイトの適切なリソースへ各リソースをマッピングできるように、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両方のサイトで構成する必要があります。

以下のリソース設定を完了してください。

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

開始する前に

保護サイトと復旧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、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいネットワークマッピングを作成するには、管理タブで*Network Mappings* > *New*を選択します。
4. ネットワークマッピング作成ウィザードで、以下の操作を行います。
 - a. 「名前が一致するネットワークのマッピングを自動的に準備する」を選択し、「次へ」を選択します。
 - b. 保護サイトと復旧サイトに必要なデータセンターオブジェクトを選択し、*マッピングの追加*を選択します。
 - c. マッピングが正常に作成されたら、*次へ*を選択してください。
 - d. 以前に逆マッピングを作成するために使用したオブジェクトを選択し、*完了*を選択します。

結果

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

ONTAP toolsでフォルダマッピングを設定する

保護サイトと復旧サイト間で通信を可能にするには、それぞれのフォルダをマッピングする必要があります。

開始する前に

保護サイトと復旧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、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいフォルダマッピングを作成するには、「管理」タブで*フォルダマッピング*>*フォルダー*アイコンを選択します。
4. Create Folder Mappingウィザードで、次の手順を実行します。
 - a. 「名前が一致するフォルダーのマッピングを自動的に準備する」を選択し、「次へ」を選択します。
 - b. 保護サイトと復旧サイトに必要なデータセンターオブジェクトを選択し、*マッピングの追加*を選択します。
 - c. マッピングが正常に作成されたら、*次へ*を選択してください。
 - d. 以前に逆マッピングを作成するために使用したオブジェクトを選択し、*完了*を選択します。

結果

[Folder Mappings]ページに、保護対象サイトのリソースとリカバリ サイトのリソースが表示されます。環境内の他のフォルダについても、同様の手順で操作できます。

ONTAP toolsでリソースマッピングを設定する

保護サイトとリカバリサイトのリソースをマッピングして、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設定する必要があります。

開始する前に

保護サイトと復旧サイトを接続しておく必要があります。



VMware Live Site Recovery では、リソースはリソース プール、ESXi ホスト、またはvSphere クラスターにすることができます。

手順

1. vCenter Server にログインし、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいリソースマッピングを作成するには、管理タブで*リソースマッピング*>*新規*を選択します。
4. Create Resource Mappingウィザードで、次の手順を実行します。

- a. *Automatically Prepare Mappings for Resources with Matching Names*を選択し、*Next*を選択します。
- b. 保護サイトと復旧サイトに必要なデータセンターオブジェクトを選択し、*マッピングの追加*を選択します。
- c. マッピングが正常に作成されたら、*次へ*を選択してください。
- d. 以前に逆マッピングを作成するために使用したオブジェクトを選択し、*完了*を選択します。

結果

リソースマッピングページには、保護対象サイトのリソースと復旧対象サイトのリソースが表示されます。環境内の他のリソースについても、同様の手順で操作できます。

ONTAP toolsでブレースホルダーデータストアを設定する

ブレースホルダーデータストアを構成して、保護対象の仮想マシン（VM）の復旧サイトにおけるvCenterインベントリのスペースを予約します。ブレースホルダーVMは小さく、通常は数百キロバイトしか使用しないため、ブレースホルダーデータストアに必要な容量は最小限です。

開始する前に

- 保護サイトと復旧サイトが接続されていることを確認してください。
- リソースマッピングが正しく設定されていることを確認してください。

手順

1. vCenter Server にログインし、サイトの復旧 > サイト を選択します。
2. 保護対象のサイトを選択し、*管理*を選択します。
3. 新しいブレースホルダーデータストアを作成するには、管理タブで「ブレースホルダーデータストア」>「新規」を選択します。
4. 適切なデータストアを選択し、**OK** をクリックしてください。



ブレースホルダーデータストアはローカルストレージまたはリモートストレージに配置できますが、レプリケーションは必要ありません。

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

ONTAP toolsのアレイマネージャを使用してSRAを設定する

VMware Live Site Recovery のアレイマネージャウィザードを使用してストレージレプリケーションアダプタ（SRA）を構成することで、VMware Live Site Recovery とストレージ仮想マシン（SVM）間の連携を有効にできます。

開始する前に

- VMware Live Site Recoveryで、保護対象サイトと復旧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、オンボーディング済みのストレージを設定しておく必要があります。
- 保護サイトとリカバリサイト間の SnapMirror 関係を設定および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を有効にする必要があります。

SRAは、クラスタレベルの管理とSVMレベルの管理をサポートします。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を検出して操作を実行できるようになります。SVMレベルでストレージを追加すると、その特定のSVMのみを管理できるようになります。

手順

1. VMware Live Site Recoveryで、「Array Managers」>「Add Array Manager」を選択します。
2. VMware Live Site Recovery でアレイを説明するために、以下の情報を入力してください。
 - a. **Display Name** フィールドに、アレイマネージャを識別するための名前を入力してください。
 - b. 「SRA タイプ」フィールドで、「NetApp Storage Replication Adapter for ONTAP」を選択します。
 - c. クラスタまたはSVMへの接続情報を入力します。

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



アレイマネージャを構成する際は、ONTAP tools for VMware vSphere でストレージシステムをオンボーディングする際に使用したのと同じ接続（IPアドレス）をストレージシステムに使用する必要があります。例えば、アレイマネージャの構成がSVMスコープの場合、ONTAP tools for VMware vSphere 配下のストレージはSVMレベルで追加する必要があります。

- d. クラスターに接続する場合は、*SVM名*フィールドにSVM名を指定するか、クラスター内のすべてのSVMを管理する場合は空白のままにしてください。
- e. 検出するボリュームを **Volume include list** フィールドに入力してください。

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

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

- f. （オプション）検出から除外するボリュームを **Volume exclude list** フィールドに入力します。

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

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

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

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

ONTAP toolsで複製されたストレージシステムを検証する

ストレージレプリケーションアダプタ（SRA）の設定後、保護サイトとリカバリサイトが正常にペアリングされていることを確認する必要があります。複製されたストレージシステムは、保護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。

開始する前に

- ストレージシステムを設定しておく必要があります。
- VMware Live Site Recoveryアレイマネージャを使用して、保護サイトとリカバリサイトをペアリングしておく必要があります。
- SRAのテストフェイルオーバー操作およびフェイルオーバー操作を実行する前に、FlexCloneライセンスとSnapMirrorライセンスを有効にしておく必要があります。
- 送信元サイトと送信先サイトで同じSnapMirrorポリシーとスケジュールを設定する必要があります。
- カスタムスケジュールを設定したカスタムSnapMirrorポリシーを使用している場合は、保護サイトと復旧サイトの両方で同じスケジュールとポリシーを設定する必要があります。
- カスタムSnapMirrorポリシー（デフォルトまたはカスタムスケジュールのいずれか）を使用している場合は、新しいポリシーが認識されるように、ONTAP toolsからストレージ検出を実行する必要があります。これを行わないと、テストフェイルオーバーやフェイルオーバーを含むSRAワークフローが失敗します。次のポイントでストレージ検出を実行します：
 - 復旧サイトでカスタムポリシーを作成した後。
 - 保護対象サイトでポリシーを再作成する再保護処理の実行後。

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てください。

ストレージシステムは、保護サイトとリカバリサイトで有効のステータスで検出される必要があります。

ONTAP toolsのファンアウト保護

ファンアウト保護シナリオでは、整合性グループは最初の宛先 ONTAP クラスターとの同期関係、および2番目の宛先 ONTAP クラスターとの非同期関係によって二重に保護されます。作成、編集、削除の SnapMirror アクティブ同期保護ワークフローは、同期保護を維持します。VMware Live Site Recovery アプライアンスのフェイルオーバーおよび再保護ワークフローは、非同期保護を維持します。



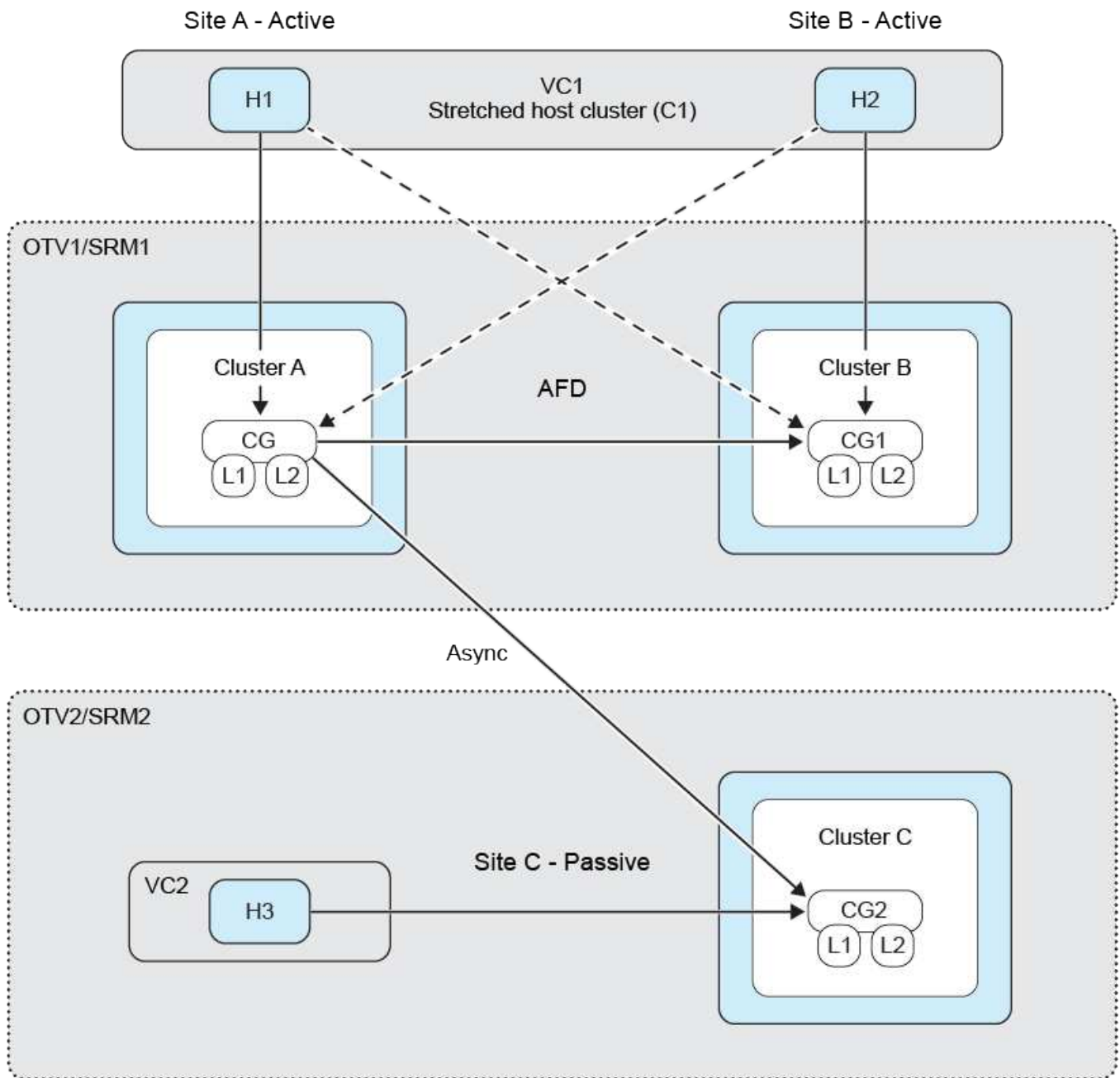
ファンアウトはSVMユーザーではサポートされていません。

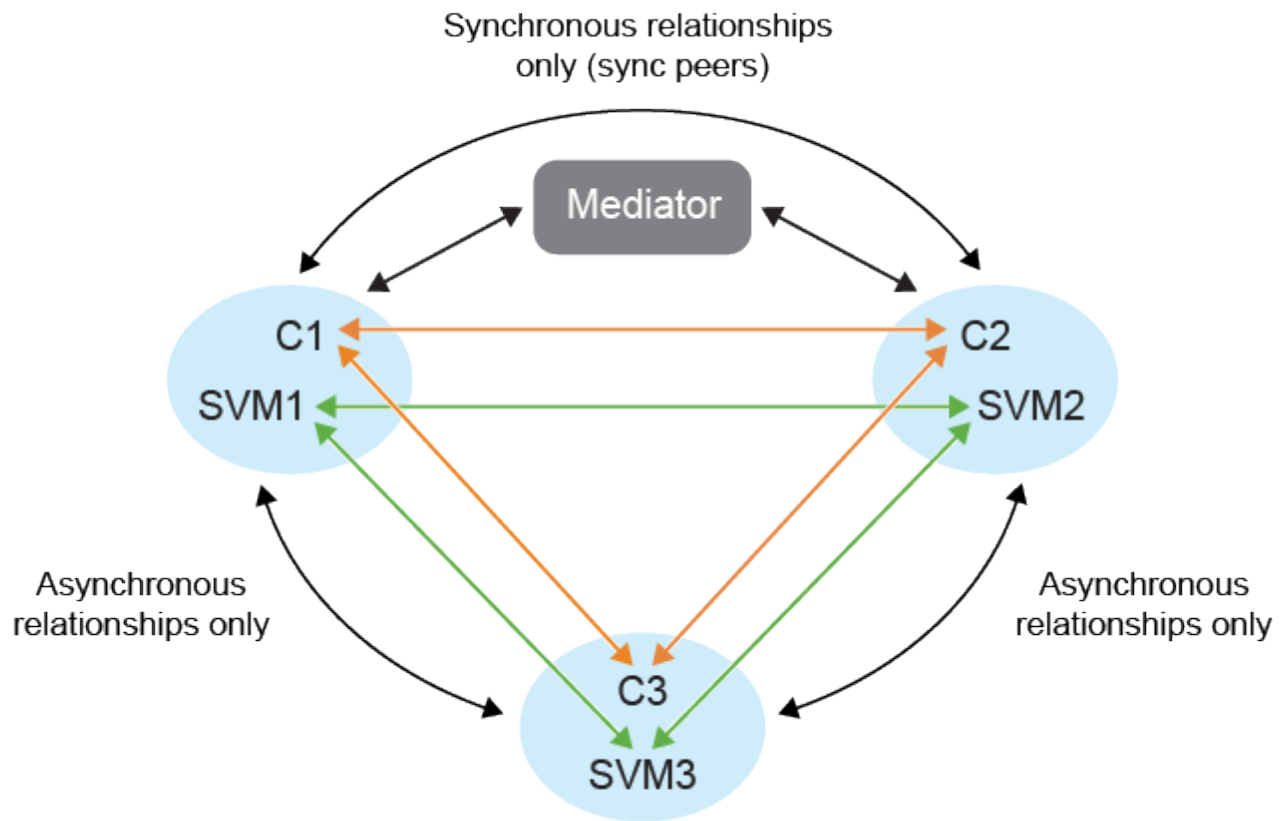
ファンアウト保護を設定するには、3つのサイトクラスターとSVMをピアリングします。

例：

実行している場合、	操作
• ソース整合性グループはクラスターc1とSVM svm1上にあります • 最初の宛先整合性グループはクラスター c2 と SVM svm2 上にあり、 • 2番目の宛先整合性グループはクラスター c3 と SVM svm3 上にあります	• ソース ONTAP クラスターのクラスタピアリングは（C1、C2）と（C1、C3）になります。 • 最初の宛先 ONTAP クラスターのクラスタピアリングは（C2、C1）と（C2、C3）となり、 • 2番目の宛先 ONTAP クラスターでのクラスタピアリングは（C3、C1）と（C3、C2）になります。 • ソースSVM上のSVMピアリングは（svm1, svm2）および（svm1, svm3）になります。 • 最初の宛先SVMでのSVMピアリングは（svm2, svm1）と（svm2, svm3）になり、 • 2番目の宛先SVMにおけるSVMピアリングは（svm3, svm1）および（svm3, svm2）となります。

次の図は、ファンアウト保護設定を示しています
：





手順

1. 新しいプレースホルダーデータストアを選択してください。段階的保護のためのプレースホルダーデータストア選択基準は以下のとおりです：
 - 保護対象のホストクラスタ内にプレースホルダーデータストアを配置しないでください。
 - ホスト クラスタにプレースホルダ データストアを含める必要がある場合は、SnapMirror アクティブ 同期保護を設定する前に、VMware Live Site Recovery アプライアンスに追加してください。この設定では、プレースホルダ データストアを保護対象から外すことができます。

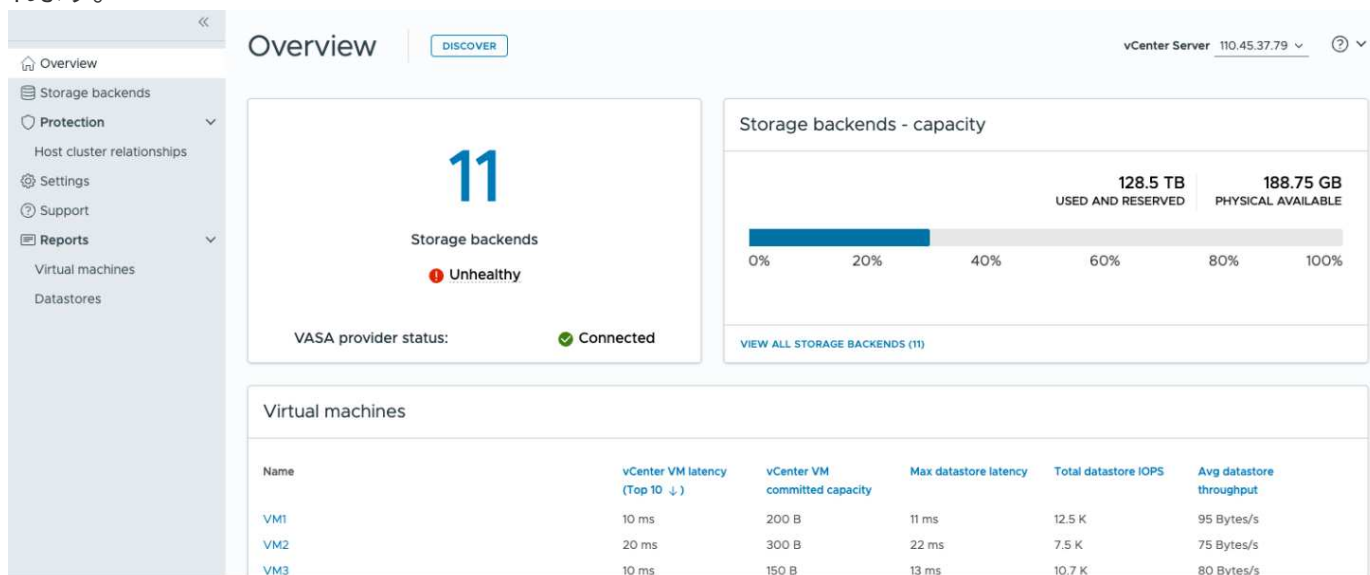
詳細については、"[プレースホルダーデータストアを選択してください](#)"を参照してください。
2. "[保護されたホストクラスタを変更する](#)"に従って、データストアをホストクラスタ保護に追加します。非同期ポリシータイプと同期ポリシータイプの両方を追加します。

