# VMware

## Enterprise applications

NetApp
May 09, 2024

# 目次

VMware . . . 1
ONTAP を使用した VMware vSphere . . . 1
ONTAPを備えた仮想ボリューム（VVOL） . . . 43
VMware Site Recovery ManagerとONTAP . . . 69
ONTAPを使用したvSphere Metroストレージクラスタ . . . 89
製品のセキュリティ . . . 119
ONTAP tools for VMware vSphere向けセキュリティ強化ガイド . . . 123

# VMware

# ONTAP を使用した VMware vSphere

## ONTAP を使用した VMware vSphere

ONTAPは、約20年にわたって業界をリードするVMware vSphere環境向けストレージ解決策であり、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。このドキュメントでは、導入の合理化、リスクの軽減、管理の簡易化を実現するために、最新の製品情報とベストプラクティスを含む ONTAP 解決策 for vSphere について説明します。

以前に公開されていたテクニカルレポート_TR-4597：『VMware vSphere for ONTAP』をこのドキュメントに差し替えます。

ベストプラクティスは、ガイドや互換性リストなどの他のドキュメントを補うものです。ラボテストに基づいて開発されており、ネットアップのエンジニアやお客様は広範な現場経験を積んでいます。すべての環境で機能する唯一のサポート対象となるわけではありませんが、一般に、ほとんどのお客様のニーズを満たす最もシンプルなソリューションです。

本ドキュメントでは、vSphere 7.0以降で実行されるONTAPの最新リリース（9.x）の機能について説明します。を参照してください "NetApp Interoperability Matrix Tool で確認できます" および "VMware Compatibility Guide" 特定のリリースに関する詳細については、を参照してください。

#### ONTAP for vSphere を選ぶ理由

ONTAPをvSphereのストレージ解決策として選択した理由は数多くあります。たとえば、SANとNASの両方のプロトコルをサポートするユニファイドストレージシステム、スペース効率に優れたSnapshotを使用した堅牢なデータ保護機能、アプリケーションデータの管理に役立つ豊富なツールなどです。ハイパーバイザーとは別のストレージシステムを使用すると、さまざまな機能をオフロードして、 vSphere ホストシステムへの投資を最大限に活用できます。このアプローチにより、ホストリソースをアプリケーションワークロードに集中できるだけでなく、ストレージ運用によるアプリケーションのランダムなパフォーマンスへの影響も回避できます。

vSphere と ONTAP を併用すると、ホストハードウェアと VMware ソフトウェアのコストを削減できます。また、一貫した高パフォーマンスを維持しながら、低コストでデータを保護することもできます。仮想化されたワークロードはモバイル対応であるため、 Storage vMotion を使用して、 VMFS 、 NFS 、または VVOL データストア間で VM を移動するさまざまなアプローチを、すべて同じストレージシステム上で検討できます。

お客様が現在重視している主な要因は次のとおりです。

- * ユニファイド・ストレージ。 * ONTAP ソフトウェアを実行するシステムは、いくつかの重要な方法で統合されています。当初、このアプローチは NAS プロトコルと SAN プロトコルの両方を指していましたが、 ONTAP は業界をリードする SAN プラットフォームであり続けており、 NAS における従来の強みもあります。vSphere 環境では、このアプローチは仮想デスクトップインフラ（ VDI ）向けのユニファイドシステムと仮想サーバインフラ（ VSI ）の組み合わせを意味する場合もあります。ONTAP ソフトウェアを実行するシステムは一般に、従来のエンタープライズアレイに比べて VSI の方が安価ですが、同じシステムで VDI を処理するための高度な Storage Efficiency 機能も備えています。また、 ONTAP は、 SSD から SATA までさまざまなストレージメディアを統合し、クラウドへの拡張を容易にします。パフォーマンスのためにフラッシュアレイを1つ、アーカイブ用にSATAアレイを1つ、クラウド用に別 々 のシステムを