ONTAP tools for VMware vSphereの管理

ONTAP toolsダッシュボードについて学ぶ

vCenterクライアントのショートカット セクションからONTAP tools for VMware vSphereプラグインのアイコンを選択すると、概要ページが開きます。このダッシュボードには、ONTAP tools for VMware vSphereプラグインの概要が表示されます。

拡張リンクモード（ELM）では、vCenter サーバのドロップダウンが表示されます。vCenter サーバを選択して、そのデータを表示します。ドロップダウンは、プラグインのすべてのリスト表示で使用できます。あるページで vCenter サーバを選択すると、プラグインでタブを切り替えても同じサーバが選択された状態が維持されます。



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



Discovery ボタンは、検出を実行するために必要な権限を持っている場合にのみ有効になります。

検出リクエストを送信すると、最近のタスクパネルでアクションの進捗状況を追跡できます。

ダッシュボードには、システムのさまざまな要素を示す複数のカードが表示されます。以下の表は、各種カードとその意味を示しています。

カード	概要
-----	----

ステータス	ステータスカードには、ストレージバックエンドの数と、ストレージバックエンドおよびVASA Providerの全体的な健全性ステータスが表示されます。ストレージバックエンドのステータスは、すべてのストレージバックエンドのステータスが正常な場合は*正常*と表示され、いずれかのストレージバックエンドに問題がある場合（不明/到達不能/低下ステータス）は*異常*と表示されます。ツールチップを選択すると、ストレージバックエンドのステータスの詳細が表示されます。詳細については、任意のストレージバックエンドを選択してください。*その他のVASA Providerの状態*リンクには、vCenter Serverに登録されているVASA Provider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集計された使用済み容量と利用可能容量が表示されます。ASA r2ストレージシステムでは、ストレージが分離されているため、容量データは表示されません。
仮想マシン	このカードには、パフォーマンス指標に基づいてソートされた上位10台の仮想マシンが表示されます。ヘッダーを選択すると、選択したメトリックの上位10台の仮想マシンが昇順または降順で表示されます。カード上で行った並べ替えやフィルタリングの変更は、ブラウザのキャッシュを変更またはクリアするまで保持されます。
データストア	このカードには、パフォーマンス指標に基づいてソートされた上位10個のデータストアが表示されます。ヘッダーを選択すると、選択したメトリックの上位10件のデータストアが昇順または降順で表示されます。カード上で行った並べ替えやフィルタリングの変更は、ブラウザのキャッシュを変更またはクリアするまで保持されます。データストアのタイプ（NFS、VMFS、または vVols）を選択するためのデータストアタイプのドロップダウンがあります。
ESXi ホストコンプライアンスカード	このカードには、すべての ESXi ホスト（選択したvCenterの場合）が、グループまたはカテゴリ別に推奨されるNetAppホスト設定に従っているかどうかが表示されます。*推奨設定を適用*リンクを選択すると、推奨設定を適用できます。ホストのコンプライアンスステータスを選択すると、ホストのリストが表示されます。

ONTAP toolsがigroupとエクスポートポリシーを管理する方法

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

ONTAP tools for VMware vSphere 9.x では、igroup はフラット構造で作成および管理され、vCenter 内の各データストアは単一の igroup に関連付けられていました。このモデルでは、複数のデータストア間での igroup の柔軟性と再利用性が制限されていました。ONTAP tools for VMware vSphere ではネストされた igroup が導入され、vCenter 内の各データストアは親 igroup に関連付けられ、各ホストはその親の下にある子 igroup にリンクされています。igroup の管理を容易にするために、ユーザー定義の名前を持つカスタム親 igroup を定義して、データストア間で再利用することができます。ONTAP tools for VMware vSphere で LUN とデータストアを管理するための igroup ワークフローを理解してください。ワークフローが異なると、生成される igroup 構成も異なります。以下の例を参照してください：



記載されている名称はあくまで例示であり、実際のigroup名を指すものではありません。ONTAP tools で管理されるigroupは「otv_」という接頭辞を使用します。カスタムigroupには任意の名前を付けることができます。

期間	説明
DS<number>	データストア
iqn<number>	イニシエーターIQN
ホスト<number>	ホストMoRef
lun<number>	LUN ID
<DSName>igroup<number>	デフォルト（ONTAP tools管理）親igroup
<Host-Moref>igroup<number>	子イニシエータグループ
Customlgroup<number>	ユーザー定義のカスタム親igroup
Classiclgroup<number>	lgroup は、ONTAP tools 9.x バージョンで使用されません。

例1：

1つのイニシエータを使用して、単一ホスト上にデータストアを作成する

ワークフロー: [作成] DS1 (lun1): host1 (iqn1)

結果：

- DS1lgroup :
 - host1lgroup → (iqn1: lun1)

ONTAP は DS1 の親 igroup DS1lgroup を作成し、子 igroup host1lgroup を lun1 にマッピングします。システムは常に LUN を子 igroup にマッピングします。

例2：

既存のデータストアを別のホストにマウントする

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

結果：

- DS1lgroup :
 - host1lgroup → (iqn1: lun1)

- host2lgroup → (iqn2: lun1)

ONTAP tools for VMware vSphere は、子 igroup host2lgroup を作成し、既存の親 igroup DS1lgroup に追加します。

例3：

ホストからデータストアをアンマウントする

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

結果：

- DS1lgroup：
 - host2lgroup → (iqn2: lun1)

ONTAP tools for VMware vSphere は、host1lgroup を階層構造から削除します。システムは子 igroup を明示的に削除しません。以下の 2 つの条件下で削除されます：

- LUNがマッピングされていない場合、ONTAPシステムは子igroupを削除します。
- スケジュールされたクリーンアップジョブによって、LUNマッピングのない孤立した子igroupが削除されます。これらのシナリオは、ONTAP tools で管理される igroup にのみ適用され、カスタム作成された igroup には適用されません。

例4：

データストアの削除

ワークフロー：[削除] DS1 (lun1): host2 (iqn2)

結果：

- DS1lgroup：
 - host2lgroup → (iqn2: lun1)

親igroupと子igroupは、別のデータストアが親igroupを再利用しない限り削除されます。子igroupは明示的に削除されません

例5：

カスタム親igroupの下に複数のデータストアを作成する

ワークフロー：

- 【作成】 DS2 (lun2)： host1 (iqn1), host2 (iqn2)
- 【作成】 DS3 (lun3)： host1 (iqn1), host3 (iqn3)

結果：

- Customlgroup1：
 - host1lgroup → (iqn1: lun2、lun3)
 - host2lgroup → (iqn2 : lun2)

- host3lgroup → (iqn3 : lun3)

Customlgroup1はDS2用に作成され、DS3で再利用されます。子iグループは、共有親iグループの下で作成または更新され、各子iグループは関連するLUNにマッピングされます。

例6：

カスタム親igroupの下にあるデータストアを1つ削除します。

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

結果：

- Customlgroup1：
 - host1lgroup → (iqn1 : lun3)
 - host3lgroup → (iqn3 : lun3)
- Customlgroup1は再利用されませんが、削除もされません。
- LUNがマッピングされていない場合、ONTAPシステムはhost2lgroupを削除します。
- host1lgroupはDS3のlun3にマッピングされているため、削除されません。カスタムigroupは、再利用状況に関わらず、削除されることはありません。

例7：

vVolsデータストアの拡張（ボリュームの追加）

ワークフロー：

拡張前：

[展開] DS4 (lun4) : host4 (iqn4)

- DS4lgroup : host4lgroup → (iqn4 : lun4)

拡張後：

[展開] DS4 (lun4, lun5) : host4 (iqn4)

- DS4lgroup : host4lgroup → (iqn4 : lun4, lun5)

新しいLUNが作成され、既存の子igroup host4lgroupにマッピングされます。

例8：

vVolsデータストアの縮小（ボリュームの削除）

ワークフロー：

縮小前：

[縮小] DS4 (lun4, lun5) : host4 (iqn4)

- DS4lgroup : host4lgroup → (iqn4 : lun4, lun5)

縮小後：

【縮小】 DS4 (lun4) : host4 (iqn4)

- DS4lgroup : host4lgroup → (iqn4 : lun4)

指定されたLUN (lun5) は、子igroupからマッピング解除されました。igroupは、少なくとも1つのマッピングされたLUNが存在する限り、アクティブな状態を維持します。

例9：

ONTAP tools 9 から 10 への移行 (igroup 正規化)

ワークフロー

ONTAP tools for VMware vSphere 9.x バージョンは、階層型 igroup をサポートしていません。バージョン 10.3 以降への移行時には、igroup を階層構造に正規化する必要があります。

移行前：

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

ONTAP tools 9.xのロジックでは、1対1のホストマッピングを強制することなく、igroupごとに複数のイニシエータを許可できます。

移行後：

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

移行中：

- 新しい親igroup (Classiclgroup1) が作成されます。
- 元のigroupはotv_という接頭辞を付けて名前が変更され、子igroupになります。

これにより、階層モデルへの準拠が保証されます。

ONTAP tools 10.5P2以降では、移行されたigroupは使用されなくなると削除されます。以前のバージョンでは、移行されたigroupは削除されませんでした。以下の点に注意してください：

- 移行されたigroupは、データストア間で再利用できません。
- カスタムigroup (ユーザー定義) は削除されず、引き続き再利用できます。

関連トピック

["igroupについて"](#)

エクスポート ポリシー

エクスポートポリシーは、ONTAP tools for VMware vSphere における NFS データストアへのアクセスとクライアントの権限を制御します。エクスポートポリシーは ONTAP システムで作成および管理され、NFS データストアと組み合わせてアクセス制御を適用するために使用できます。各エクスポートポリシーは、アクセスを許可するクライアント (IP アドレスまたはサブネット) と付与される権限 (読み取り専用または読み書き

可能)を指定するルールで構成されます。

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

新しいESXiホストにNFSデータストアをマウントすると、ONTAP tools for VMware vSphereは、データストアに関連付けられている既存のエクスポートポリシーにホストのIPアドレスを追加します。これにより、新しいホストは新しいエクスポートポリシーを作成することなくデータストアにアクセスできるようになります。

ESXi ホストから NFS データストアを削除またはアンマウントすると、ONTAP tools for VMware vSphere はホストの IP アドレスをエクスポートポリシーから削除します。他のホストがそのエクスポートポリシーを使用していない場合、そのポリシーは削除されます。NFS データストアを削除すると、ONTAP tools for VMware vSphere は、他のデータストアで再利用されていない場合、そのデータストアに関連付けられているエクスポートポリシーを削除します。エクスポートポリシーが再利用される場合、ホストの IP アドレスは維持され、変更されません。データストアを削除すると、エクスポートポリシーはホストの IP アドレスの割り当てを解除し、デフォルトのエクスポートポリシーを割り当てます。これにより、ONTAP システムは必要に応じてそれらにアクセスできます。

エクスポートポリシーを異なるデータストア間で再利用する場合、その割り当て方法は異なります。エクスポートポリシーを再利用する場合、ポリシーに新しいホストIPアドレスを追加できます。共有エクスポートポリシーを使用するデータストアを削除またはアンマウントしても、ポリシー自体は削除されません。ポリシーは変更されず、他のデータストアと共有されているため、ホストIPアドレスも削除されません。エクスポートポリシーの再利用は、アクセスや遅延の問題を引き起こす可能性があるため、推奨されません。

関連トピック

["エクスポート ポリシーの作成"](#)

ONTAP toolsによるigroupの管理方法

ONTAP tools VMとONTAPストレージシステムの両方を管理する場合、特にONTAP toolsで管理されていない環境から管理されている環境へデータストアを移動する際には、igroupの動作を理解することが重要です。このページでは、ONTAP tools for VMware vSphereがigroupをどのように表現し管理するかについて説明します。これは、以前のリリースと現在のネストされたigroupモデルとの間の動作の違いを理解するための概念的な情報です。

ONTAP tools for VMware vSphere 10.4以降、ONTAP toolsはONTAPおよびvCenterオブジェクトを自動的に作成および維持し、VMwareデータセンター環境におけるデータストア管理を簡素化します。ONTAP tools for VMware vSphere 10.5 P2以降、移行されたigroupは使用されなくなると自動的に削除されます。

簡単な動作概要

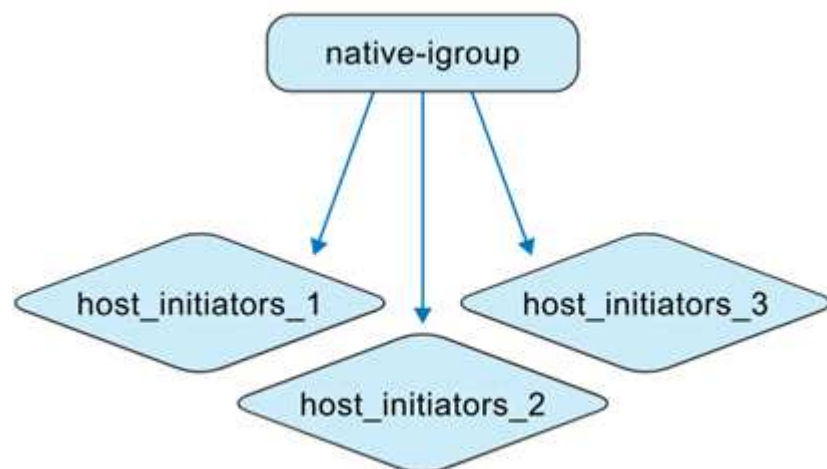
- ONTAP tools で管理される VMFS データストアは、ネストされた igroup を使用します（データストアコンテキストごとに 1 つの親 igroup、ホストごとに子 igroup）。
- LUNマッピングは子igroupに適用されます。
- カスタム親igroupは、複数のデータストア間で再利用できます。
- ONTAP tools 9.xから移行されたigroupは再利用できません。

igroup コンテキスト

ONTAP tools for VMware vSphereは、igroupを2つのコンテキストで処理します。

ONTAP以外のツールで管理されるigroup

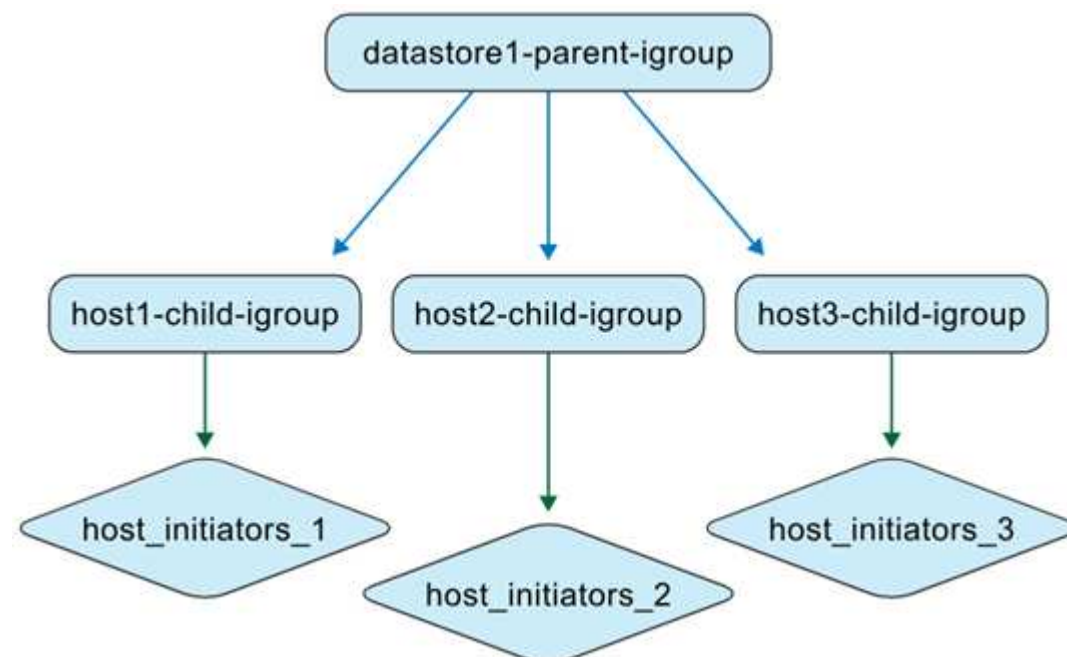
ストレージ管理者は、ONTAPシステム上でigroupをフラット構造またはネスト構造として作成できます。次の図は、ONTAPで直接作成されたフラットigroupを示しています。

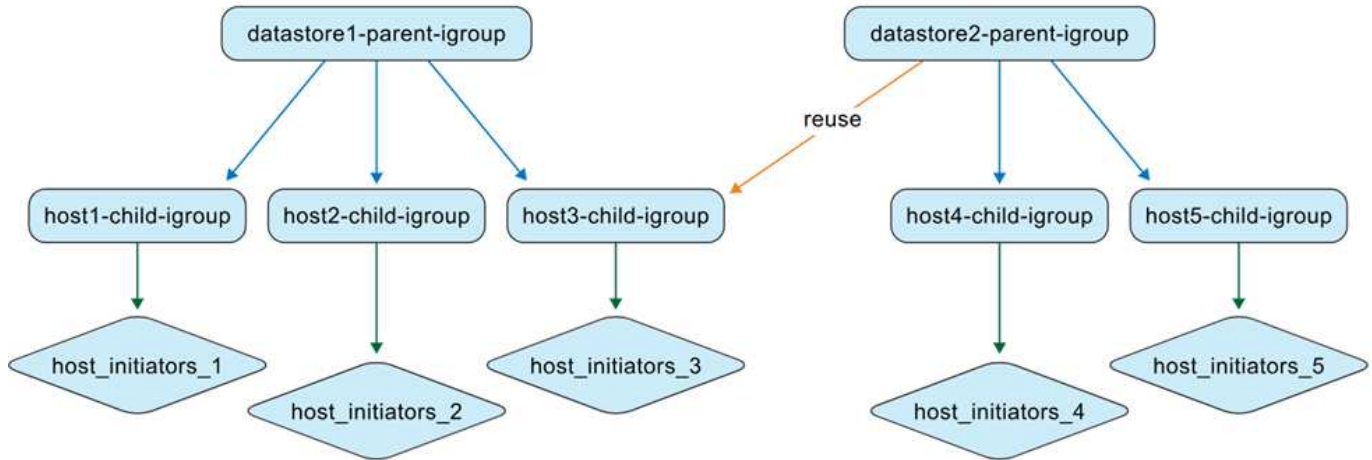


ONTAP tools が管理する igroup

データストアを作成すると、ONTAP tools for VMware vSphereはネスト構造でigroupを作成します。

例えば、datastore1 が作成されてホスト 1、2、3 にマウントされ、新しいデータストア（datastore2）が作成されてホスト 3、4、5 にマウントされた場合、ONTAP tools は効率的な管理のためにホストレベルの igroup を再利用します。





命名の動作

データストアを作成し、igroupフィールドを空白のままにすると、ONTAP toolsは、デフォルトでネストされたigroup構造を作成します。

- 親igroupの命名パターン：
otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>
- 子igroupの命名パターン： otv_<hostMoref>_<vcguid>

ONTAP システムインターフェースでは、*親イニシエータグループ*フィールドに親igroupと子igroup間の関係が表示されます。

シナリオ別の動作

シナリオ	親igroupの動作	子 igroup の動作	LUNのマッピングと可視性
デフォルトのigroup設定で作成されたデータストア	デフォルトの ONTAP tools で管理される親igroup が作成されます。	ホストレベルの子igroupは必要に応じて作成されます。	LUNは子igroupにマッピングされます。データストアはvCenter Serverインベントリに表示されます。
カスタムigroup名で作成されたデータストア	指定された名前でカスタム親igroupが作成されます。	ホストが重複する場合、既存のホストレベルの子igroupが再利用されます。	新しいデータストアLUNは、再利用または新規作成された子igroupにマッピングされます。データストアはvCenter Serverに表示されます。
データストア作成時に既存のカスタムigroupが再利用されます	既存のカスタム親igroupが選択され、再利用されます。	子igroupは、ホストのメンバーシップに基づいて再利用または拡張されます。	新しいデータストアLUNは、関連付けられた子igroupを介してマッピングされます。データストアはvCenter Serverに表示されます。

シナリオ	親igroupの動作	子 igroup の動作	LUNのマッピングと可視性
データストアとigroupはONTAPとvCenterでネイティブに作成され、その後ONTAP toolsによって検出されます	ONTAP toolsは、管理コンテキスト内に親igroupを作成し、元のigroup名を保持します。	ONTAP tools for VMware vSphereは、元のigroupの名前を `otv_` プレフィックスで変更し、階層内で子igroupとして表します。	イニシエータのマッピングは変更されません。データストアにマッピングされたigroupのみが、検出時に変換されます。

カスタムigroupの再利用とAPIの動作

ONTAP tools のユーザーインターフェイスでは、データストアを作成する際に、ドロップダウンリストから既存のカスタム親igroupを再利用できます。

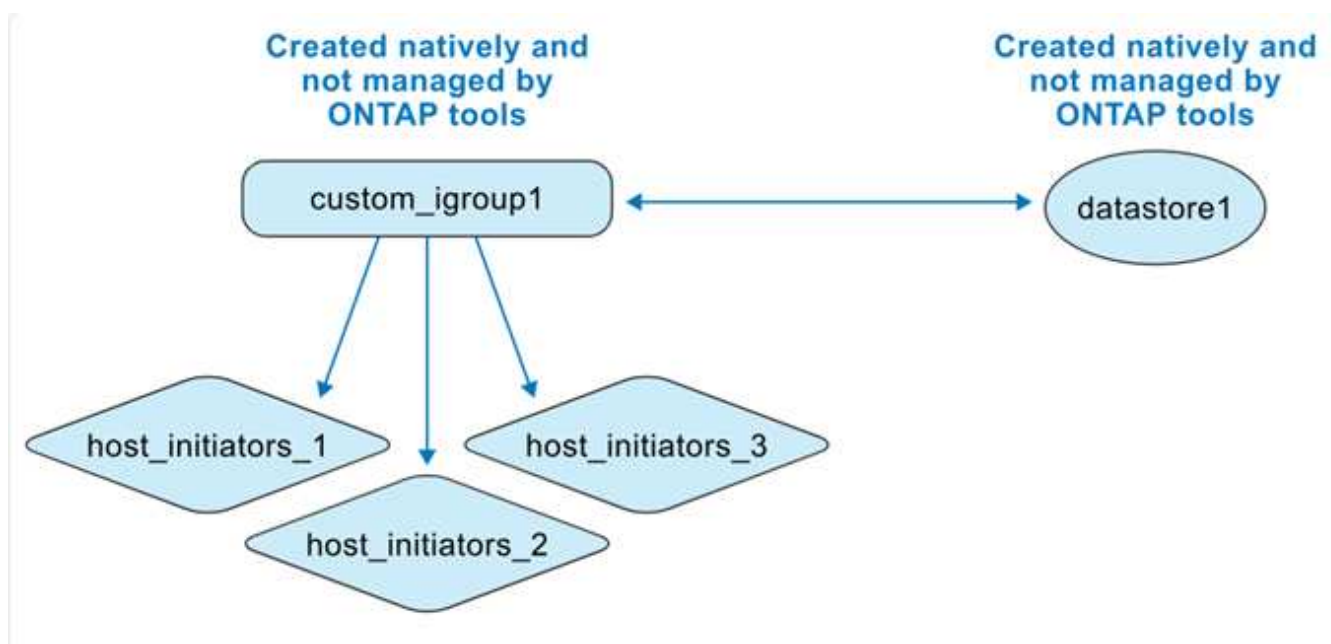
API を通じても同様の動作がサポートされています。データストアの作成時に既存の igroup を再利用するには、API リクエストのペイロードに igroup の UUID を指定します。



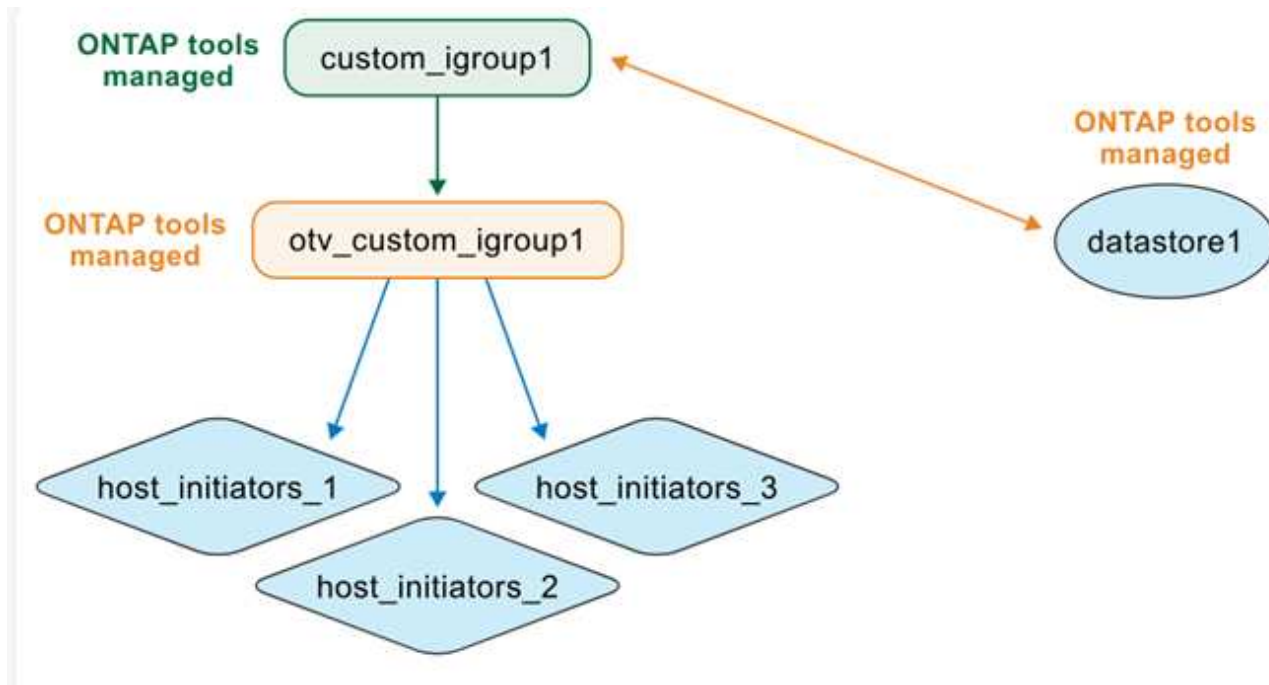
再利用できるのはカスタムigroupのみです。ONTAP tools 9.xから移行されたigroupは再利用できず、ONTAP tools 10.5 P2以降では、使用されなくなると自動的に削除されます。

ネイティブからマネージドへの変換ビュー

ONTAP システムおよびVMware環境でigroupとデータストアを直接作成する場合、ONTAP tools は初期状態ではこれらのオブジェクトを管理しません。これにより、フラットなigroup構造になります。



データストア検出後、ONTAP toolsは、データストアにマッピングされたigroupを識別して登録し、それらをネストされたモデルで表現します。親igroupはデータストアレベルで表現され、既存のigroupは `otv\_` プレフィックスを持つ子igroupとして名前が変更され、イニシエータのマッピングは変更されません。



ONTAP tools for VMware vSphereは、ONTAPシステムで作成されたigroupのうち、データストアにマッピングされていないか、ONTAP toolsにリンクされていないigroupを検出または管理しません。検出時に、ONTAP toolsは検出されたデータストアにマッピングされているigroupのみを変換します。その他のigroupは管理対象外のままです。

検出されたネイティブigroupの再利用

ONTAP tools が検出されたネイティブ igroup を管理すると、その igroup はデータストア作成用のカスタムイニシエータグループ名のドロップダウンリストで使えるようになります。

新しいデータストアLUNは、正規化された子igroupにマッピングされます。例：otv_NativeIgroup1

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

ONTAP toolsマネージャのユーザーインターフェイスについて学ぶ

ONTAP tools for VMware vSphereはマルチテナンシーをサポートし、複数のvCenter Serverインスタンスの管理を可能にします。

ONTAP tools Manager は、ONTAP tools for VMware vSphere、vCenter Server インスタンス、ストレージバックエンド、および高可用性（HA）やノードスケーリングなどのアプライアンス構成を管理するための Web ベースのコンソールです。

ONTAP tools Managerは以下の機能を提供します：

- アラートの管理 - ONTAP tools for VMware vSphere によって生成されたアラートを表示およびフィルタリングします。
- ストレージバックエンドの管理 - ONTAPストレージクラスタを追加および管理し、グローバルにvCenter

Serverインスタンスにマッピングします。

- vCenter Server インスタンスの管理 - ONTAP tools 内で vCenter Server インスタンスを追加および管理します。
- ジョブの監視 - ONTAP tools プラグイン インターフェイスと ONTAP tools Manager インターフェイスの両方から開始された非同期ジョブを監視およびデバッグします。期間を指定してジョブを絞り込んだり、ページ サイズを調整したり、エラーやサブタスクを含むジョブの詳細を表示したりできます。エラーの詳細を表示するには、失敗ステータスをクリックしてください。サブタスクのあるジョブの場合は、行を展開して説明とステータスを確認してください。サブジョブについては、ジョブのドリルダウン機能を使用して詳細を表示してください。
- ログバンドルのダウンロード - ONTAP tools for VMware vSphere のトラブルシューティング用のログファイルを収集します。
- 証明書の管理 - 自己署名証明書をカスタム CA 証明書に置き換え、VASA Provider と ONTAP tools の証明書を更新またはリフレッシュします。
- パスワードのリセット - VASA ProviderとSRAのパスワードを変更します。
- アプライアンス設定の管理 - HA の有効化やノードサイズのスケールアップなど、ONTAP tools アプライアンスを設定します。

ONTAP tools Manager にアクセスするには、ブラウザから `https://<ONTAPtoolsIP>:8443/virtualization/ui/` を起動し、デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報でログインしてください。

ONTAP tools Manager

Overview

EDIT APPLIANCE SETTINGS

Appliance

Healthy

Size: Small

HA: Enabled

VASA Provider: Enabled

SRA: Enabled

VIEW DETAILS

Alerts

Last 24 hours

No alerts

VIEW ALL ALERTS (0)

vCenters

1 Healthy

VIEW ALL VCENTERS (1)

Storage backends

No storage backends added

VIEW ALL STORAGE BACKENDS (0)

ONTAP tools nodes

vee-lab3-vm41

Healthy

Deploy_OVA_b29c029_998

VIEW DETAILS

vee-lab3-vm184

Healthy

Deploy_OVA_b29c029_9982

VIEW DETAILS

vee-lab3-vm187

Healthy

Deploy_OVA_b29c029_9983

VIEW DETAILS

カード	概要
アプライアンスカード	アプライアンス カードには、ONTAP tools アプライアンスの全体的なステータス、構成の詳細、および有効になっているサービスのステータスが表示されます。詳細情報を表示するには、「詳細を表示」リンクを選択してください。アプライアンスの設定を変更すると、変更が完了するまで、カードにジョブのステータスと詳細が表示されます。
アラートカード	アラートカードには、HAノードレベルのアラートを含め、種類別に分類されたONTAP toolsのアラートが表示されます。カウントのハイパーリンクをクリックすると、詳細なアラートを表示できます。クリックすると、選択したアラートタイプでフィルタリングされたアラートページに移動します。
vCentersカード	vCentersカードには、ONTAP toolsが管理するすべてのvCenter Serverインスタンスの正常性ステータスが表示されます。対応するリンクを選択すると、選択したインスタンスに関する詳細情報が掲載されているページに移動し、各vCenterの詳細を確認できます。
ストレージバックエンドカード	ストレージバックエンドカードには、ONTAP tools で設定されたすべての ONTAP ストレージクラスタの健全性と接続状態が表示されます。対応するリンクを選択すると、選択したクラスタに関する詳細情報が掲載されたページに移動し、各ストレージバックエンドの詳細を確認できます。
ONTAP tools ノードカード	ONTAP tools のノードカードには、アプライアンス内のすべてのノードが表示されます。これには、ノード名、VM名、ステータス、ネットワーク情報が含まれます。特定のノードの詳細情報を表示するには、*詳細を表示*を選択してください。[NOTE] 非HA構成では、ノードは1つしか表示されません。HA構成では、3つのノードが表示されます。

ONTAP tools Manager の設定を管理する

ONTAP toolsのAutoSupport設定を編集する

ONTAP tools for VMware vSphereを初めて設定する際、AutoSupportはデフォルトで有効になっています。有効化されてから24時間後に、テクニカルサポートにメッセージを送信します。

AutoSupport を無効にする

AutoSupport を無効にすると、プロアクティブなサポートおよびモニタリングを受けられなくなります。



AutoSupport は、問題の検出と解決を迅速化するのに役立つため、有効のままにしておくことをお勧めします。AutoSupport が無効になっている場合でも、システムは引き続きローカルで情報を収集および保存しますが、ネットワーク経由でレポートを送信しません。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 設定 > テレメトリ > 編集 オプションを選択します。
4. **AutoSupport** オプションの選択を解除して、変更を保存します。

AutoSupport プロキシ URLの更新

AutoSupport プロキシ URL を更新して、AutoSupport 機能がセキュアな送信のためにプロキシ サーバ経由でデータをルーティングするようにします。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから*設定*を選択してください。
4. 設定 > テレメトリ > 編集 オプションを選択します。
5. 有効な **Proxy URL** を入力して変更を保存してください。

AutoSupportを無効にすると、プロキシURLも無効になります。

ONTAP toolsにNTPサーバーを追加する

NTPサーバーの詳細を入力して、ONTAP tools アプライアンスの時刻を同期します。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 設定 > **NTPサーバー** > 編集 オプションを選択します。
4. カンマ区切りの完全修飾ドメイン名 (FQDN) 、IPv4アドレス、またはIPv6アドレスを入力してください。

画面を更新して、更新された値を確認してください。

ONTAP toolsでVASA ProviderとSRAの認証情報をリセットする

VASA Provider または SRA の認証情報を忘れた場合は、ONTAP tools Manager インターフェイスを使用して新しいパスワードにリセットできます。新しいパスワードは 8 文字以上 256 文字以下にする必要があります。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 設定 > **VASA Provider / SRA credentials** > **Reset Password** オプションを選択してください。
4. 新しいパスワードを入力し、確認します。
5. 変更を適用するには、*保存*を選択してください。

ONTAPツールのバックアップ設定を編集する

ONTAP tools for VMware vSphere 10.5 以降、バックアップ機能はデフォルトで有効になっており、10分ごとにバックアップが作成されます。バックアップを無効にするか、バックアップの頻度を変更することができます。

バックアップを無効にしないでください。無効にすると、ONTAP tools が低い RPO を維持できなくなります。バックアップを無効にしても、既存のバックアップファイルは削除されません。バックアップの頻度は、10 分から 60 分の間の値に変更できます。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 設定 > バックアップ > 編集 オプションを選択します。
4. 編集ウィンドウでは、バックアップを無効にしたり、バックアップの頻度を編集したりできます。

ONTAP toolsサービスを有効にする

ONTAP tools Manager を使用して管理者パスワードを変更することで、VASA プロバイダーなどのサービスの有効化、vVols 構成のインポート、および ONTAP tools Manager を使用したディザスタリカバリ（SRA）を利用できます。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 概要セクションで*アプライアンス設定の編集*を選択してください。
4. 「サービス」セクションでは、必要に応じて VASA プロバイダー、vVols 構成のインポート、ディザスタリカバリ（SRA）などのオプションサービスを有効にできます。

サービスを初めて有効にする際には、VASA プロバイダーと SRA の認証情報を作成する必要があります。これらは、vCenter サーバで VASA プロバイダーおよび SRA サービスを登録または有効化するために使用されます。ユーザー名には、英字、数字、アンダースコアのみを使用できます。パスワードの長さは 8 文字から 256 文字の間である必要があります。



オプションのサービスを無効にする前に、ONTAP tools で管理されている vCenter Server がそれらのサービスを使用していないことを確認してください。

*vVols 設定のインポートを許可する*オプションは、VASA プロバイダーサービスが有効になっている場合にのみ表示されます。このオプションを使用すると、ONTAP tools 9.xx から ONTAP tools 10.5 への vVols データ移行が可能になります。

ONTAP tools アプライアンスの設定を変更する

ONTAP tools Manager を使用して、ノード数を増やすか、高可用性（HA）を有効にすることで、ONTAP tools for VMware vSphere の構成をスケールアップします。デフォルトでは、ONTAP tools for VMware vSphere アプライアンスは、単一ノードの非 HA 構成で導入されます。