購入する必要はありません。ONTAP は、これらすべてを 1 つにまとめます。

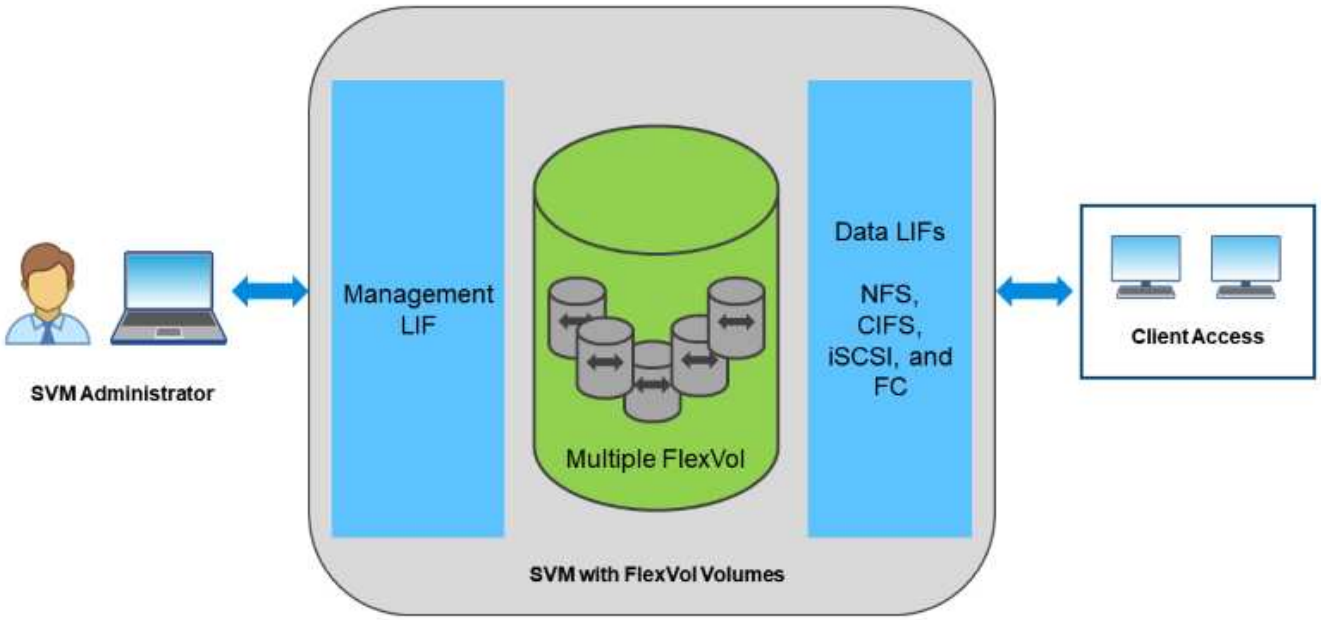
- 仮想ボリュームとストレージポリシーベースの管理。 NetAppは、vSphere Virtual Volume（VVOL）の開発においてVMwareの初期の設計パートナーであり、アーキテクチャに関する情報を提供し、VVOLとVMware vSphere APIs for Storage Awareness（VASA）を早期にサポートしています。このアプローチにより、VMFSでVMストレージをきめ細かく管理できるだけでなく、ストレージポリシーベースの管理によるストレージプロビジョニングの自動化もサポートされました。このアプローチにより、ストレージアーキテクトは、 VM 管理者が簡単に利用できるさまざまな機能を備えたストレージプールを設計できます。ONTAP は VVOL 規模でストレージ業界をリードし、 1 つのクラスタで数十万もの VVol をサポートします。一方、エンタープライズアレイや小規模なフラッシュアレイベンダーは、アレイあたり数千の VVol をサポートします。ネットアップは、 VVOL 3.0 のサポートに向けて、今後追加される機能で、きめ細かな VM 管理の進化も推進しています。
- ストレージ効率。NetAppは本番ワークロードに重複排除機能を初めて提供しましたが、このイノベーションはこの分野の最初のものでも最後のものでもありませんでした。まず、パフォーマンスに影響を与えないスペース効率に優れたデータ保護メカニズムであるSnapshotと、本番環境およびバックアップ用にVMの読み取り/書き込みコピーを瞬時に作成するFlexCloneテクノロジから始まりました。ネットアップは、重複排除、圧縮、ゼロブロック重複排除などのインライン機能を提供し、高価な SSD のストレージを最後まで絞ります。ONTAP は最近、圧縮機能を使用して、より小さな I/O 処理とファイルをディスクブロックに圧縮する機能を追加しました。これらの機能を組み合わせることで、 VSI では最大 5 分の 1 、 VDI では最大 30 分の 1 のコストを削減できました。
- * ハイブリッド・クラウド。 * オンプレミスのプライベート・クラウド、パブリック・クラウド・インフラストラクチャー、または両方の利点を組み合わせたハイブリッド・クラウドのいずれに使用しても、ONTAP ソリューションはデータ管理を合理化し、最適化するためのデータ・ファブリックの構築を支援します。まずハイパフォーマンスのオールフラッシュシステムを導入し、データ保護とクラウドコンピューティングのためにディスクストレージシステムとクラウドストレージシステムのどちらかと組み合わせます。Azure 、 AWS 、 IBM 、 Google のクラウドから選択して、コストを最適化し、ロックインを回避できます。必要に応じて、 OpenStack とコンテナテクノロジの高度なサポートを活用できます。ネットアップ ONTAP では、クラウドベースのバックアップ（ SnapMirror クラウド、 Cloud Backup Service 、 Cloud Sync ）やストレージ階層化 / アーカイブツール（ FabricPool ）も提供しており、運用コストの削減とクラウドの幅広いリーチの活用を支援します。
- * その他。 * NetApp AFF A シリーズアレイの卓越したパフォーマンスを活用して、コストを管理しながら仮想インフラを高速化できます。スケールアウト ONTAP クラスタを使用して、ストレージシステムのメンテナンスからアップグレード、完全な交換まで、完全なノンストップオペレーションを実現します。ネットアップの暗号化機能を追加コストなしで使用して、保存データを保護できます。きめ細かいサービス品質機能により、パフォーマンスがビジネスサービスレベルを満たしていることを確認します。これらはすべて、業界をリードするエンタープライズデータ管理ソフトウェアであるONTAPに付属する幅広い機能の一部です。