開始する前に

- OVA テンプレートの OVA バージョンがノード 1 と同じであることを確認してください。ノード 1 はデフォルト ノードで、ONTAP tools for VMware vSphere OVA が最初に展開されます。
- CPU のホット アドとメモリのホットプラグが有効になっていることを確認してください。
- vCenter Server で、ディザスタリカバリサービス（DRS）の自動化レベルを「部分自動化」に設定します。HA を導入した後、完全自動化に戻してください。
- HA 構成におけるノードのホスト名は小文字で指定する必要があります。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 概要セクションで*アプライアンス設定の編集*を選択してください。
4. 「構成」セクションで、ノードサイズをスケールアップし、HA 構成を有効にします。vCenter Server の認証情報を使用して変更を行います。

HA 構成では、コンテンツライブラリの詳細を変更できます。編集ごとにパスワードを入力してください。



ONTAP tools for VMware vSphere では、ノードサイズを増やすことのみが許可されており、ノードサイズを小さくすることはできません。非 HA 構成では、中規模構成のみがサポートされます。HA 構成では、中規模および大規模構成がサポートされます。

5. HA 切り替えボタンを使用して、HA 構成を有効にします。*HA 設定*ページで、以下の点を確認してください：
 - コンテンツライブラリは、ONTAP tools ノード VM が実行されているのと同じ vCenter サーバーに属しています。vCenter サーバーの認証情報は、アプライアンスの変更に使用する OVA テンプレートの検証およびダウンロードに使用されます。
 - ONTAP tools をホストする仮想マシンは、ESXi ホストに直接デプロイされません。VM はクラスターまたはリソース プールにデプロイする必要があります。



HA構成を有効にした後は、HA構成ではないシングルノード構成に戻すことはできません。

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



ONTAP tools は、ワークフローを簡素化するために、ほとんどの入力オプションにノード 1 のネットワーク詳細情報を事前に入力します。ウィザードの最終ページに進む前に、入力データを編集できます。他の 2 つのノードの IPv6 アドレスの詳細を入力できるのは、ONTAP tools 管理ノードで IPv6 アドレスが有効になっている場合のみです。

各ESXiホストにONTAP tools VMが1つだけ含まれていることを確認してください。次のウィンドウに移動するたびに、入力内容が検証されます。

7. 「概要」セクションの詳細を確認し、変更内容を「保存」してください。

次の手順

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

HA デプロイメントが失敗し、新しいノードのステータスが「新規」の場合は、HA を再度有効にする前に vCenter で新しい VM を削除してください。

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

VMware vSphereホストをONTAPツールに追加する

新しい VMware vSphere ホストを ONTAP tools for VMware vSphere に追加して、ホスト上のデータストアを管理および保護します。

手順

1. VMware vSphere クラスターにホストを追加するには、次のページのワークフローに従ってください： "[クイックスタートワークフローを使用して ESX ホストを vSphere クラスターに追加する方法](#)"
2. ホストを追加したら、ONTAP tools のメインメニューを開き、概要パネルで「検出」を選択します。検出プロセスが完了するまでお待ちください。または、スケジュールされたホスト検出が完了するまで待つこともできます。

結果

新しいホストは、ONTAP tools for VMware vSphere によって検出および管理されるようになりました。新しいホスト上のデータストアの管理に進むことができます。

関連トピック

- "[vVolデータストアのマウント](#)"新しいホスト上で。
- "[NFSおよびVMFSデータストアをマウントする](#)"新しいホスト上で。

データストアの管理

ONTAP toolsでNFSおよびVMFSデータストアをマウントする

追加のホストにデータストアをマウントすると、そのホストからストレージにアクセスできるようになります。ホストをVMware環境に追加したあとで、そのホストにデータストアをマウントできます。



新しい ESXi ホストを追加する場合は ["ESX ホストをvSphere クラスターワークフローに追加する"](#)、スケジュールされたホスト検出が完了するまで待ってから ONTAP tools に表示されることを確認してください。または、NetApp ONTAP tools の概要画面から手動で検出を実行することもできます。

タスク概要

- 一部の右クリック操作は、vSphere クライアントのバージョンと選択されたデータストアの種類によっては、無効または使用できない場合があります。
 - vSphere クライアント 8.0 以降のバージョンを使用している場合、右クリックオプションの一部が非表示になっています。
 - vSphere 7.0U3 から vSphere 8.0 バージョンでは、オプションが表示されても、そのアクションは無効になります。
- vSphere は、ホストクラスタが統一構成で保護されている場合、マウントデータストアオプションを無効にします。

手順

1. vSphere Client のホームページで、*「ホストとクラスタ」*を選択します。
2. 左側のナビゲーションペインで、ホストが格納されているデータセンターを選択します。
3. 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、右クリックして **NetApp ONTAP tools > Mount Datastores** を選択します。
4. マウントするデータストアを選択し、*マウント*を選択します。

次の手順

最近のタスクパネルで進捗状況を確認できます。

関連トピック

["新しい VMware vSphere ホストを追加する"](#)

ONTAP toolsでNFSおよびVMFSデータストアをアンマウントする

データストアのマウント解除アクションは、ESXiホストからNFSまたはVMFSデータストアを削除します。これは、ONTAP tools for VMware vSphereによって検出または管理されているデータストアで利用可能です。

手順

1. vSphere クライアントにログインします。

2. NFSまたはVMFSデータストアオブジェクトを右クリックし、「データストアのマウント解除」を選択します。

vSphere クライアントはダイアログボックスを開き、データストアをマウントしている ESXi ホストの一覧を表示します。保護されたデータストアに対して操作を実行すると、画面に警告メッセージが表示されます。

3. データストアをアンマウントするESXiホストを1つ以上選択してください。

データストアをすべてのホストからアンマウントすることはできません。ユーザーインターフェースでは、代わりにデータストアの削除操作を使用するように促されます。

4. 「マウント解除」ボタンを選択します。

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



保護対象のデータストアがアンマウントされた場合、既存の保護設定によって部分的な保護しか得られない可能性があります。完全な保護を有効にするには、"[保護されたホストクラスタを変更する](#)"を参照してください。

次の手順

最近のタスクパネルで進捗状況を確認できます。

ONTAP tools で vVols データストアをマウントする

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



新しい ESXi ホストを追加する場合は "[ESX ホストをvSphere クラスターワークフローに追加する](#)"、スケジュールされたホスト検出が完了するまで待ってから ONTAP tools に表示されることを確認してください。または、NetApp ONTAP tools の概要画面から手動で検出を実行することもできます。

手順

1. vSphere Client のホームページで、*「ホストとクラスタ」*を選択します。
2. ナビゲーションペインで、データストアが格納されているデータセンターを選択します。
3. データストアを右クリックし、**NetApp ONTAP tools** > データストアのマウント を選択します。
4. 「ホストへのデータストアのマウント」ダイアログボックスで、データストアをマウントするホストを選択し、「マウント」を選択します。

最近のタスクパネルには、進捗状況が表示されます。

関連トピック

["新しい VMware vSphere ホストを追加する"](#)

ONTAP toolsでNFSおよびVMFSデータストアのサイズを変更する

データストアのサイズを変更することで、仮想マシンファイルの保存容量を増やすことができます。インフラストラクチャの要件が変化するにつれて、データストアのサイズを変更できます。

タスク概要

NFSおよびVMFSデータストアのサイズを増やすことができます。これらのデータストア内のFlexVol volumeは、現在のサイズを下回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、*「ホストとクラスタ」*を選択します。
2. ナビゲーションペインで、データストアが格納されているデータセンターを選択します。
3. NFSまたはVMFSデータストアを右クリックし、**NetApp ONTAP tools** > *データストアのサイズ変更*を選択します。
4. 「サイズ変更」ダイアログボックスで、データストアの新しいサイズを入力し、**OK** を選択します。

ONTAP tools で vVols データストアを拡張する

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



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

手順

1. vSphere Client のホームページで、*「ホストとクラスタ」*を選択します。
2. ナビゲーションペインで、データストアが格納されているデータセンターを選択します。
3. データストアを右クリックし、**NetApp ONTAP tools** > データストアへのストレージの追加 を選択します。
4. 「ボリュームの作成または選択」ウィンドウでは、新しいボリュームを作成するか、既存のボリュームから選択することができます。画面の指示に従って選択してください。
5. 「概要」ウィンドウで選択内容を確認し、「展開」を選択します。最近のタスクパネルで進捗状況を確認できます。

ONTAP tools で vVols データストアを縮小する

このページでは、vVols データストアからボリュームを削除する方法について説明します。

vCenter Server内のONTAP toolsで管理されている任意のvVolsデータストアに対して、「データストアからストレージを削除」アクションを使用します。

ボリュームに vVols が含まれている場合、そのボリュームからストレージを削除することはできません。このようなボリュームでは削除オプションは無効になります。データストアからボリュームを削除する場合、選択したボリュームを ONTAP ストレージから削除するオプションもあります。



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

手順

1. vSphere Client のホームページで、*「ホストとクラスタ」*を選択します。
2. ナビゲーションペインで、データストアが格納されているデータセンターを選択します。
3. vVol データストアを右クリックし、**NetApp ONTAP tools** > データストアからストレージを削除 を選択します。
4. vVols のないボリュームを選択し、*削除*を選択します。



vVolsが配置されているボリュームを選択するオプションは無効になっています。

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

ONTAP toolsでデータストアを削除する

このページでは、vCenter ServerでONTAP toolsを使用して、NFS、VMFS、またはvVols データストアを削除する方法について説明します。

データストアを削除すると、データストアの種類に応じて以下の処理が実行されます。

- vVolコンテナがアンマウントされました。
- igroupが使用されていない場合、そのイニシエータはigroupから削除されます。
- vVolコンテナが削除されました。
- FlexVolボリュームはストレージアレイ上に残ります。

データストアを削除できるのは、選択したデータストアに vVols が存在しない場合のみです。

手順

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



仮想マシンが使用するデータストアは削除できません。削除する前に、仮想マシンを別のデータストアに移動してください。保護されたホストクラスタの一部であるボリュームは削除できません。

- a. NFSまたはVMFSデータストアの場合、そのデータストアを使用している仮想マシンの一覧が表示されたダイアログボックスが表示されます。
- b. VMFSデータストアに関連付けられている仮想マシンがない場合、確認ダイアログが表示されます。ホストクラスタ保護が有効になっており、AFD関係が存在する場合、セカンダリストレージ要素をク

リーンアップできます。

- c. ASA r2システムで保護されたVMFSデータストアの場合、削除する前に保護を解除してください。ONTAP 9.17.1およびONTAP tools for VMware vSphere 10.5以降では、保護されたデータストアを削除できます。保護グループ内にデータストアが1つしかない場合、ホストクラスタの保護は自動的に解除されます。
 - d. vVols データストアの場合、vVols が存在しない場合にのみデータストアを削除できます。「データストアの削除」ダイアログボックスには、ONTAP クラスタからボリュームを削除するオプションが含まれています。
 - e. vVols データストアが ASA r2 システム上にある場合、データストアの削除 オプションを使用して ONTAP からバックアップ ボリュームを削除することはできません。
3. ONTAP ストレージのバックアップ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*を選択します。



保護されたホスト クラスタの一部である統合 ONTAP ストレージ上の VMFS データストアの場合、ONTAP クラスタからボリュームを削除することはできません。

NFS、VMFS、またはvVolsデータストアを削除すると、親igroupはONTAPシステムに残ります。いずれのLUNにもマッピングされていない子igroupは自動的に削除されます。ONTAP toolsは、マッピングされていないデフォルトの親igroupを削除するために、毎日クリーンアップを実行します。カスタム親igroupはONTAPで手動で削除してください。ONTAP toolsは、古い親igroupを再利用できません。

ONTAP tools のデータストアの ONTAP ストレージ ビュー

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

手順

1. vSphere クライアントから、データストアに移動します。
2. 右側のペインにある「設定」タブを選択します。
3. **NetApp ONTAP tools > ONTAP Storage** を選択します。データストアの種類によって表示が変わります。下の表を参照してください。

データストアの種類	情報入手可能
NFSデータストア	「ストレージの詳細」ページには、ストレージバックエンド、アグリゲート、およびボリューム情報が含まれています。「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含まれています。
VMFSデータストア	「ストレージの詳細」ページには、ストレージバックエンド、アグリゲート、ボリューム、およびストレージの可用性ゾーン（SAZ）の詳細が含まれています。「ストレージユニットの詳細」ページには、ストレージユニットの詳細が記載されています。

vVolsデータストア	すべてのボリュームを一覧表示します。ONTAP ストレージペインからストレージを拡張または削除できます。ONTAP tools は、ASA r2 システムベースの vVols データストアに対してこのビューをサポートしていません。
-------------	---

ONTAP toolsの仮想マシンストレージビュー

ストレージビューには、仮想マシンが作成する vVols の一覧が表示されます。



このビューは、ONTAP tools for VMware vSphere が管理する vVols データストアのディスクを少なくとも 1 つ持つ VM に適用されます。

手順

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

「列の管理」オプションを使用すると、さまざまな列を表示または非表示にできます。

ONTAP toolsでストレージしきい値を管理する

ボリュームおよびアグリゲートの容量が一定のレベルに達したときに vCenter Server で通知を受け取るためのしきい値を設定できます。

手順：

1. vSphere クライアントにログインします。
2. ショートカットページで、プラグインセクションにある **NetApp ONTAP tools** を選択します。
3. ONTAP tools の左側のペインで、設定 > しきい値設定 > 編集 に移動します。
4. 「しきい値の編集」ウィンドウで、「ほぼ満杯」と「満杯」のフィールドに希望の値を入力し、「保存」を選択します。しきい値を推奨デフォルト値（ほぼ満杯の場合は 80、満杯の場合は 90）に戻すことができます。

ONTAP toolsでストレージバックエンドを管理する

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

ストレージを検出する

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を待たずにオンデマンドで実行でき、ストレージの詳細を即座に更新できます。MetroCluster構成の場合は、スイッチオーバー後にONTAP toolsの検出手動で実行してください。

ストレージバックエンドを検出するには、以下の手順に従ってください。

手順

1. vSphere クライアントにログインします。
2. ショートカットページで、プラグインセクションにある **NetApp ONTAP tools** を選択します。
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、ストレージバックエンドを選択します。
4. 縦に並んだ3点メニューを選択し、*ストレージの検出*を選択します。

最近のタスクパネルで進捗状況を確認できます。

ストレージバックエンドを変更する

ストレージバックエンドの認証情報またはポート名を変更できます。ONTAP tools Manager を使用して、グローバル ONTAP クラスターのストレージバックエンドを変更することもできます。証明書の有効期限が30日以内に切れる場合、ONTAP tools に警告が表示されます。ストレージバックエンドを変更し、ONTAP 管理者から新しい証明書をアップロードしてください。

ストレージバックエンドを変更すると、ONTAP tools for VMware vSphere はストレージバックエンドの検出を実行して、ストレージの詳細を更新します。

ストレージバックエンドを変更するには、このセクションの手順に従ってください。

1. vSphere クライアントにログインします。
2. ショートカットページで、プラグインセクションにある **NetApp ONTAP tools** を選択します。
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、ストレージバックエンドを選択します。
4. 縦に並んだ三点リーダーのメニューを選択し、「変更」を選択して認証情報またはポート名を変更します。最近のタスクパネルで進捗状況を確認できます。

ONTAP tools Manager を使用して、グローバル ONTAP クラスターを次のように変更します。

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーからストレージバックエンドを選択してください。
4. 変更したいストレージバックエンドを選択してください。
5. 縦三点リーダーのメニューを選択し、**Modify** を選択します。
6. 認証情報またはポートを変更できます。ストレージバックエンドを変更するには、**Username** と **Password** を入力してください。

ストレージバックエンドを削除する

ストレージバックエンドを削除する前に、ストレージバックエンドに接続されているすべてのデータストアを削除する必要があります。ストレージバックエンドを削除するには、以下の手順に従ってください。

1. vSphere クライアントにログインします。

2. ショートカットページで、プラグインセクションにある **NetApp ONTAP tools** を選択します。
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、ストレージバックエンドを選択します。
4. 縦に並んだ三点リーダーのメニューを選択し、*削除*を選択します。ストレージバックエンドにデータストアが含まれていないことを確認してください。最近のタスクパネルで進捗状況を確認できます。

ONTAP tools Managerを使用して、グローバルONTAPクラスタを削除できます。

1. Web ブラウザから ONTAP tools Manager を起動します：
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから「ストレージバックエンド」を選択します。
4. 削除するストレージバックエンドを選択してください
5. 縦に並んだ三点リーダーのメニューを選択し、*削除*を選択します。

ストレージバックエンドの詳細ビュー

ストレージバックエンドのページには、すべてのストレージバックエンドが一覧表示されます。追加したストレージバックエンドに対しては、ストレージの検出、変更、削除といった操作を実行できますが、クラスタ配下の個々の子SVMに対しては実行できません。

コンポーネントの概要を表示するには、親クラスターまたは子クラスターを選択してください。親クラスターの場合、アクションのドロップダウンを使用して、ストレージの検出、ストレージバックエンドの変更、または削除を行います。

概要ページには、以下の詳細情報が表示されます：

- ストレージバックエンドの状態
- 容量情報
- VMに関する基本情報
- 証明書のステータスや有効期限などの証明書の詳細。
- ネットワークのIPアドレスやポート番号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です。
- ストレージ バックエンドに対して許可および制限されているPrivileges。子SVMの場合、情報は親ストレージ バックエンドと同じです。ONTAP toolsは、クラスタベースのストレージ バックエンドでのみPrivilegesを表示します。SVMをストレージ バックエンドとして追加した場合、Privileges情報は表示されません。
- ASA r2 システムクラスタのドリルダウンビューでは、SVM またはクラスタの非集約プロパティが「true」に設定されている場合、ローカルティアタブは含まれません。
- ASA r2 SVMシステムでは、容量ポートレットは表示されません。容量ポータルは、SVMまたはクラスタの「分離」プロパティが「true」に設定されている場合にのみ必要です。
- ASA r2 SVMシステムの場合、基本情報セクションにはプラットフォームの種類が表示されます。