## ユニファイドストレージ

NetApp ONTAPは、シンプルなソフトウェア定義型アプローチによってストレージを統合し、セキュアで効率的な管理、パフォーマンスの向上、シームレスな拡張性を実現します。このアプローチにより、データ保護が強化され、クラウドリソースを効果的に利用できるようになります。

当初、このユニファイドアプローチでは、1つのストレージシステムでNASとSANの両方のプロトコルをサポートすることが推奨されていましたが、ONTAPは引き続き業界をリードするSAN向けプラットフォームであり、当初からNASで強みを発揮しています。ONTAPでは、S3オブジェクトプロトコルもサポートされるようになりました。S3はデータストアには使用されませんが、ゲスト内アプリケーションに使用できます。S3プロトコルのサポートの詳細については、ONTAPを参照してください。 "S3構成の概要"。

Storage Virtual Machine（SVM）は、ONTAPのセキュアマルチテナンシーの単位です。これは、ONTAPソフトウェアを実行しているシステムへのクライアントアクセスを許可する論理構成要素です。SVM は、論理インターフェイス（ LIF ）を介して複数のデータアクセスプロトコルを使用して同時にデータをやり取りできます。SVM は、 CIFS や NFS などの NAS プロトコルでファイルレベルのデータアクセスを提供し、 iSCSI 、 FC / FCoE 、 NVMe などの SAN プロトコルでブロックレベルのデータアクセスを提供します。SVM は、S3と同様に、SANクライアントとNASクライアントそれぞれに同時にデータを提供できます。




vSphere 環境では、このアプローチは仮想デスクトップインフラ（ VDI ）向けのユニファイドシステムと仮想サーバインフラ（ VSI ）の組み合わせを意味する場合もあります。ONTAP ソフトウェアを実行するシステムは一般に、従来のエンタープライズアレイに比べて VSI の方が安価ですが、同じシステムで VDI を処理するための高度な Storage Efficiency 機能も備えています。また、 ONTAP は、 SSD から SATA までさまざまなストレージメディアを統合し、クラウドへの拡張を容易にします。パフォーマンスのためにフラッシュアレイを1つ、アーカイブ用にSATAアレイを1つ、クラウド用に別 々 のシステムを購入する必要はありません。ONTAP は、これらすべてを 1 つにまとめます。

注： SVM、ユニファイドストレージ、およびクライアントアクセスの詳細については、 "ストレージ仮想化" ONTAP 9 ドキュメントセンターを参照してください。

## ONTAP の仮想化ツール

ネットアップでは、 ONTAP および vSphere と組み合わせて使用し、仮想環境を管理できるスタンドアロンのソフトウェアツールをいくつか提供しています。

ONTAP ライセンスには、追加コストなしで次のツールが含まれています。vSphere 環境でこれらのツールがどのように連携するかについては、図 1 を参照してください。