インターフェイスタブには、インターフェイスに関する詳細情報が表示されます。

ローカルティアタブには、アグリゲートリストに関する詳細情報が表示されます。

ONTAP tools で vCenter Server インスタンスを管理する

vCenter Server インスタンスは、ホスト、仮想マシン、ストレージバックエンドを制御できる中央管理プラットフォームです。

ストレージバックエンドとvCenter Serverインスタンスの関連付けを解除する

vCenter サーバー一覧ページには、関連付けられているストレージバックエンドの数が表示されます。各 vCenter サーバーインスタンスには、ストレージバックエンドとの関連付けまたは関連付け解除を行うオプションがあります。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから必要なvCenter Serverインスタンスを選択します。
4. ストレージバックエンドと関連付けたり、関連付けを解除したりする vCenter Server に対して縦の省略記号を選択します。
5. 「ストレージバックエンドの関連付けを解除」を選択します。

vCenter Server インスタンスを変更する

以下の手順に従って、vCenter Server インスタンスを変更します。

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから該当するvCenter Serverインスタンスを選択します
4. 変更する vCenter Server に対して縦の省略記号を選択し、*変更*を選択します。
5. **vCenter** の変更 ウィンドウで、ユーザー名、パスワード、およびポートの詳細を入力します。
6. 証明書をアップロードし、*変更*を選択します。

vCenter Server インスタンスを削除する

削除する前に、vCenter Server からすべてのストレージバックエンドを削除してください。

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. サイドバーから該当する vCenter Server インスタンスを選択します
4. 削除する vCenter Server に対して縦の省略記号を選択し、*削除*を選択します。



vCenter Server インスタンスを削除すると、アプリケーションによる管理が行われなくなります。

ONTAP tools で vCenter Server インスタンスを削除すると、以下の操作が自動的に実行されます：

- プラグインが未登録です。
- プラグイン権限とプラグインロールが削除されました。

vCenter Server 証明書の更新

ONTAP tools は、vCenter 証明書の有効期限が近づいているか、または期限切れになっていることを通知します。vCenter 証明書を更新したら、以下の手順に従って新しい証明書を ONTAP tools にアップロードしてください。

1. ONTAP tools のリモート診断シェルにログインします。
2. 更新された vCenter 証明書を診断シェルから取得します：

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN  
CERTIFICATE/,/END CERTIFICATE/p'
```

3. 証明書がBase 64 ASCII形式であり、開始行と終了行が含まれていることを確認してください。例：

ONTAP tools証明書の管理

自己署名証明書は、デプロイ時にデフォルトで ONTAP tools および VASA Provider に対して生成されます。ONTAP tools Manager インターフェースを使用して、この証明書を更新したり、カスタム CA 証明書に置き換えたりすることができます。マルチvCenter デプロイメントでは、カスタム CA 証明書の使用が必要です。

開始する前に

始める前に、以下のものを用意してください。

- 仮想IPアドレスにマッピングされたドメイン名。
- ドメイン名のnslookupが正常に実行され、正しいIPアドレスに解決されることが確認されました。
- ドメイン名とONTAP tools のIPアドレスを使用して作成された証明書。



ONTAP tools の IP アドレスは、完全修飾ドメイン名 (FQDN) にマッピングされている必要があります。証明書には、サブジェクトまたはサブジェクトの別名に、ONTAP tools の IP アドレスにマッピングされた同じ FQDN が含まれている必要があります。



認証局署名付き証明書から自己署名付き証明書に切り替えることはできません。

ONTAP tools 証明書のアップグレード

ONTAP tools タブには、証明書の種類（自己署名／CA署名）やドメイン名などの詳細情報が表示されます。デプロイ時には、デフォルトで自己署名証明書が生成されます。証明書を更新するか、CA証明書にアップグレードすることができます。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 証明書 > **ONTAP tools** > 更新 を選択して証明書を更新します。

証明書の有効期限が切れている場合、または有効期限が近づいている場合は、更新することができます。証明書の種類が認証局（CA）署名の場合、更新オプションが利用可能です。ポップアップウィンドウに、サーバー証明書、秘密鍵、ルート CA、および中間証明書の詳細を入力してください。



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

4. 自己署名証明書をカスタム CA 証明書にアップグレードするには、証明書 > **ONTAP tools** > **CA** へのアップグレード オプションを選択します。
 - a. ポップアップウィンドウで、サーバー証明書、サーバー証明書の秘密鍵、ルートCA証明書、および中間証明書ファイルをアップロードします。
 - b. この証明書を生成したロードバランサーの IP アドレスの FQDN を入力し、証明書をアップグレードしてください。



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

VASAプロバイダー証明書のアップグレード

ONTAP tools for VMware vSphereは、VASA Provider用の自己署名証明書を使用してデプロイされます。これにより、vVols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つだけになります。複数のvCenter Serverインスタンスを管理し、それらのインスタンスでvVols機能を有効にする場合は、自己署名証明書をカスタムCA証明書に変更する必要があります。

手順

1. Web ブラウザから ONTAP tools Manager を起動します：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. デプロイ時に指定した ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. **Certificates** > **VASA Provider** または **ONTAP tools** > **Renew** を選択して証明書を更新します。
4. **Certificates** > **VASA Provider** または **ONTAP tools** > **Upgrade to CA** を選択して、自己署名証明書をカスタムCA証明書にアップグレードします。
 - a. ポップアップウィンドウで、サーバー証明書、サーバー証明書の秘密鍵、ルートCA証明書、および中間証明書ファイルをアップロードします。

- b. この証明書を生成したロードバランサーの IP アドレスの FQDN を入力し、証明書をアップグレードしてください。



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

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

ONTAP toolsのメンテナンスコンソールについて学ぶ

ONTAP tools for VMware vSphere のメンテナンスコンソールを使用すると、アプリケーション、システム、ネットワークの設定を管理できます。管理者パスワードとメンテナンスパスワードの更新、サポートバンドルの生成、ログレベルの設定、TLS設定の管理、リモート診断の有効化を行うことができます。

ONTAP tools for VMware vSphere を導入後、メンテナンスコンソールにアクセスできない場合は、vCenter Server から VMware Tools をインストールしてください。`maint`ユーザー名とデプロイ時に設定したパスワードを使用してログインします。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** を使用してください。



リモート診断を有効にする際は、`diag`ユーザー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、デプロイした ONTAP tools for VMware vSphere の「概要」タブを使用してください。  を選択すると、メンテナンスコンソールが起動します。

コンソールメニュー	オプション
Application Configuration	1. Display server status summary 2. ONTAP tools サービスのログレベルを変更する 3. 証明書検証フラグを変更する
System Configuration	1. Reboot virtual machine 2. Shutdown virtual machine 3. 「maint」ユーザのパスワードの変更 4. タイムゾーンの変更 5. jailディスク サイズの拡張 (/jail) 6. Upgrade 7. VMware Toolsのインストール

Network Configuration	1. Display IP address settings 2. Display domain name search settings 3. ドメイン名検索設定の変更 4. Display static routes 5. 静的ルートの変更 6. Commit changes 7. Ping a host 8. Restore default settings
Support and Diagnostics	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 3. バックアップ用の vCenter 認証情報を入力してください 4. バックアップを取得する

ONTAP toolsのリモート診断アクセスを設定する

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

開始する前に

vCenter Server インスタンスの VASA プロバイダー拡張機能を有効にします。

タスク概要

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

- SSHの有効化ごとに、ログインアカウントは1つしか許可されていません。
- diagユーザ アカウントへのSSHアクセスは、次のいずれかの状況になると無効になります。
 - タイムアウトした場合。

ログインセッションは翌日の午前0時に期限切れとなります。

- SSHを使用してdiagユーザとして再度ログインした場合。

手順

1. vCenter Serverで、VASA Providerへのコンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. `4`を入力して、「サポートと診断」を選択してください。
4. Enter `2`を押して「リモート診断アクセスを有効にする」を選択します。
5. `y`を確認ダイアログボックスに入力して、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ONTAP toolsノードでSSHを起動します

アップグレードする前に、他のノードでSSHを起動する必要があります。

開始する前に

vCenter Server インスタンスの VASA プロバイダー拡張機能を有効にします。

タスク概要

アップグレードを行う前に、各ノードでこの手順を繰り返してください。

手順

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

ONTAP toolsでvCenter Serverのクレデンシャルを更新

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

開始する前に

メンテナンスユーザーのログイン認証情報が必要です。

タスク概要

デプロイ後に vCenter Server の認証情報を変更した場合は、この手順を使用して更新してください。

手順

1. vCenter Serverで、VASA Providerへのコンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. `2`を入力してシステム設定メニューを選択します。
4. `8`を入力して、vCenterの資格情報を変更します。

ONTAP toolsで証明書検証フラグを変更する

デフォルトでは、証明書検証フラグは有効（true に設定）になっています。SAN 証明書のチェックをバイパスする必要がある場合は、ONTAP ストレージバックエンドの証明書検証フラグを false に設定できます。この設定は vCenter サーバー証明書には適用されません。

開始する前に

メンテナンスユーザーのログイン認証情報が必要です。

手順

1. vCenter Server から、ONTAP tools へのコンソールを開きます。
2. メンテナンス ユーザとしてログインします。
3. `1`を入力して、「アプリケーション設定」メニューを選択します。
4. 証明書の検証フラグを変更するには、`3`を入力してください。

メンテナンスコンソールには証明書検証フラグの状態が表示され、変更を促されます。

5. フラグを切り替えるには「y」を、キャンセルするには「n」を入力してください。

証明書検証フラグを有効にする（trueに設定する）と、ONTAP toolsは、すべてのストレージバックエンドがサブジェクト代替名（SAN）付きの証明書を使用していることを確認します。バックエンドでSANのない証明書を使用している場合、証明書の検証を有効にすることはできません。このフラグを有効にする前に、すべてのストレージバックエンドがSANベースの証明書を使用していることを確認してください。証明書検証フラグを無効にする（falseに設定する）と、ONTAP toolsは、設定されているすべてのストレージバックエンドの証明書検証をバイパスします。

ストレージバックエンドの **SAN** ベースの証明書を検証する

安全な通信と適切な検証を確保するには、すべてのストレージ バックエンドが SAN ベースの証明書を使用していることを確認します：

1. ONTAP管理証明書にサブジェクト代替名（SAN）エントリが含まれていることを確認してください。
2. SAN エントリが ONTAP 管理 IP アドレスまたは DNS 名、あるいはその両方と一致することを確認してください。
3. ONTAPのオンボーディングに使用する詳細情報が、証明書のSANエントリ内のIPアドレスまたはDNS名と一致することを確認してください。

これらの手順に従うことで、証明書の検証に関する問題を防ぎ、ONTAPシステムが安全に統合されることを保証します。

次のサンプル証明書は、デコードされた情報を示しています：


```
HG8u6GK r2JJonWe/kjoKTUnkjwW7feDI747RUuFrthcvTDqhBNWL76jihNp1VX7
v0SDWMaVdecTeU1X/1X3qMxIL+tU4p9SbKVpQw6hjM/zi0LNC784EYIOSQ7qVob
6f21mfP0JHbqs5fLim9NFFUu2DQIDAQA8oQw0jBABgNVHREEEOT43hwShsSHdKXsgi9z
dGkyMjAtdnNpbS1zcjA1MWUtY2OuY2Rs LmdkbC5lbmdsYWJuZKThcPHauY29nt
BgkqhkiG9wQBAQsFAAOCCAQAEEagptz11RN7PLuJUo-SSQExBsF5/3JHr0+sSIMZDzm
4P24kbxQZbfryy68itKGF4LeAid0hgyxc3y9iv4zKlx85fLNgITnVqAe8'KYNoyD6
IEWppDUE0eVNZIZQjrZ9QjUAAF9ifjq8+SKr'lphoXnYYUiM6utvobPMG8cR8Gca
jiLibiMM01K6rD7Ng+7+ydUCAwBQwMDDwdn8+7RIRdKgwx9QDLegcC5IL5WFLwbMc
2GBv8VM839m0KUAKXSDGwJBZ5nSHQdNi7MU3AES7Nzkv63kGEQJT/5Wr1DmOwlf
osl4qeeeMRigrAbFL6EHMsOMSP0521rtTrJrjBooB22r0tyDA--
-----END CERTIFICATE-----
```

Certificate Information:

- ✓ Common Name: **test.xyz.com**
- ✓ Subject Alternative Names: IP Address: **xxx.xx.xxx.xxx**, **test.xyz.com**
- ✓ Organization: Self-signed-certificate
- ✓ Organization Unit:
- ✓ Locality: N/A
- ✓ State: N/A
- ✓ Country: XX
- ✓ Valid From: March 8, 2026
- ✓ Valid To: March 7, 2028
- ✓ Issuer: **test.xyz.com**, Self-signed-certificate
- ✓ Serial Number: 640c2752bd2c972c5775180070cfdd2120809ee

ONTAP tools 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に関する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、ユーザー インターフェイスの「概要」ページに遷移します。「レポート」タブを選択すると、仮想マシンとデータストアのレポートを表示できます。

仮想マシン レポートには、検出された仮想マシンのリスト（少なくとも 1 つのディスクが ONTAP ストレージベースのデータストアに存在する必要があります）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、インターフェイスにディスク関連のデータストア情報がすべて表示されます。

データストアレポートには、ONTAP tools for VMware vSphere が検出または認識した、任意の ONTAP ストレージを使用するデータストアがパフォーマンス指標とともに一覧表示されます。

「列の管理」オプションを使用すると、さまざまな列を表示または非表示にできます。

仮想マシンの管理

ONTAP toolsにおける仮想マシンの移行とクローン作成に関する考慮事項

ONTAP tools for VMware vSphereは、コンピューティング専用（vMotion）、ストレージ専用（Storage vMotion）、およびすべてのデータストアにわたるコンピューティングとストレージの統合移行など、すべての主要な仮想マシン移行タイプをサポートしています。このトピックでは、基盤となるデータストアのタイプに関わらず、仮想マシンの移行とクローン作成を成功させるための重要な考慮事項とベストプラクティスについて概説します。

保護されている仮想マシンの移行

保護された仮想マシンは、以下の場所に移行できます：

- 別の ESXi ホスト上の同じデータストア
- 同じESXiホスト上の別の互換性のあるデータストア
- 別のESXiホスト上の別の互換性のあるデータストア

仮想マシンを別のFlexVolボリュームに移行すると、システムはそのボリュームのメタデータファイルを仮想マシン情報で更新します。仮想マシンが別のESXiホストに移行されても、ストレージが同じ場合、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。

仮想マシンの移行に関する情報については、Broadcomのドキュメントを参照してください：["vSphere仮想マシンの移行"](#)

保護されている仮想マシンのクローニング

保護されている仮想マシンは、次の場所にクローニングできます。

- レプリケーション グループを使用した同じ FlexVol ボリュームの同じコンテナ

同じFlexVol volumeのメタデータファイルは、クローンされた仮想マシンの詳細情報で更新されます。

- レプリケーショングループを使用した異なるFlexVolボリュームの同じコンテナ

クローン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がクローンされた仮想マシンの詳細情報で更新されます。

- 別のコンテナまたはvVolsデータストア

クローンされた仮想マシンが配置されているFlexVolボリュームでは、メタデータファイルが仮想マシンの詳細情報で更新されます。

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

保護された仮想マシンのクローンのクローンがサポートされています。

詳細については、Broadcomのドキュメントを参照してください。["クローン作成用の仮想マシンの作成"](#)

仮想マシンのスナップショット

ONTAP tools は、標準的な VMware ワークフローを通じて仮想マシンのスナップショットをサポートします。スナップショットは、テストやパッチの準備などのユースケースを想定した、短期的なロールバックポイントです。これらは、バックアップやレプリケーションベースのデータ保護の代替手段ではありません。スナップショット上で仮想マシンを長期間実行すると、不安定性やデータ損失を引き起こす可能性があります。

サポートされているすべてのデータストアタイプで「crash consistent state（障害など予期しないシャットダウン時と同様）」の状態のスナップショット（メモリ状態を含まないスナップショット。仮想マシンを一貫性のある状態に再起動するために使用できます）を取得できます。VMware Toolsを使用してメモリ内のデータをディスクに書き出してからキャプチャする、静止スナップショットもサポートされています。スナップショットの種類と動作の概要については、["vSphereにおける仮想マシンのスナップショットの概要"](#)を参照してください。



メモリのスナップショットは、実行中のメモリの状態をキャプチャし、仮想マシンを一時的に停止させます。ONTAP tools のワークフローではサポートされていません。仮想マシンにメモリ スナップショットがある場合は、ONTAP tools で管理される整合性グループまたはホスト クラスタ関係に仮想マシンを含める前に、メモリ スナップショットを削除する必要があります。

ASA r2ストレージシステムでは、仮想マシンのスナップショットの動作が他のストレージタイプとは異なります。スナップショットは読み取り専用です。仮想マシンを起動すると、VASA Providerは読み取り専用のスナップショットからLUNを作成し、IOPSを有効にします。仮想マシンの電源を切ると、VASA ProviderはLUNを削除し、IOPSを無効にします。

仮想マシンのスナップショットの管理方法については、Broadcomのドキュメント ["スナップショットを使用して仮想マシンを管理する"](#)を参照してください。

ONTAP tools で仮想マシンを vVols データストアに移行する

仮想マシンを NFS および VMFS データストアから仮想ボリューム（vVols）データストアに移行することで、ポリシーベースの VM 管理およびその他の vVols 機能を活用できます。vVols データストアを利用することで、増加するワークロード要件に対応できます。

開始する前に

移行予定の仮想マシン上でVASA Providerが実行されていないことを確認してください。VASA Providerを実行している仮想マシンをvVolsデータストアに移行すると、vVolsデータストア上の仮想マシンの電源オンを含む管理操作を実行できなくなります。

タスク概要

NFSおよびVMFSデータストアからvVolsデータストアに移行する場合、vCenterサーバーは、VMFSデータストアからデータを移動する際には配列統合用vStorage API（VAAI）のオフロードを使用しますが、NFS VMDKファイルからデータを移動する際には使用しません。VAAIオフロードは通常、ホストへ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** を選択します。
2. 「ストレージのみ変更」を選択し、「次へ」を選択します。
3. 仮想ディスクフォーマット、VM ストレージポリシー、および移行対象のデータストアの機能に合致する vVol データストアを選択してください。

4. 設定内容を確認し、*完了*を選択してください。

ONTAP toolsでVASA構成をクリーンアップする

VASAのクリーンアッププロセスを完了するには、以下の手順に従ってください。



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

手順

1. プラグインの登録を解除するには、\https://OTV_IP:8143/Register.htmlに移動します
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 toolsでVMにデータディスクを接続または切断する

vSphere の仮想マシンに対してデータディスクをアタッチまたはデタッチし、ストレージリソースを管理するには、次の手順に従ってください。

仮想マシンにデータディスクを接続する

仮想マシンにデータディスクを接続することで、ストレージ容量を増やすことができます。

手順

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

結果

ハードディスクが仮想ハードウェアデバイスの一覧に表示されます。

仮想マシンからデータディスクを取り外す

不要になったデータディスクは、仮想マシンから取り外してください。ディスクは削除されません。ONTAPストレージシステムに残ります。

手順

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



仮想マシンからディスクが取り外されました。他の仮想マシンがディスクを共有している場合、ディスクファイルは削除されません。

関連情報

["仮想マシンに新しいハードディスクを追加する"](#)

["仮想マシンに既存のハードディスクを追加する"](#)

ONTAP toolsでストレージシステムとホストを検出する

ONTAP tools for VMware vSphereがvSphere Clientで初めて起動されると、ESXiホスト、それに関連付けられたLUNとNFSエクスポート、およびこれらのリソースを所有するNetAppストレージシステムが自動的に検出されます。

開始する前に

- すべてのESXiホストの電源がオンになっており、接続されていることを確認してください。
- 検出対象のすべてのストレージ仮想マシン（SVM）が実行中であり、各クラスタノードに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 が少なくとも 1 つ設定されていることを確認してください。

タスク概要

新しいストレージシステムを検出したり、既存のストレージシステムを更新したりすることで、最新の容量や設定の詳細を取得できます。また、ストレージシステムへのアクセスに使用する ONTAP tools for VMware vSphere の認証情報を変更することもできます。

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

手順

1. vSphere Client のホームページで、*「ホストとクラスタ」*を選択します。
2. 必要なデータセンターを右クリックして、**NetApp ONTAP tools > Update Host Data** を選択します。

「確認」ダイアログボックスで、選択内容を確定してください。
3. ステータスが `Authentication Failure` の検出済みストレージコントローラを選択し、**Actions > *Modify*** を選択します。
4. 「ストレージシステムの変更」ダイアログボックスに必要事項を入力してください。
5. `Authentication Failure` ステータスのすべてのストレージコントローラに対して、手順4と5を繰り返します。

検出プロセスが完了したら、次の操作を実行してください：

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

ONTAP Toolsを使用したESXiホストの設定の変更

VMware vSphere の ONTAP tools ダッシュボードを使用して、構成の問題を特定し、ESXi ホストを選択し、NetApp の推奨設定を確認して適用します。

開始する前に

ESXiホストシステムポートレットは、ESXiホストの設定に関する問題を表示します。ホスト名またはIPアドレスを表示するには、該当する問題を選択してください。

手順

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



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てください。
7. 概要ペインで値を確認し、*完了*を選択します。最近のタスクパネルで進捗状況を確認できます。

関連情報

["ESXiホスト設定を構成する"](#)

パスワードの管理

ONTAP tools Manager 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://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. ONTAP tools for VMware vSphere の管理者認証情報を使用してログインします。
3. 画面右上の*administrator*アイコンを選択し、*Change password*を選択してください。
4. パスワード変更のポップアップウィンドウに、古いパスワードと新しいパスワードを入力してください。ユーザーインターフェース画面にパスワードの要件が表示されます。
5. 変更を適用するには、「変更」を選択してください。

ONTAP tools Manager のパスワードをリセット

ONTAP tools Manager のパスワードを忘れた場合は、ONTAP tools for VMware vSphere のメンテナンスコンソールで生成されたりセットトークンを使用して、管理者アクセスを復元できます。

手順

1. ウェブブラウザを開き、`https://<ONTAPtoolsIP>:8443/virtualization/ui/` に移動して ONTAP tools Manager にアクセスします。
2. ログインページで*パスワードのリセット*を選択してください。
3. ONTAP tools for VMware vSphere メンテナンスコンソールを使用してパスワードリセットトークンを生成します：
 - a. vCenter Server にログインし、メンテナンスコンソールを開きます。
 - b. `2` を押して「システム構成」を選択します。
 - c. Enter キーを押して 3「maint」ユーザーのパスワードを変更*を選択します。
4. パスワードリセットダイアログで、リセットトークン、ユーザー名、および新しいパスワードを入力してください。
5. 認証情報を更新するには、*リセット*を選択してください。
6. 新しいパスワードを使用して ONTAP tools Manager にログインします。

ONTAP tools でアプリケーションユーザーのパスワードをリセットする

ONTAP tools for VMware vSphere を使用して vCenter Server に SRA および VASA Provider を登録するために必要なアプリケーション ユーザー パスワードをリセットするには、次の手順を実行します。

手順

1. ウェブブラウザを開き、次のアドレスにアクセスしてください：
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. ONTAP tools の導入時に設定した管理者認証情報を使用してログインします。
3. サイドバーから*設定*を選択してください。
4. 「VASA/SRA credentials」ページで、「Reset password」を選択します。
5. 新しいパスワードを入力し、確認してください。
6. 新しいパスワードを適用するには、*リセット*を選択してください。

ONTAP tools のメンテナンスコンソールのパスワードをリセットする

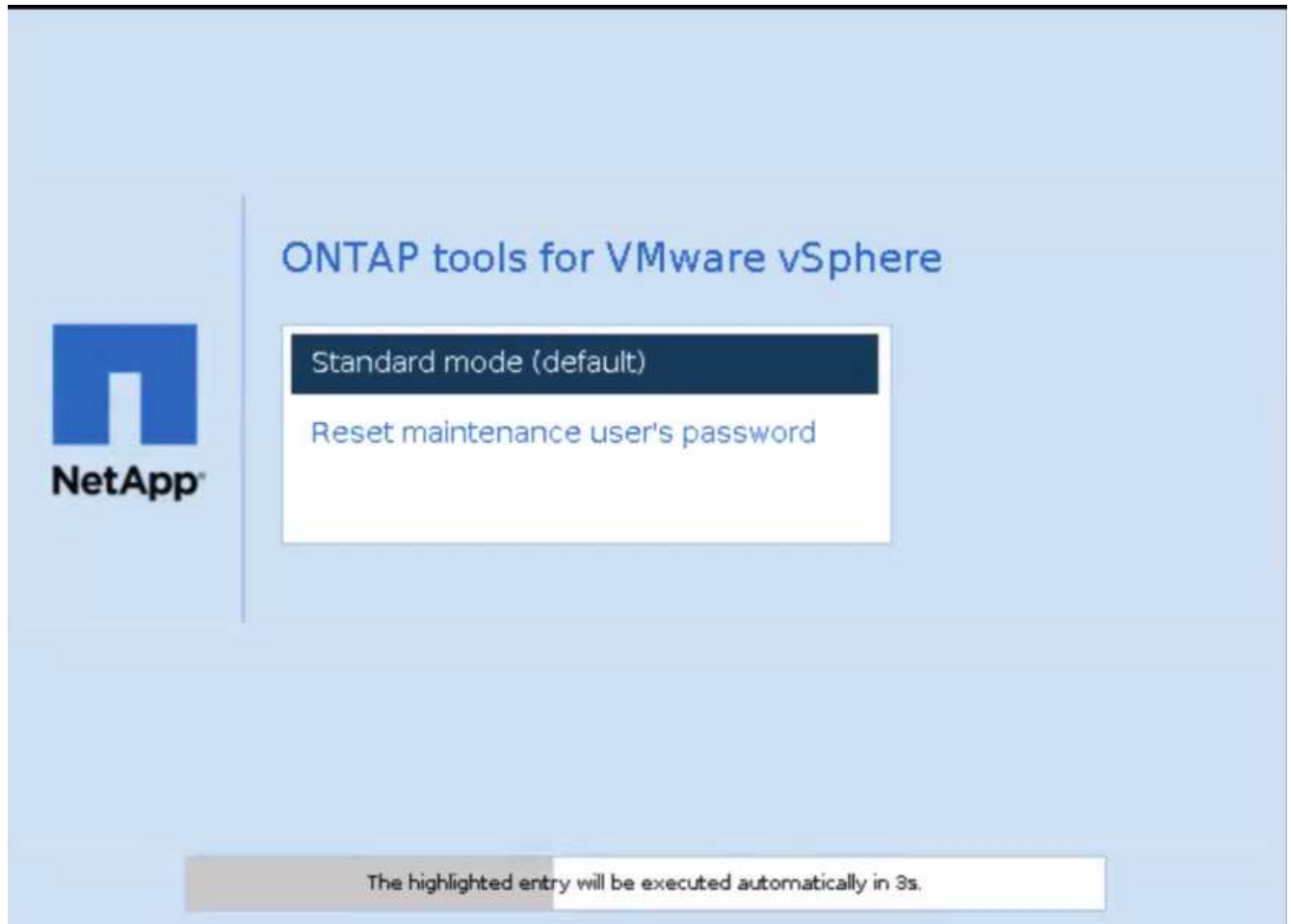
ゲスト OS の再起動操作中に、GRUB メニューにメンテナンスコンソールユーザーのパスワードをリセットするオプションが表示されます。このオプションを使用して、VM 上のメンテナンスコンソールユーザーのパスワードを更新します。パスワードをリセットすると、VM が再起動して新しいパスワードを設定します。HA 構成の展開シナリオでは、VM の再起動後、パスワードは他の 2 台の VM 上で自動的に更新されます。



ONTAP tools for VMware vSphere の HA 展開では、ONTAP tools 管理ノード (node1) のメンテナンスコンソールのユーザーパスワードを変更する必要があります。

手順

1. vCenter Server にログインします
2. VMを右クリックして、**Power > Restart Guest OS** を選択します。システム再起動中に、次の画面が表示されます
:



選択肢を選ぶ時間は5秒です。いずれかのキーを押すと、処理が停止し、GRUBメニューがフリーズします。

3. 「メンテナンスユーザーのパスワードをリセットする」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. コンソールに新しいパスワードを入力し、確認してください。3回まで試行できます。新しいパスワードを正しく入力すると、システムが再起動します。
5. 続行するには **Enter** キーを押してください。システムは仮想マシン上のパスワードを更新します。



仮想マシンを起動すると、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、*Restart Guest OS*オプションと併用する場合にのみ使用してください。

ホストクラスタ保護の管理

ONTAP toolsで保護されたホストクラスタを変更する

ホストクラスタの保護設定は、単一のワークフローで変更できます。以下の変更がサポートされています：

- 保護対象クラスターに新しいデータストアまたはホストを追加します。
- 新しい SnapMirror 関係を保護設定に追加します。
- 保護設定から既存の SnapMirror 関係を削除します。
- 既存の SnapMirror 関係を変更します。



ホストクラスタの保護設定を作成、編集、または削除した後は、変更内容を反映させるためにストレージ検出を実行する必要があります。ストレージ検出を実行しない場合、変更内容は定期的なストレージ検出がトリガーされた後に反映されます。

ホストクラスタ保護を監視する

保護状態、SnapMirror関係、データストア、および保護対象ホストクラスタごとのSnapMirrorステータスを監視します。

手順

1. vSphere クライアントにログインします。
2. **NetApp ONTAP tools** > 保護 > ホストクラスタ関係 に移動します。

保護列には、保護状態を示すアイコンが表示されます。

3. アイコンにカーソルを合わせると、詳細が表示されます。

新しいデータストアまたはホストを追加する

保護されたクラスターにホストを追加したり、データストアを作成したりするには、vCenter ユーザーインターフェースを使用します。

手順

1. vSphere クライアントにログインします。
2. 保護されたクラスターのプロパティを編集するには、次のいずれかの方法を使用できます。
 - a. **NetApp ONTAP tools** > 保護 > *ホストクラスタ関係*に移動し、クラスタの横にある省略記号メニューを選択して、*編集*または
 - b. ホストクラスタを右クリックして、* NetApp ONTAP tools* > *クラスタの保護*を選択します。
3. データストアをvCenterユーザーインターフェースで作成すると、保護されていない状態として表示されます。ダイアログボックスで、クラスタ内のすべてのデータストアとその保護状態を確認できます。保護を有効にするには、*保護*ボタンを選択してください。



vCenter Server のユーザーインターフェイスでデータストアを作成したら、概要ページで「検出」を選択すると、ホストクラスタ内で保護対象候補としてデータストアが表示されます。次回の定期的な保護検出後、保護ステータスは「保護済み」に更新されます。

4. 新しいESXiホストを追加すると、保護状態が「部分的に保護されています」と表示されます。SnapMirror 設定の省略記号メニューを選択し、「編集」を選択して、新しく追加したESXiホストの近接度を設定します。



非同期関係の場合、第三サイトのターゲット SVM を同じインスタンスに追加できないため、ONTAP tools での編集はサポートされていません。関係構成を変更するには、ターゲット SVM 上で System Manager または CLI を使用してください。

5. 変更後、*保存*を選択してください。
6. 変更内容は「クラスターの保護」ウィンドウで確認できます。

ONTAP tools は vCenter タスクを作成し、その進捗状況は「最近のタスク」パネルで確認できます。

新しい **SnapMirror** 関係を追加する

手順

1. vSphere クライアントにログインします。
2. 保護されたクラスターのプロパティを編集するには、次のいずれかの方法を使用できます。
 - a. **NetApp ONTAP tools** > 保護 > *ホストクラスタ関係*に移動し、クラスタの横にある省略記号メニューを選択して、*編集*または
 - b. ホストクラスタを右クリックして、* NetApp ONTAP tools* > *クラスタの保護*を選択します。
3. 「関係を追加」を選択します。
4. 新しい関係を 非同期 または **AutomatedFailOverDuplex** ポリシータイプとして追加します。
5. *Protect*を選択します。

変更内容は「クラスターの保護」ウィンドウで確認できます。

ONTAP tools は vCenter タスクを作成し、その進捗状況は「最近のタスク」パネルで確認できます。

既存の **SnapMirror** 関係を削除する

SnapMirror 非同期関係を削除するには、セカンダリサイトの SVM またはクラスターが ONTAP tools for VMware vSphere にストレージバックエンドとして追加されていることを確認してください。すべての SnapMirror 関係を一度に削除することはできません。関係を削除すると、ONTAP クラスターから対応する関係も削除されます。Automated Failover Duplex SnapMirror 関係を削除すると、システムは宛先データストアのマッピングを解除し、宛先 ONTAP クラスターから整合性グループ、LUN、ボリューム、および igroup を削除します。

関係を削除すると、システムはセカンダリサイトを再スキャンし、ホストからマッピングされていないLUNをアクティブなパスとして削除します。

手順

1. vSphere クライアントにログインします。

2. 保護されたクラスターのプロパティを編集するには、次のいずれかの方法を使用できます。
 - a. **NetApp ONTAP tools** > 保護 > *ホストクラスタ関係*に移動し、クラスタの横にある省略記号メニューを選択して、*編集*または
 - b. ホストクラスタを右クリックして、* NetApp ONTAP tools* > *クラスタの保護*を選択します。
3. SnapMirror設定の省略記号メニューを選択し、*削除*を選択します。
 - 保護対象ホストクラスタの非同期ポリシータイプに基づく関係を削除する場合は、三次ストレージクラスタからストレージ要素を手動で削除する必要があります。ストレージ要素には、整合性グループ、ボリューム（ONTAP システムの場合）、ストレージユニット（LUN/ネームスペース）、およびスナップショットが含まれます。
 - 保護されたホストクラスタの自動フェイルオーバーデュプレックス（AFD）ポリシーベースの関係を削除する場合、インターフェースから直接、セカンダリストレージ上の関連するストレージ要素を削除することを選択できます。
 - 自動フェイルオーバーデュプレックス（AFD）のポリシーベースの関係を削除し、整合性グループがアプリケーションレベルのバックアップに対して階層構造になった場合、バックアップへの影響に関する警告が表示されます。続行するには確認してください。確認後、セカンダリストレージ上の関連するストレージ要素を削除してください。削除しない場合、それらはセカンダリサイトに残ります。

ONTAP tools は vCenter タスクを作成し、その進捗状況は「最近のタスク」パネルで確認できます。

既存のSnapMirror関係を変更する

SnapMirror非同期関係を変更するには、セカンダリ サイトのSVMまたはクラスターがONTAP tools for VMware vSphereにストレージ バックエンドとして追加されていることを確認してください。Automated Failover Duplex SnapMirror関係では、均一な構成の場合はホストの近接性を、非均一な構成の場合はホストアクセスを更新できます。非同期ポリシー タイプとAutomated Failover Duplexポリシー タイプ間の変更はサポートされていません。クラスター内で新しく検出されたホストの近接性またはアクセス設定を構成できません。



既存の SnapMirror 非同期関係を編集することはできません。

手順

1. vSphere クライアントにログインします。
2. 保護されたクラスターのプロパティを編集するには、次のいずれかの方法を使用できます。
 - a. **NetApp ONTAP tools** > 保護 > *ホストクラスタ関係*に移動し、クラスタの横にある省略記号メニューを選択して、*編集*または
 - b. ホストクラスタを右クリックして、* NetApp ONTAP tools* > *クラスタの保護*を選択します。
3. AutomatedFailOverDuplexポリシータイプが選択されている場合は、ホストの近接性またはホストアクセスの詳細を追加してください。
4. 「保護」ボタンを選択します。

ONTAP tools は vCenter タスクを作成します。最近のタスク パネルで進捗状況を確認できます。

ONTAP toolsでホストクラスタ保護を削除する

ホストクラスタの保護を解除すると、データストアは保護されなくなります。

手順

1. 保護されているホスト クラスターの一覧を表示するには、**NetApp ONTAP tools** > 保護 > *ホスト クラスター関係*に移動します。

このページでは、保護されたホスト クラスター、保護状態、SnapMirror 関係、およびステータスを監視できます。整合性グループを選択すると、容量、関連するデータストア、および子グループが表示されます。

2. 「ホスト クラスター保護」ウィンドウで、クラスターの横にある省略記号メニューを選択し、「保護の削除」を選択します。
 - ホスト クラスターから保護を削除する場合、SnapMirror 非同期関係のみの場合は、ストレージ要素を手動で削除する必要があります。ストレージ要素には、整合性グループ、ボリューム（ONTAP システム）、ストレージユニット（LUN）、およびスナップショットが含まれます。
 - 自動フェイルオーバー デュプレックススペースの SnapMirror ポリシー関係と非階層的な整合性グループのみを持つホスト クラスターから保護を削除する場合、同じ画面からセカンダリ ストレージ上の関連するストレージ要素を直接削除できます。
 - SnapMirror ポリシーとバックアップ用の階層的な整合性グループの両方が設定されているホスト クラスターから保護を削除すると、バックアップへの影響に関する警告が表示されます。続行するには確認してください。確認後、セカンダリ ストレージ上の関連するストレージ要素を削除してください。クリーンアップを行わない場合、ストレージ要素はセカンダリ サイトに残ります。

ONTAP tools のセットアップを復元する

ONTAP tools for VMware vSphere 10.5 以降、バックアップ機能はデフォルトで有効になっています。

ONTAP tools for VMware vSphere 仮想マシンをデプロイするデータストアにバックアップファイルが保存されます。ONTAP tools の IP アドレスにちなんで名付けられたフォルダ（ドットはアンダースコアに置き換えられ、末尾に *OTV_backup* が付加されます）には、最新の 2 つのバックアップファイル（*OTV_backup_1.tar.enc* と *OTV_backup_2.tar.enc*）と、最新のバックアップの名前を含む情報ファイル（*OTV_backup_info.txt*）が保存されます。

新しい仮想マシンが同じ ONTAP tools の IP アドレスを使用し、有効なサービス、ノードサイズ、HA モードなどの初期システム構成と一致していることを確認してください。

手順

1. 元の仮想マシンのデータストアからバックアップファイルをローカルシステムにダウンロードします。
 - a. ストレージセクションに移動し、仮想マシンのバックアップファイルが格納されているデータストアを選択してください。
 - b. 「ファイル」セクションを選択してください。
 - c. 必要なバックアップディレクトリをダウンロードしてください。
2. 既存の仮想マシンの電源を切ります。次に、元のデプロイメントと同じOVAファイルを使用して、新しい仮想マシンをデプロイします。
3. vCenter Server から、メンテナンスコンソールを開きます。
4. メンテナンス ユーザとしてログインします。
5. `4`を入力して、「サポートと診断」を選択してください。

6. '2'を入力して「リモート診断アクセスを有効にする」オプションを選択し、診断アクセス用の新しいパスワードを作成してください。
7. ダウンロードしたディレクトリからバックアップファイルを選択してください。最新のバックアップを確認するには、`OTV_backup_info.txt` ファイルを参照してください。
8. バックアップファイルを新しい仮想マシンに転送するには、次のコマンドを使用します。指示が表示されたら、診断パスワードを入力してください。