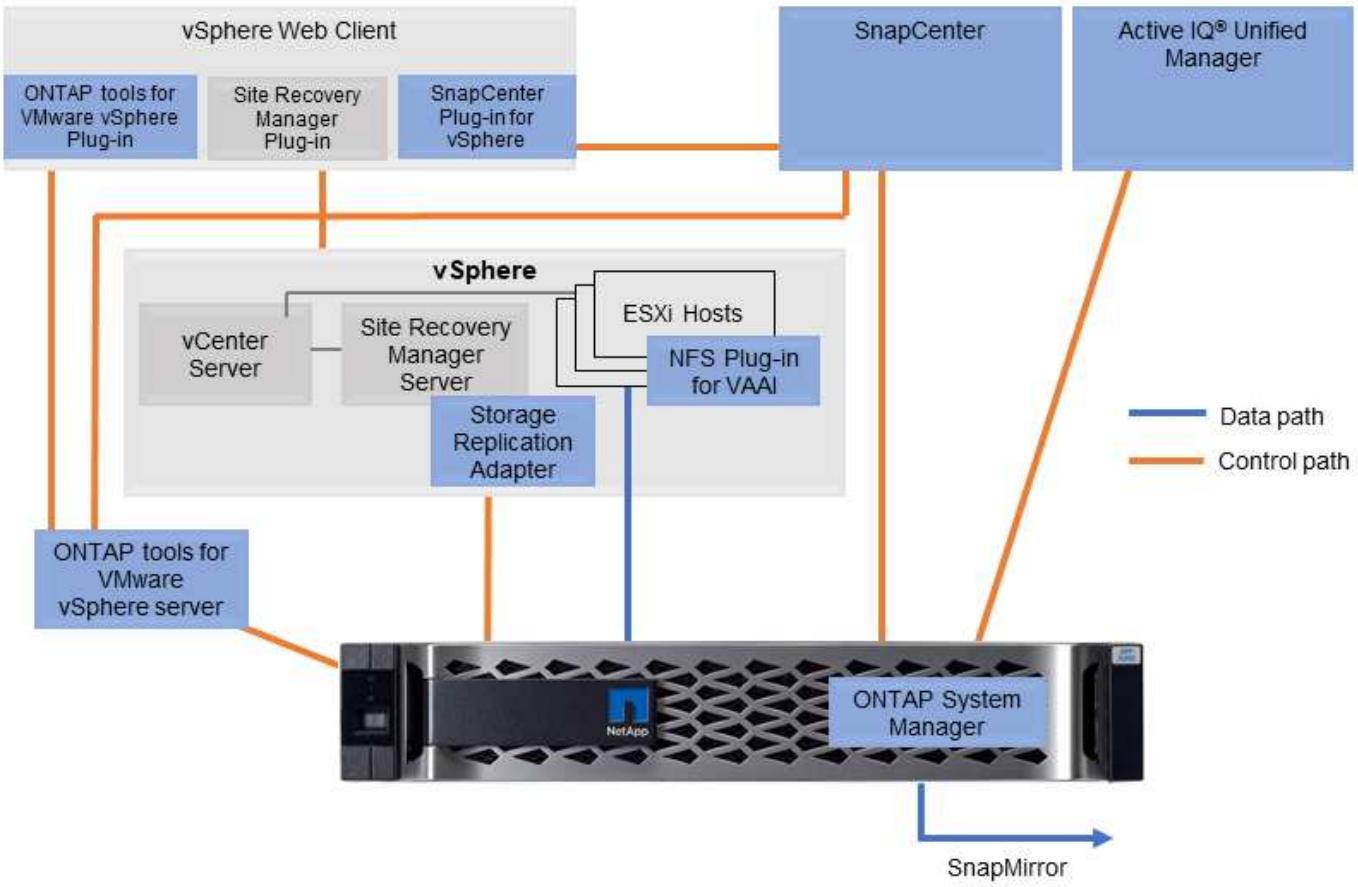
### VMware vSphere 用の ONTAP ツール

VMware vSphere 用の ONTAP ツールは、 vSphere とともに ONTAP ストレージを使用するための一連のツー

ルです。vCenter プラグインは、以前 Virtual Storage Console （ VSC ）と呼ばれていたもので、 SAN と NAS のどちらを使用している場合でも、ストレージ管理と効率化機能の簡易化、可用性の向上、ストレージコストと運用オーバーヘッドの削減を実現します。データストアのプロビジョニングのベストプラクティスを使用して、 NFS 環境およびブロックストレージ環境用の ESXi ホスト設定を最適化します。以上のメリットのために、ネットアップでは、 ONTAP ソフトウェアを実行しているシステムで vSphere を使用する際のベストプラクティスとして、これらの ONTAP ツールを使用することを推奨します。サーバアプライアンス、vCenter、VASA Provider、Storage Replication Adapterのユーザインターフェイス拡張機能が含まれています。ONTAP ツールのほぼすべてを、最新の自動化ツールで利用できるシンプルなREST APIを使用して自動化できます。

- * vCenter UIの拡張機能* ONTAP ツールのUI拡張機能は、vCenter UIにホストとストレージを管理するための使いやすいコンテキスト依存メニュー、情報ポートレット、およびネイティブアラート機能を直接組み込み、ワークフローを合理化することで、運用チームやvCenter管理者の業務を簡素化します。
- * VASA Provider for ONTAP 。* VASA Provider for ONTAP は、VMware vStorage APIs for Storage Awareness（VASA）フレームワークをサポートしています。VMware vSphere 用の ONTAP ツールの一部として提供され、導入を容易にする単一の仮想アプライアンスとして提供されます。VASA Provider では、 VM ストレージのプロビジョニングと監視に役立つように vCenter Server と ONTAP を接続します。VMware Virtual Volumes （ VVol ）のサポート、ストレージ機能プロファイルと個々の VM VVol のパフォーマンスの管理、およびプロファイルの容量と準拠状況の監視用アラームが可能になります。
- * Storage Replication Adapter. SRAは、VMware Site Recovery Manager（SRM）と併用して、本番サイトと災害復旧サイト間のデータ複製を管理し、DRレプリカを無停止でテストします。検出、リカバリ、再保護のタスクを自動化します。Windows SRM サーバおよび SRM アプライアンス用の SRA サーバアプライアンスと SRA アダプタの両方が含まれています。