```
scp <OTV_backup_X.tar.enc>  
diag@<node_ip>:/home/diag/system_recovery.tar.enc
```



コマンドで指定されている宛先パスとファイル名 (`/home/diag/system_recovery.tar.enc`) は変更しないでください。

9. バックアップファイルの転送が完了したら、診断シェルにログインして、次のコマンドを実行します。

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

ログは `_var/log/post-deploy-upgrade.log` ファイルに記録されます。

復旧が完了すると、ONTAP tools はサービスと vCenter オブジェクトを復元します。

ONTAP toolsをアンインストールする

ONTAP tools for VMware vSphereをアンインストールすると、ツール内のすべてのデータが削除されます。

手順

1. ONTAP tools for VMware vSphere が管理するデータストアからすべての仮想マシンを削除または移動します。
 - 仮想マシンを削除するには、["VMとVMテンプレートを削除して再登録する"](#)を参照してください。
 - 管理対象外のデータストアに移動するには、["ストレージ vMotion を使用して仮想マシンを移行する方法"](#)を参照してください。
2. ["データストアを削除します"](#) ONTAP tools for VMware vSphere で作成されました。
3. VASAプロバイダーを有効にしている場合は、ONTAP toolsで「Settings」>「VASA Provider settings」>「Unregister」を選択して、すべてのvCenterサーバーからVASAプロバイダーの登録を解除します。
4. すべてのストレージバックエンドを vCenter Server インスタンスから関連付け解除します。["ストレージバックエンドとvCenter Serverインスタンスの関連付けを解除する"](#) を参照してください。
5. すべてのストレージバックエンドを削除します。["ストレージバックエンドの管理"](#)を参照してください。
6. VMware Live Site RecoveryからSRAアダプタを削除します。
 - a. VMware Live Site Recovery アプライアンスの管理インターフェイスにポート 5480 を使用して管理者としてログインします。

- b. 「Storage Replication Adapters」を選択します。
 - c. 該当するSRAカードを選択し、ドロップダウンメニューから*削除*を選択してください。
 - d. アダプターを削除した場合の結果を理解した上で、*削除*を選択してください。
7. ONTAP tools for VMware vSphereにオンボードされたvCenterサーバーインスタンスを削除します。"[vCenter Server インスタンスの管理](#)"を参照してください。
 8. vCenter ServerからONTAP tools for VMware vSphereのVMの電源をオフにし、VMを削除します。

次は？

["FlexVol ボリュームの削除"](#)

ONTAP toolsをアンインストールした後、FlexVolボリュームを削除する

専用の ONTAP クラスターを ONTAP tools for VMware のデプロイメントに使用すると、多くの未使用の FlexVol ボリュームが作成されます。ONTAP tools for VMware vSphere を削除した後は、パフォーマンスへの影響を避けるために FlexVol ボリュームを削除してください。

手順

1. ONTAP tools management ノード VM から、VMware vSphere 用 ONTAP tools のデプロイメントタイプを確認します。デプロイメントタイプを確認するには、次のコマンドを実行します：`cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol`

iSCSI環境の場合は、igroupも削除してください。
2. FlexVol volumeの一覧を取得します。`kubectl describe persistentvolumes | grep internalName | awk -F='{' '{print $2}'`
3. VM をvCenter Server から削除します。"[VMとVMテンプレートを削除して再登録する](#)"を参照してください。
4. FlexVol ボリュームを削除します。"[FlexVolの削除](#)"を参照してください。ボリュームを削除するには、CLI コマンドに正確な FlexVol ボリューム名を入力してください。
5. iSCSI 展開の場合は、ONTAP ストレージシステムから SAN igroups を削除します。"[SANのイニシエータとigroupの表示と管理](#)"を参照してください。

VMware vSphere 向け ONTAP tools のアップグレード

ONTAP tools for VMware vSphere 10.x から 10.5 へのアップグレード

ONTAP tools for VMware vSphere 10.3 または 10.4 から 10.5 にアップグレードできます。ただし、ONTAP tools 10.0、10.1、または 10.2 から 10.5 にアップグレードするには、まず 10.3 または 10.4 にアップグレードしてから 10.5 に進む必要があります。



- ASA r2 システムの場合は、ストレージ可用性ゾーン（SAZ）を追加で設定する前に、ONTAP tools for VMware vSphere を 10.5 に、ONTAP を 9.16.1 にアップグレードしてください。
- ONTAP tools for VMware vSphere 10.3 または 10.4 から 10.5 へのアップグレードが失敗した場合、ロールバックはできません。設定を復元するには、低RPOまたはスナップショットリカバリを使用してください。ONTAP tools for VMware vSphere 10.2以前のバージョンの場合は、設定を復元するためにゼロRPOを使用してください。

開始する前に

- すべてのノードがアクティブであることを確認してください。
- ONTAP システム証明書とオンボードされた vCenter 証明書の有効期間が少なくとも 5 日間あることを確認してください。証明書の有効期限がそれより早く切れる場合、アップグレードは失敗します。
- すべてのノードに、容量100GBの5台目のディスクが搭載されていることを確認してください。
- ノード構成が下記の表の仕様と一致していることを確認してください。

デプロイメントタイプ	ノードあたりのCPU（コア）	ノードあたりのメモリ容量（GB）	ノードあたりのディスク容量（GB）	合計CPU（コア）	メモリ（GB）	ディスク容量合計（GB）
非HA Small	9	18	350	9	18	350
非HA Medium	13	26	350	13	26	350
HA Small	9	18	350	27	54	1050
HA Medium	13	26	350	39	78	1050
HA Large	17	34	350	51	102	1050

- CPUとRAMのホットプラグインが有効になっていることを確認してください。
- 低 RPO バックアップを有効にし、vCenter クライアントインターフェースにバックアップが 1 つ表示されていることを確認してください。アップグレード前にバックアップフォルダをダウンロードしてください。
- RPO（目標復旧時点）が低いバックアップを推奨します。ただし、非HA展開では、アップグレード前にONTAP tools仮想マシンの静止スナップショットを取得できます。

バックアップとリカバリの詳細については、["バックアップ設定を編集する"](#)および["ONTAP tools のセット"](#)

[アップを復元する](#)を参照してください。

手順

1. ONTAP tools for VMware vSphere のアップグレード 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、「アクション」>「設定の編集」を選択します。プライマリVM名を特定するには：
 - a. 任意のノードで診断シェルを有効にする
 - b. 次のコマンドを実行します。

```
grep sourceHost /opt/netapp/meta/ansible_vars.yaml
```
3. 編集設定ウィンドウの「CD/DVDドライブ」フィールドで、「コンテンツライブラリISOファイル」を選択します。
4. ISOファイルを選択し、**CD/DVD drive** フィールドの **Connected** ボックスにチェックを入れて、**OK** をクリックします。
5. vCenter Server から、ONTAP tools へのコンソールを開きます。
6. メンテナンス ユーザとしてログインします。
7. **2** を入力して **System Configuration** メニューを選択します。
8. 「アップグレード」オプションを選択するには、**6** を入力してください。
9. プロンプトが表示されたら、vCenter のクレデンシャルを入力します。これは、ONTAP tools がホストされている vCenter インスタンスです。

2つのvCenter Server構成でONTAP toolsを使用している場合（アプライアンスが1つのvCenterインスタンスでホストされ、別のインスタンスを管理する場合）、ONTAP toolsをホストしているvCenterインスタンスに制限付きロールを割り当てることができます。OVFテンプレートのデプロイに必要な権限のみを持つ専用のvCenterユーザーとロールを作成できます。詳細については、"[ONTAP tools for VMware vSphere 10 に含まれるロール](#)"に記載されているロールを参照してください。

ONTAP tools で管理される vCenter インスタンスについて、vCenter ユーザーアカウントに管理者権限があることを確認してください。

アップグレード中に、オンボーディングされたストレージバックエンド証明書にサブジェクト代替名（SAN）エントリが欠落している場合、欠落しているSANを示すプロンプトが表示されます。SANの検証を行わずに続行することを選択した場合、アップグレードは継続されますが、潜在的なセキュリティリスクがあるため、これは推奨されません。

10. アップグレードを行うと、以下の操作が自動的に実行されます：
 - a. ゲートウェイ証明書は、1年間の有効期間で更新されます。以前の SRA アダプターを削除して新しい 10.5 アダプターをアップロードすると、SRA 証明書の有効期間が 10 年から 1 年に変更されます。
 - b. リモートプラグインがアップグレードされました
 - c. ONTAPおよびvCenter Serverの証明書が検証され、ONTAP toolsに追加されます
 - d. バックアップが有効になっています

次の手順

ONTAP tools for VMware vSphere 10.5 へのアップグレード後：

- ・システムアラートを監視し、ゲートウェイ証明書の有効期限が1年後に切れる前に更新する計画を立ててください。
- ・ONTAP tools 10.4 または 10.3 の SRA アダプタを削除し、10.5 SRA アダプタの tar ファイルをアップロードします。
- ・SRAアダプタのtarファイルをアップロードした後、インストールコマンドを実行します。その後、SRAアダプタを再スキャンして、VMware Site Recovery のストレージレプリケーションアダプタページを更新します。

アップグレード後は、以下のことが可能になります。

- ・マネージャーのユーザーインターフェースからサービスを無効にします
- ・非HA構成からHA構成へ移行する
- ・非HAの小型構成を非HAの中型構成、またはHAの中型もしくは大型構成にスケールアップします。

関連情報

["ONTAP tools for VMware vSphere 9.xx から 10.5 への移行"](#)

ONTAP toolsのアップグレードエラーコード

ONTAP tools for VMware vSphereのアップグレード操作中にエラーコードが表示される場合があります。エラーコードは5桁で、最初の2桁は問題が発生したスクリプトを表し、最後の3桁はそのスクリプト内の特定のワークフローを表します。

すべてのエラーログは、問題の追跡と解決を容易にするために、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 タスクが含まれています。



このページに記載されているエラーコードは参考情報としてのみご利用ください。エラーが解消されない場合、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。

以下の表は、エラーコードとそれに対応するファイル名を示しています。

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

09	post-deploy-upgrade.pl
----	------------------------

エラーコードの最後の3桁は、スクリプト内の具体的なワークフローエラーを示します。

アップグレードエラーコード	ワークフロー	解決
052	ISOイメージは、現行バージョンと同じか、現行バージョンから2つ上のバージョンである可能性があります。	現在使用しているバージョンからアップグレードするには、互換性のあるISOバージョンを使用してください。
068	Debianパッケージのロールバックが失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
069	ファイルの復元に失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
070	バックアップの削除に失敗しました	-
071	Kubernetesクラスターが正常ではありませんでした	-
074	ISOのマウントに失敗しました	/var/log/upgrade-run.logを確認し、アップグレードを再試行してください。
075	アップグレードの事前チェックが失敗しました	アップグレードを再試行してください。
076	レジストリのアップグレードに失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
077	レジストリのロールバックに失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
078	オペレーターのアップグレードに失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
079	オペレーターのロールバックが失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
080	サービスのアップグレードに失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。

アップグレードエラーコード	ワークフロー	解決
081	サービスのロールバックに失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
082	コンテナから古いイメージを削除できませんでした	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
083	バックアップの削除に失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
084	JobManagerを本番環境に戻す変更が失敗しました	アップグレードを復旧／完了するには、以下の手順を実行してください。1.診断シェルを有効にします。2.次のコマンドを実行します : <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</code> 3./var/log/post-deploy-upgrade.log のログを確認してください。
087	アップグレード後の手順が失敗しました。	アップグレードを復旧／完了するには、以下の手順を実行してください。1.診断シェルを有効にします。2. <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</code> コマンドを実行します。3./var/log/post-deploy-upgrade.log のログを確認してください。
088	journald のログローテーションの設定に失敗しました	VMがホストされているホストと互換性のあるVMのネットワーク設定を確認してください。VMを別のホストに移行して再起動してみてください。
089	サマリーログローテーション設定ファイルの所有権変更失敗しました	アップグレードを再試行してください。
095	OSアップグレードに失敗しました	OSアップグレードの復旧はできません。ONTAP tools サービスがアップグレードされ、新しいポッドが稼働します。
096	動的ストレージプロビジョナーをインストールする	アップグレードログを確認し、アップグレードを再試行してください。

アップグレードエラーコード	ワークフロー	解決
097	アップグレードのためのサービスのアンインストールに失敗しました	RPOゼロまたはスナップショットベースのリカバリを使用して、アップグレードを再試行してください。
098	ntv-system から dynamic storage provisioner 名前空間への dockercred シークレットのコピーに失敗しました	アップグレードログを確認し、アップグレードを再試行してください。
099	新しいHDDの追加を検証できませんでした	HA構成の場合はすべてのノードに、非HA構成の場合は1つのノードに新しいHDDを追加してください。
109	永続ボリュームデータのバックアップに失敗しました	アップグレードログを確認し、アップグレードを再試行してください。
110	永続ボリュームデータの復元に失敗しました	ゼロRPOまたはスナップショットベースのリカバリを使用し、アップグレードを再試行してください。
111	RKE2 の etcd タイムアウトパラメータの更新に失敗しました	アップグレードログを確認し、アップグレードを再試行してください。
112	動的ストレージプロビジョナーのアンインストールに失敗しました	-
113	セカンダリノードのリソース更新に失敗しました	アップグレードログを確認し、アップグレードを再試行してください。
104	セカンダリノードの再起動に失敗しました	ノードを1つずつ手動で再起動します。
100	カーネルのロールバックに失敗しました	-
051	動的ストレージプロビジョナーのアップグレードに失敗しました	アップグレードログを確認し、アップグレードを再試行してください。
056	移行バックアップの削除に失敗しました	NA
090	ストレージバックエンドおよびvCenterの証明書検証が失敗しました	アップグレードログと/var/log/cert_validation_error.logにあるログファイルを確認し、アップグレードを再試行してください。

アップグレードエラーコード	ワークフロー	解決
114	MongoDBコレクションの内部証明書更新が失敗しました	アップグレードがエラーコード114で失敗した場合は、以下の手順を実行してください： 1. プライマリノード上のアップグレード用ISOに接続し、診断シェルを有効にします。 2. プライマリ ノードへの SSH セッションから ISO をマウントします。 <pre>sudo mount /dev/cdrom sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade</pre> 3. Debianパッケージをインストールする： <pre>sudo dpkg -iE /upgrade/dists/sque eze/main/binary- amd64/vplatform.deb sudo dpkg -iE /upgrade/dists/sque eze/main/binary- amd64/vpupgrader.de b sudo dpkg -iE /upgrade/dists/sque eze/main/binary- amd64/vmware- tools.deb</pre> 4. ビルド情報ファイルをコピーします： <pre>sudo cp /upgrade/APPLIANCE_ BUILD /</pre> 診断シェルを有効にして以下のコマンドを実行することで、証



ONTAP tools for VMware vSphere 10.3 以降、ゼロ RPO はサポートされていません。⁵

明書をコレクションに追加しま

詳細については、"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を復元する方法"

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--internal_cert_upd
ate_collection
```

```
`/var/log/otvng/pos
t-deploy-
upgrade.log`でログを
確認してください。
```

6. ノードを再起動します。

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. アップグレード後の手順を実行します。

ONTAP tools for VMware vSphere 9.xx から 10.5 への移行

ONTAP tools for VMware vSphere 9.xx から 10.5 への移行

NetApp ONTAP tools for VMware vSphereのセットアップをバージョン9.xxから10.5に移行するには、バージョン間で製品的大幅なアップデートと機能強化が行われているため、移行プロセスが必要です。

ONTAP tools for VMware vSphere 9.12D1、9.13D2、および 9.13P2 リリースから ONTAP tools for VMware vSphere 10.5 に移行できます。

セットアップにNFSおよびVMFSデータストアがあり、vVolsデータストアがない場合は、ONTAP tools 9.xxをアンインストールして、ONTAP tools 10.5を導入するだけです。ただし、セットアップにvVolsデータストアが含まれている場合は、VASAプロバイダーとSRAを移行するプロセスを実行する必要があります。

以下の表は、これら2つの異なるシナリオにおける移行プロセスを示しています。

セットアップにvVolsデータストアがある場合	セットアップにNFSおよびVMFSデータストアのみが含まれている場合
手順： 1." VASAプロバイダーを移行する " 2. " VMストレージポリシーを作成する "	手順： 1.お使いの環境から ONTAP tools 9.xx を削除します。 " 環境からOTV 9.xxを削除する方法 " NetApp ナレッジベースの記事を参照してください。 2." ONTAP tools for VMware vSphere 10.5 のデプロイと構成 " 3." SRAの更新 " 4. " VMストレージポリシーを作成する "



ONTAP tools for VMware vSphere 9.xx から 10.5 に移行すると、NVMe/FC プロトコルを使用する vVols データストアは、ONTAP tools 10.5 が NVMe-oF プロトコルを VMFS データストアでのみサポートするため、動作しなくなります。

VASA プロバイダーを移行し、ONTAP ツールで SRA を更新する

このセクションの手順に従って、ONTAP tools for VMware vSphere 9.xx から ONTAP tools for VMware vSphere 10.5 に VASA プロバイダーを移行し、VMware Live Site Recovery アプライアンス上の Storage Replication Adapter (SRA) を更新します。

VASAプロバイダーを移行する手順

1. 既存の ONTAP tools for VMware vSphere で Derby PORT 1527 を有効にするには、rootユーザーを有効にして、SSH経由でCLIにログインします。次に、以下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 10.5 の OVA をデプロイします。
3. 移行対象のvCenter ServerインスタンスをONTAP tools for VMware vSphere 10.5リリースに追加します。
詳細については、"[vCenter Server インスタンスを追加する](#)"を参照してください。
4. "[VASA Provider の有効化](#)" ONTAP tools for VMware vSphere 10.5 上のサービス。
5. vCenter サーバー API を使用して、ONTAP tools プラグイン用の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。詳細については、"[vSphere クライアントインターフェースを使用してストレージバックエンドを追加する](#)"を参照してください。
6. REST API リクエストを認証するためのアクセストークンを取得します。以下の例を参考に、変数をご使用の環境に合わせた値に置き換えてください。
8. ログを確認して、正常に完了したことを確認します。

```
do perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--postupgrade
```

```
curl --request POST \
  --location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/vcenter-
login" \
  --header "Content-Type: application/json" \
  --header "Accept: */*" \
  -d '{"username": "$MYUSER", "password": "$MYPASSWORD", "vcenter
hostname": "$MYVCENTER"}'
```