次の図は、 vSphere 用の ONTAP ツールを示しています。



#### NFS Plug-in for VMware VAAI のこと

NetApp NFS Plug-in for VMware VAAIはESXiホスト向けのプラグインで、ONTAP 上のNFSデータストアでVAAI機能を使用できます。クローン処理、シック仮想ディスクファイルのスペースリザベーション、およびスナップショットオフロードのコピーオフロードをサポートします。コピー処理をストレージにオフロードしても、完了までの時間が必ずしも短縮されるとは限りませんが、ネットワーク帯域幅の要件が軽減され、CPUサイクル、バッファ、キューなどのホストリソースがオフロードされます。VMware vSphere用のONTAP ツールを使用して、ESXiホストまたはサポートされている場合はvSphere Lifecycle Manager（VLCM）にプラグインをインストールできます。

### Virtual Volumes （ VVol ）と Storage Policy Based Management （ SPBM ）

ネットアップは、 vSphere Virtual Volumes （ VVol ）の開発において VMware と初期の設計パートナーとして、アーキテクチャに関する情報提供と、 VVol および VMware vSphere APIs for Storage Awareness （ VASA ）のサポートを提供していました。このアプローチにより、VMのきめ細かなストレージ管理がVMFSで実現しただけでなく、Storage Policy Based Management（SPBM）によるストレージプロビジョニングの自動化もサポートされました。

SPBM は、仮想化環境で使用できるストレージサービスと、プロビジョニングされたストレージ要素の間の抽象化レイヤとして機能するフレームワークを、ポリシーを通じて提供します。このアプローチにより、ストレージアーキテクトは、 VM 管理者が簡単に利用できるさまざまな機能を備えたストレージプールを設計できます。仮想マシンのワークロード要件をプロビジョニングされたストレージプールと照合することで、仮想マシンごとまたは仮想ディスクレベルのさまざまな設定をきめ細かく制御できます。

ONTAP は VVol の規模においてストレージ業界をリードし、 1 つのクラスタで数十万もの VVol をサポートします。一方、エンタープライズアレイや小規模なフラッシュアレイベンダーは、アレイあたり数千の VVol をサポートします。また、 VVOL 3.0 をサポートする機能が追加され、 VM のきめ細かな管理が進化しています。

VMware vSphere Virtual Volumes 、 SPBM 、および ONTAP の詳細については、を参照してください "TR-4400 ：『 VMware vSphere Virtual Volumes with ONTAP 』"。

## データストアおよびプロトコル

#### vSphereデータストアとプロトコルの機能の概要

VMware vSphereとONTAP ソフトウェアを実行しているシステム上のデータストアの接続には、次の7つのプロトコルが使用されます。

- FCP
- FCoE
- NVMe/FC
- NVMe/FC
- iSCSI
- NFS v3
- NFS v4.1

FCP、FCoE、NVMe/FC、NVMe/FC、NVMe/FC、NVMe/FC、およびiSCSIはブロックプロトコルで、vSphere Virtual Machine File System（VMFS）を使用して、ONTAP FlexVol ボリュームに含まれるONTAP LUNまたはNVMeネームスペースにVMを格納します。vSphere 7.0 以降では、 VMware は本番環境でのソフトウェア FCoE をサポートしなくなりました。NFS はファイルプロトコルで、 VM をデータストア（ ONTAP ボリューム）に配置し、 VMFS を必要としません。SMB（CIFS）、iSCSI、NVMe/FC、NFSもゲストOSからONTAPに直接使用できます。

次の表に、vSphereがサポートするONTAPの従来のデータストア機能を示します。この情報はVVOLデータストアには該当しませんが、通常は、サポートされているONTAP リリースを使用する環境 vSphere 6.x以降のリリースで使用されます。を参照することもできます "VMwareコウセイノサイダイスウ" 個々の vSphere リリースに固有の制限を確認するため。

| 機能 / 特徴 | FC / FCoE | iSCSI | NVMe-oF | NFS |
|---|---|---|---|---|
| の形式で入力し | VMFS または raw デバイスマッピング（ RDM ） | VMFS または RDM | VMFS | 該当なし |
| データストアまたは LUN の最大数 | ホストあたり1、024個のLUN | サーバあたり1、024個のLUN | サーバごとに256名を指定します | 256マウント<br>デフォルトのNFS。MaxVolumes は 8 です。VMware vSphere 用の ONTAP ツールを使用して 256 まで増やす。 |
| データストアの最大サイズ | 64TB | 64TB | 64TB | 100TB 以上の FlexVol ボリュームと FlexGroup ボリューム |
| データストアの最大ファイルサイズ | 62TB | 62TB | 62TB | 62TB（ONTAP 9.12.1P2以降使用時） |
| LUN またはファイルシステムごとのキューの深さの最適値 | 64 ~ 256 | 64 ~ 256 | 自動ネゴシエーション | のNFS.MaxQueueDepthを参照してください "推奨される ESXi ホストとその他の ONTAP 設定"。 |

次の表に、サポートされる VMware ストレージ関連機能を示します。

| 容量 / 機能 | FC / FCoE | iSCSI | NVMe-oF | NFS |
|---|---|---|---|---|
| vMotion | はい。 | はい。 | はい。 | はい。 |
| Storage vMotion の機能です | はい。 | はい。 | はい。 | はい。 |
| VMware HA | はい。 | はい。 | はい。 | はい。 |
| ストレージ分散リソーススケジューラ（ SDRS ） | はい。 | はい。 | はい。 | はい。 |

| 容量 / 機能 | FC / FCoE | iSCSI | NVMe-oF | NFS |
|---|---|---|---|---|
| VMware vStorage APIs for Data Protection （ VADP ）対応のバックアップソフトウェア | はい。 | はい。 | はい。 | はい。 |
| VM 内の Microsoft Cluster Service （ MSCS ）またはフェイルオーバークラスタリング | はい。 | はい * | はい * | サポート対象外 |
| フォールトトレランス | はい。 | はい。 | はい。 | はい。 |
| Site Recovery Manager の略 | はい。 | はい。 | いいえ ** | v3のみ** |
| シンプロビジョニングされた VM （仮想ディスク） | はい。 | はい。 | はい。 | はい。<br>VAAIを使用しない場合、NFS上のすべてのVMに対してこの設定がデフォルトになります。 |
| VMware 標準マルチパス | はい。 | はい。 | はい、新しい高性能プラグイン（HPP）を使用して | NFS v4.1セッショントランキングにはONTAP 9.14.1以降が必要 |

次の表に、サポートされる ONTAP ストレージ管理機能を示します。

| 機能 / 特徴 | FC / FCoE | iSCSI | NVMe-oF | NFS |
|---|---|---|---|---|
| データ重複排除 | アレイ内での容量削減 | アレイ内での容量削減 | アレイ内での容量削減 | データストア内での容量削減 |
| シンプロビジョニング | データストアまたは RDM | データストアまたは RDM | データストア | データストア |
| データストアのサイズを変更 | 拡張のみ | 拡張のみ | 拡張のみ | 拡張、自動拡張、縮小 |
| Windows 、 Linux アプリケーション用の SnapCenter プラグイン（ゲスト内） | はい。 | はい。 | いいえ | はい。 |
| VMware vSphere 用の ONTAP ツールを使用した監視とホストの設定 | はい。 | はい。 | いいえ | はい。 |

| 機能 / 特徴 | FC / FCoE | iSCSI | NVMe-oF | NFS |
|---|---|---|---|---|
| VMware vSphere 用の ONTAP ツールを使用したプロビジョニング | はい。 | はい。 | いいえ | はい。 |

次の表に、サポートされるバックアップ機能を示します。

| 機能 / 特徴 | FC / FCoE | iSCSI | NVMe-oF | NFS |
|---|---|---|---|---|
| ONTAPスナップショット | はい。 | はい。 | はい。 | はい。 |
| 複製バックアップでサポートされるSRM | はい。 | はい。 | いいえ ** | v3のみ** |
| Volume SnapMirrorの略 | はい。 | はい。 | はい。 | はい。 |
| VMDK イメージアクセス | VADP 対応のバックアップソフトウェア | VADP 対応のバックアップソフトウェア | VADP 対応のバックアップソフトウェア | VADP 対応のバックアップソフトウェア、 vSphere Client 、 vSphere Web Client データストアブラウザ |
| VMDK のファイルレベルアクセス | VADP 対応のバックアップソフトウェア、 Windows のみ | VADP 対応のバックアップソフトウェア、 Windows のみ | VADP 対応のバックアップソフトウェア、 Windows のみ | VADP 対応のバックアップソフトウェアとサードパーティ製アプリケーション |
| NDMP の単位 | データストア | データストア | データストア | データストアまたはVM |

- VMFSデータストア内でマルチライター対応のVMDKを使用するのではなく、Microsoftクラスタにゲスト内iSCSIを使用することを推奨します。このアプローチは Microsoft と VMware によって完全にサポートされており、 ONTAP （オンプレミスまたはクラウドの ONTAP システムへの SnapMirror ）を使用した優れた柔軟性、設定と自動化が容易で、 SnapCenter で保護できます。vSphere 7 で、新しいクラスタ化された VMDK オプションが追加されました。これは、マルチライター対応のVMDKとは異なります。マルチライター対応のVMDKを使用するには、クラスタ化されたVMDKをサポートするFCプロトコルを介して提供されるデータストアが必要です。その他の制限が適用されます。VMwareの詳細 "Windows Server フェールオーバークラスタリングのセットアップ" 設定ガイドラインについては、ドキュメントを参照してください
    - NVMe-oFとNFS v4.1を使用するデータストアには、vSphereレプリケーションが必要です。アレイベースのレプリケーションはSRMではサポートされていません。