レスポンスで返されたアクセストークンをコピーして保存してください。

7. Swagger または Postman から次の API を発行して移行します。

```
curl -X POST
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

```
sudo umount -l -f
```

```
/dev/cdrom
```

SwaggerにはこのURLからアクセスできます： `https://$FQDN_IP_PORT/`、例えば：
`https://10.67.25.33:8443/`。

10. プライマリ ノードをリブート
します：

```
sudo reboot -f
```


HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTPメソッド	パス
POST	/api/v1

処理タイプ

非同期

Curl の例

```
curl -X POST 'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <auth_token>' \
--header 'Content-Type: application/json' \
--data '{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxxx",
    "password": "*****"
  },
  "database_password": "*****"
}'
```

他のリリースへの移行に関するリクエスト本文：

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxxx",
    "password": "*****"
  }
}
```

JSON出力例

システムはジョブオブジェクトを返します。次のステップで使用するため、ジョブ識別子を保存してください。

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

8. Swagger でステータスを確認するには、以下の URI を使用してください：

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

前の手順で移行ジョブから返された「id」値を使用します。ジョブが完了したら、ジョブ応答の移行レポートを確認します。

9. VASA Provider を ONTAP tools for VMware vSphere に登録します。手順については、["VASAプロバイダーを登録する"](#)を参照してください。
10. VASA Provider の登録を確認します：
 - a. vSphere Client で、vCenter Server に移動します。
 - b. **Configure > Storage Providers** を選択します。
 - c. 前の手順で登録した VASA プロバイダーがオンラインになっていることを確認します。
11. 以下の手順に従って、ONTAP tools for VMware vSphere ストレージプロバイダー 9.10/9.11/9.12/9.13 の VASA Provider サービスを停止します。
 - a. ONTAP tools 9.x で、Webコンソールを開きます。
 - b. メンテナンス コンソールにアクセスします。
 - c. `1`を入力して、「アプリケーション設定」メニューを選択します。
 - d. 入力 `5`して、VASA ProviderおよびSRAサービスを停止します。
 - e. vSphere Client で、vCenter Server に移動し、**Configure > Storage Providers** を選択します。
 - f. オフラインの VASA Provider for ONTAP tools 9.x を選択し、*削除*を選択します。

古い VASA プロバイダーが停止された後、vCenter サーバーは 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 がアクセス可能になり、ONTAP tools for VMware vSphere から提供されます。

12. 移行された NFS および VMFS データストアは、データストア検出ジョブの後に ONTAP tools for VMware vSphere 10.5 に表示されます。このジョブには最大 30 分かかる場合があります。概要ページでの表示状況を確認してください。
13. SwaggerまたはPostmanの以下のAPIを使用してパッチ移行を実行します。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTPメソッド	パス
PATCH	/api/v1

処理タイプ

非同期

Swaggerでは以下のURIを使用してください。

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次のメソッドとエンドポイントを使用します。

HTTPメソッド	パス
PATCH	/api/v1

処理タイプ

非同期

Swaggerでは以下のURIを使用してください。

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Curl の例

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-4ce66f802c35`
```

JSON出力例

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



ステップ7で返された「migration_id」値を<migration_id>としてPATCH API呼び出しで使
します。パッチ操作のリクエスト本体は空です。



UUIDは、post-migrate APIへの応答として返される移行UUIDです。

パッチ移行APIを実行した後、すべての仮想マシンはストレージポリシーに準拠します。

次の手順

移行が完了し、ONTAP tools 10.5 を vCenter Server に登録したら、次の手順に従ってください。

- **Discovery** が完了するまでお待ちください。システムはすべてのホスト上で証明書を自動的に更新しま
す。
- データストアおよび仮想マシンの操作を開始する前に、しばらくお待ちください。待ち時間は、ホスト、
データストア、仮想マシンの数によって異なります。待機しない場合、断続的な障害が発生することがあ
ります。

アップグレード後、仮想マシンのコンプライアンス状態が古い場合は、以下の手順に従ってストレージポリ
シーを再適用してください。

1. データストアに移動し、概要 > *VMストレージポリシー*を選択します。
2. システムは、*VMストレージポリシー準拠*のコンプライアンスステータスを*期限切れ*として表示しま
す。
3. ストレージVMポリシーと、それに対応するVMを選択します。
4. 「適用」を選択します。
5. *VMストレージポリシー準拠*における準拠状況は「準拠」と表示されます。

関連情報

- ["ONTAP tools for VMware vSphere 10 RBACについて"](#)
- ["ONTAP tools for VMware vSphere 10.x から 10.5 へのアップグレード"](#)

ストレージレプリケーションアダプタ（SRA）を更新する手順

開始する前に

復旧計画において、保護サイトとは仮想マシンが現在稼働している場所を指し、復旧サイトとは仮想マシンが
復旧される場所を指します。VMware Live Site Recovery アプライアンスのインターフェイスには、保護対象
サイトとリカバリサイトに関する詳細情報とともに、リカバリプランの状態が表示されます。復旧プランで
は、CLEANUP ボタンと REPROTECT ボタンは無効になりますが、TEST ボタンと RUN ボタンは有効なま
まです。これは、そのサイトがデータ復旧に対応できる状態にあることを示しています。SRA を移行する前

に、一方のサイトが保護状態にあり、もう一方のサイトが復旧状態に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いても、再保護が保留中の場合は、移行を開始しないでください。移行を進める前に、再保護プロセスが完了していることを確認してください。テスト フェイルオーバーが進行中の場合は、テスト フェイルオーバーをクリーンアップして移行を開始します。

1. VMware Site Recovery で VMware vSphere 9.xx 用の ONTAP tools SRA アダプタを削除するには、次の手順に従ってください：
2. VMware Live Site Recovery の構成管理ページに移動します。
 - a. 「Storage Replication Adapter」セクションに移動してください。
 - b. 省略記号メニューから*設定のリセット*を選択してください。
 - c. 省略記号メニューから*削除*を選択してください。
3. 保護サイトと復旧サイトの両方で、これらの手順を実行してください。
 - a. ["ONTAP tools for VMware vSphere サービスを有効にする"](#)
 - b. 次の手順に従って、VMware vSphere 10.5 SRA アダプター用の ONTAP tools for VMware vSphere を設定します。"[VMware Live Site RecoveryアプライアンスでSRAを構成する](#)"
 - c. VMware Live Site Recovery インターフェースで、**Discover Arrays** と **Discover Devices** を実行します。デバイスが移行前と同じように表示されることを確認します。

REST API を使用した自動化

ONTAP tools REST APIについて学ぶ

ONTAP tools for VMware vSphere 10は、仮想マシンのライフサイクル管理のためのツールセットです。自動化プロセスの一部として使用できる堅牢なREST APIが含まれています。

基盤としてのREST Webサービス

Representational State Transfer (REST) は、Web サービス API の設計を含む、分散型 Web アプリケーションを作成するためのスタイルです。これは、サーバーベースのリソースを公開し、その状態を管理するための一連の技術を確立するものです。

リソースと状態の表示

リソースは、REST Webサービスアプリケーションの基礎となる構成要素です。REST APIを設計する際には、まず2つの重要なタスクがあります：

- システムまたはサーバーベースのリソースを特定する
- リソースの状態と関連する状態遷移操作を定義します

クライアントアプリケーションは、明確に定義されたメッセージフローを通じて、リソースの状態を表示および変更できます。

HTTPメッセージ

ハイパーテキスト転送プロトコル（HTTP）は、Webサービスクライアントとサーバーがリソースに関するメッセージを交換するために使用するプロトコルです。これは、作成、読み取り、更新、削除という一般的な操作に基づくCRUDモデルに従っています。HTTPプロトコルには、リクエストヘッダーとレスポンスヘッダー、およびレスポンスステータスコードが含まれます。

JSONデータフォーマット

利用可能なメッセージ形式はいくつかありますが、最も人気のあるオプションはJavaScriptオブジェクト表記法（JSON）です。JSONは、シンプルなデータ構造をプレーンテキストで表現するための業界標準であり、リソースや必要なアクションを記述する状態情報を転送するために使用されます。

セキュリティ

セキュリティはREST APIの重要な側面です。ネットワーク上のHTTPトラフィックを保護するために使用されるトランスポート層セキュリティ（TLS）プロトコルに加えて、ONTAP tools for VMware vSphere 10 REST APIも認証にアクセストークンを使用します。アクセストークンを取得し、以降のAPI呼び出しで使用する必要があります。

非同期リクエストのサポート

ONTAP tools for VMware vSphere 10 REST API は、ほとんどのリクエストを同期的に処理し、操作が完了するとステータスコードを返します。また、完了までに時間がかかるタスクに対して、非同期処理もサポートしています。

ONTAP tools Manager環境

ONTAP tools Manager環境には、考慮すべきいくつかの側面があります。

仮想マシン

ONTAP tools for VMware vSphere 10 は、vSphere リモートプラグインアーキテクチャを使用してデプロイされます。REST API のサポートを含むソフトウェアは、別の仮想マシンで実行されます。

ONTAP tools の IP アドレス

ONTAP tools for VMware vSphere 10は、仮想マシンの機能へのゲートウェイを提供する単一のIPアドレスを公開します。初期設定時にアドレスを指定する必要があり、そのアドレスは内部ロードバランサーコンポーネントに割り当てられます。このアドレスは、ONTAP tools Managerのユーザーインターフェース、Swaggerドキュメントページへのアクセス、およびREST APIへの直接アクセスに使用されます。

2つのREST API

ONTAP tools for VMware vSphere 10 REST API に加えて、ONTAP クラスターには独自の REST API があります。ONTAP tools Manager は、ストレージ関連のタスクを実行するクライアントとして ONTAP REST API を使用します。これら 2 つの API は別個のものであることを念頭に置いておくことが重要です。詳細については、["ONTAPの自動化"](#)を参照してください。

ONTAP tools REST API実装の詳細

REST はオープン スタンダードな技術とベストプラクティスを確立しますが、各 API の具体的な実装は設計上の選択によって異なる場合があります。ONTAP tools for VMware vSphere 10 REST API を使用する前に、その設計について理解しておく必要があります。

REST API には、vCenters やアグリゲートなど、複数のリソースカテゴリが含まれています。詳細については、["API リファレンス"](#)を参照してください。

REST API へのアクセス方法

ONTAP tools for VMware vSphere 10 REST API には、ONTAP tools の IP アドレスとポートを使用してアクセスできます。完全な URL は、以下のいくつかの部分から構成されています。

- ONTAP tools の IP アドレスとポート
- APIのバージョン
- リソースカテゴリ
- 特定のリソース

初期設定時にIPアドレスを設定する必要がありますが、ポート番号は8443に固定されています。URLの最初の部分は、ONTAP tools for VMware vSphere 10の各インスタンスで共通です。エンドポイント間で変更されるのは、リソースカテゴリと特定のリソースのみです。



以下の例に示されているIPアドレスとポート番号は、あくまで例示目的です。ご使用の環境に合わせてこれらの値を変更する必要があります。

認証サービスにアクセスする例

https://10.61.25.34:8443/virtualization/api/v1/auth/login

このURLを使用すると、POSTメソッドでアクセストークンをリクエストできます。

vCenter サーバーを一覧表示する例

https://10.61.25.34:8443/virtualization/api/v1/vcenters

このURLを使用して、GETメソッドで定義済みのvCenterサーバーインスタンスのリストをリクエストできます。

HTTP の詳細

ONTAP tools for VMware vSphere 10 REST API は、HTTP および関連するパラメータを使用して、リソースインスタンスとコレクションに対して操作を実行します。HTTP 実装の詳細については、以下に示します。

HTTPメソッド

REST API でサポートされている HTTP メソッド（動詞）を以下の表に示します。

方法	CRUD	説明
GET	読み取り	リソースインスタンスまたはコレクションのオブジェクトプロパティを取得します。コレクションで使用する場合、これはリスト操作とみなされます。
POST	作成	入力パラメータに基づいて新しいリソースインスタンスを作成します。
PUT	更新	指定されたJSONリクエストボディを使用して、リソースインスタンス全体を更新します。ユーザーが変更できないキー値は保持されます。
PATCH	更新	リクエストで選択された変更内容をリソースインスタンスに適用するように要求します。
DELETE	削除	既存のリソース インスタンスを削除します。

リクエストヘッダーとレスポンスヘッダー

次の表は、REST API で使用される最も重要な HTTP ヘッダーをまとめたものです。

ヘッダー	Type	使用上の注意
Accept	要求	これは、クライアントアプリケーションが受け入れることができるコンテンツの種類です。有効な値には `*/` または `application/json` が含まれます。
x-auth	要求	クライアントアプリケーションを通じてリクエストを発行したユーザーを識別するアクセストークンが含まれています。
Content-Type	応答	サーバーから返された値（`Accept` リクエストヘッダーに基づく）。

HTTPステータスコード

REST API で使用される HTTP ステータスコードについて、以下に説明します。

Code	説明	説明
200	OK	新しいリソースインスタンスを作成しない呼び出しが成功したことを示します。
201	Created	リソースインスタンスの一意的識別子を持つオブジェクトが正常に作成されました。
202	Accepted	リクエストは承認され、リクエストを実行するためのバックグラウンドジョブが作成されました。
204	コンテンツなし	リクエストは成功しましたが、コンテンツは返されませんでした。
400	Bad request	要求の入力が認識されないか不適切です。
401	Unauthorized	ユーザーには権限が付与されていないため、認証を行う必要があります。
403	Forbidden	認証エラーのためアクセスが拒否されました。
404	Not found	リクエストで参照されているリソースは存在しません。
409	競合	オブジェクトがすでに存在するため、オブジェクトの作成に失敗しました。
500	内部エラー	サーバで一般的な内部エラーが発生しました。

認証

REST API に対するクライアントの認証は、アクセストークンを使用して実行されます。トークンおよび認証プロセスの関連する特性は次のとおりです。

- クライアントは、ONTAP tools Manager の管理者認証情報（ユーザー名とパスワード）を使用してトークンを要求する必要があります。
- トークンはJSON Web Token（JWT）形式でフォーマットされます。
- 各トークンは60分後に有効期限が切れます。
- クライアントからの API リクエストには、`x-auth` リクエストヘッダーにトークンを含める必要があります。

アクセストークンの要求と使用例については、["最初のREST API呼び出し"](#)を参照してください。

同期リクエストと非同期リクエスト

ほとんどの REST API 呼び出しは迅速に完了するため、同期的に実行されます。つまり、リクエストが完了するとステータスコード（200 など）を返します。処理に時間がかかるリクエストは、バックグラウンドジョブを使用して非同期で実行されます。

非同期で実行されるAPI呼び出しを発行した後、サーバーはHTTPステータスコード202を返します。これは、リクエストが受理されたものの、まだ完了していないことを示しています。バックグラウンドジョブを照会することで、成功または失敗などのステータスを確認できます。

非同期処理は、データストアやvVol操作など、長時間実行される複数の種類の操作に使用されます。詳細については、SwaggerページのREST APIのジョブマネージャーカテゴリを参照してください。

最初のONTAP tools REST API呼び出しを実行する

curl を使用して API 呼び出しを発行することで、ONTAP tools for VMware vSphere 10 REST API を使い始めることができます。

開始する前に

curlの例で必要とされる情報とパラメータを確認してください。

必須情報

必要なものは以下のとおりです：

- ONTAP tools for VMware vSphere 10 の IP アドレスまたは FQDN とポート番号
- ONTAP tools Manager 管理者の資格情報（ユーザー名とパスワード）

パラメータと変数

以下に示すcurlの例には、Bashスタイルの変数が含まれています。これらの変数は、Bash環境で設定することも、コマンドを実行する前に手動で更新することもできます。変数を設定すると、シェルは各コマンドを実行する前に、その値を代入します。各変数は以下の表に記載されています。

変数	説明
\$FQDN_IP_PORT	ONTAP tools Manager の完全修飾ドメイン名または IP アドレスとポート番号。
\$MYUSER	ONTAP tools Manager アカウントのユーザー名。
\$MYPASSWORD	ONTAP tools Manager のユーザー名に関連付けられたパスワード。
\$ACCESS_TOKEN	ONTAP tools Manager によって発行されたアクセストークン。

Linux CLI での以下のコマンドと出力は、変数の設定方法と表示方法を示しています。

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

ステップ1：アクセストークンを取得する

REST API を使用するには、アクセストークンを取得する必要があります。アクセストークンを要求する方法の例を以下に示します。ご使用の環境に合わせて適切な値を代入してください。

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login" \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d '{"username": "$MYUSER", "password": "$MYPASSWORD"}'
```

レスポンスで提供されるアクセストークンをコピーして保存してください。

ステップ2：REST API呼び出しを発行する

アクセストークンを取得したら、curl を使用して REST API 呼び出しを発行できます。最初のステップで取得したアクセストークンを含めてください。

Curlの例

```
curl --request GET \  
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \  
--header "Accept: */*" \  
--header "x-auth: $ACCESS_TOKEN"
```

JSON レスポンスには、ONTAP tools Manager に設定された VMware vCenter インスタンスのリストが含まれています。

ONTAP tools REST APIリファレンス

ONTAP tools for VMware vSphere 10 REST API リファレンスには、すべての API 呼び出しに関する詳細が記載されています。この資料は、自動化アプリケーションを開発する際に役立ちます。

ONTAP tools for VMware vSphere 10 の REST API ドキュメントには、Swagger ユーザーインターフェースを通じてオンラインでアクセスできます。ONTAP tools for VMware vSphere 10 ゲートウェイサービスの IP アドレスまたは FQDN、およびポートが必要です。

手順

1. 以下のURLをブラウザに入力し、変数の部分を適切なIPアドレスとポートの組み合わせに置き換えて、*Enter*キーを押します。

https://\$FQDN_IP_PORT/

例

https://10.61.25.33:8443/

2. 個々のAPI呼び出しの例として、**vCenters** カテゴリまでスクロールし、エンドポイントの横にある **GET** を選択します。 /virtualization/api/v1/vcenters

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

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

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

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

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

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

プライバシー ポリシー

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

オープンソース

通知ファイルは、NetAppソフトウェアで使用されるサードパーティの著作権とライセンスに関する情報を提供します。

["ONTAP tools for VMware vSphere 10.5 に関するお知らせ"](#)

著作権に関する情報

Copyright © 2026 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。