ストレージプロトコルを選択

ONTAP ソフトウェアを実行するシステムは、主要なストレージプロトコルをすべてサポートしているため、既存および計画されているネットワークインフラやスタッフのスキルに応じて、お客様は環境に最適なものを選択できます。ネットアップのテストでは、一般に、ほぼ同じ速度の回線で実行されているプロトコル間の違いはほとんど見られませんでした。そのため、物理プロトコルのパフォーマンスよりもネットワークインフラとスタッフの能力に重点を置くことを推奨します。

プロトコルの選択を検討する際には、次の要素が役立ちます。

- * 現在のお客様の環境。 * 一般に、 IT チームはイーサネット IP インフラの管理のスキルを持っていますが、すべてのチームが FC SAN ファブリックの管理のスキルを持っているわけではありません。ただし、ストレージトラフィック用に設計されていない汎用IPネットワークを使用すると、うまく機能しない場合があります。現在利用しているネットワークインフラストラクチャ、計画的な改善点、およびそれらを管理するためのスタッフのスキルと可用性を考慮します。
- * セットアップの容易さ * FC ファブリックの初期構成（追加のスイッチとケーブル配線、ゾーニング、 HBA とファームウェアの相互運用性の検証）に加えて、ブロックプロトコルを使用するには、 LUN の作成とマッピング、ゲスト OS による検出とフォーマットも必要です。作成およびエクスポートされた NFS ボリュームは、 ESXi ホストによってマウントされ、使用可能な状態になります。NFS では、ハードウェアの認定や管理に関する特別なファームウェアはありません。
- * 管理の容易さ。 * SAN プロトコルでは、より多くのスペースが必要な場合、 LUN の拡張、新しいサイズの検出のための再スキャン、ファイルシステムの拡張など、いくつかの手順が必要です。LUN の拡張は可能ですが、 LUN のサイズを縮小することはできず、未使用スペースのリカバリには追加の作業が必要になる場合があります。NFS を使用すると、簡単なサイジングが可能です。このサイズ変更は、ストレージシステムで自動化できます。SAN では、ゲスト OS のトリム / マッピング解除コマンドを使用してスペース再生が可能で、削除されたファイルのスペースをアレイに戻すことができます。NFS データストアでは、このようなスペース再生がより困難になります。
- * ストレージスペースの透過性。 * シンプロビジョニングによって削減効果が即座に現れるため、 NFS 環境では一般にストレージ利用率が見やすくなります。同様に、重複排除とクローニングによる削減効果は、同じデータストア内の他の VM や他のストレージシステムボリュームで即座に利用できます。一般に、 VM の密度は NFS データストア内でも高くなります。管理するデータストアが少ないため、重複排除による削減効果が向上すると同時に管理コストも削減されます。

### データストアのレイアウト

ONTAP ストレージシステムは、 VM および仮想ディスク用のデータストアを柔軟に作成できます。を使用する場合、 ONTAP の多くのベストプラクティスが適用されますが vSphere 用のデータストアをプロビジョニングする VSC （を参照） "推奨される ESXi ホストとその他の ONTAP 設定") 、考慮すべきその他のガイドラインを次に示します。

- ONTAP NFS データストアを使用して vSphere を導入することで、高性能でありながら管理が容易な実装を実現でき、ブロックベースのストレージプロトコルでは達成できない VM / データストア比率が提供されます。このアーキテクチャでは、データストア密度を 10 倍に増やすことも可能で、それに伴いデータストアの数は減少します。データストアのサイズを大きくするとストレージ効率が向上し、運用上のメリットが得られますが、ハードウェアリソースのパフォーマンスを最大限に引き出すためには、少なくとも 4 つのデータストア（ FlexVol ボリューム）を使用して 1 つの ONTAP コントローラに VM を格納することを検討してください。また、異なるリカバリポリシーを使用してデータストアを確立することもできます。ビジネスニーズに基づいて、他のバックアップや複製の頻度を高められるものもあります。FlexGroup ボリュームは設計上拡張できるため、複数のデータストアを使用する必要はありません。
- NetAppでは、ほとんどのNFSデータストアにFlexVolボリュームを使用することを推奨しています。ONTAP 9.8以降でFlexGroupは、データストアとしての使用もサポートされており、特定のユースケースでの使用が一般的に推奨されます。qtreeなどのその他のONTAPストレージコンテナは、現在ONTAP Tools for VMware vSphereまたはNetApp SnapCenter Plugin for VMware vSphereでサポートされていないため、一般に推奨されません。とはいえ、1つのボリューム内の複数のqtreeとしてデータストアを導入することは、データストアレベルのクォータやVMファイルクローンのメリットが得られる高度に自動化された環境に役立つ可能性があります。
- FlexVol ボリュームデータストアの適切なサイズは 4~8TB です。このサイズは、パフォーマンス、管理のしやすさ、データ保護のバランスが取れた適切なサイズです。小規模構成から開始して（ 4TB など）、必要に応じてデータストアを拡張します（最大 100TB まで）。小規模なデータストアは、バックアップ

や災害からのリカバリにかかる時間が短く、クラスタ間で迅速に移動できます。使用済みスペースの変化に応じてボリュームを自動的に拡張または縮小するには、 ONTAP のオートサイズを使用することを検討してください。VMware vSphere データストアプロビジョニングウィザードの ONTAP ツールでは、新しいデータストアに対してデフォルトでオートサイズが使用されます。拡張および縮小のしきい値と最大および最小サイズは、 System Manager またはコマンドラインを使用して追加でカスタマイズできます。

- または、 VMFS データストアを、 FC 、 iSCSI または FCoE でアクセスする LUN で構成することもできます。VMFS を使用すると、クラスタ内の各 ESX サーバから同時に従来型の LUN にアクセスすることができます。VMFS データストアは、最大 64TB まで拡張でき、最大 32 個の 2TB LUN （ VMFS 3 ）または単一の 64TB LUN （ VMFS 5 ）で構成できます。ONTAP の最大LUNサイズは、ほとんどのシステムで16TBで、オールSANアレイシステムでは128TBです。したがって、ほとんどの ONTAP システムでは、最大サイズの VMFS 5 データストアを、 4 つの 16TB LUN を使用して作成できます。複数のLUN（ハイエンドのFAS またはAFF システムを使用）を使用する高I/Oワークロードではパフォーマンス上のメリットを得られますが、データストアLUNの作成、管理、保護の複雑さが増し、可用性のリスクが増大することで、このメリットを相殺することができます。ネットアップでは、通常、各データストアに 1 つの大きな LUN を使用し、 16TB を超えるデータストアを追加する必要がある場合にのみスパンすることを推奨しています。NFS と同様に、複数のデータストア（ボリューム）を使用することで、 1 台の ONTAP コントローラのパフォーマンスを最大化することを検討してください。
- 古いゲストオペレーティングシステム（ OS ）では、パフォーマンスとストレージ効率を最大化するために、ストレージシステムとのアライメントが必要でした。しかし、 Microsoft や Linux ディストリビュータ（ Red Hat など）が提供する、ベンダーがサポートする最新の OS では、ファイルシステムのパーティションを仮想環境の基盤となるストレージシステムのブロックにアライメントするように調整する必要はありません。アライメントが必要な古い OS を使用している場合は、ネットアップサポートの技術情報で「 VM のアライメント」に関する記事を検索するか、ネットアップの営業担当者またはパートナー担当者に TR-3747 のコピーを請求してください。
- デフラグユーティリティはゲストOS内では使用しないでください。パフォーマンス上のメリットはなく、ストレージ効率とスナップショット容量の使用にも影響します。また、仮想デスクトップのゲスト OS で検索インデックスを無効にすることを検討してください。
- ONTAP は、革新的な Storage Efficiency 機能で業界をリードし、使用可能なディスクスペースを最大限に活用できるようにしています。AFF システムでは、デフォルトのインライン重複排除機能と圧縮機能により、この効率性がさらに向上しています。データはアグリゲート内のすべてのボリュームにわたって重複排除されるため、類似するオペレーティングシステムやアプリケーションを 1 つのデータストア内にまとめて、最大限の削減効果を得る必要はありません。
- 場合によっては、データストアが不要なこともあります。パフォーマンスと管理性を最大限に高めるためには、データベースや一部のアプリケーションなどの高 I/O アプリケーションにはデータストアを使用しないでください。代わりに、ゲストが管理する NFS や iSCSI ファイルシステムなど、ゲスト所有のファイルシステムや RDM を使用することを検討してください。アプリケーションに関する具体的なガイダンスについては、ご使用のアプリケーションに関するネットアップのテクニカルレポートを参照してください。例： "ONTAP を基盤にした Oracle データベース" 仮想化に関するセクションと役立つ詳細情報が記載されています。
- 第 1 クラスのディスク（または強化された仮想ディスク）を使用すると、 vSphere 6.5 以降を搭載した VM に関係なく、 vCenter で管理されるディスクを使用できます。主に API で管理されますが、 VVol では特に OpenStack ツールや Kubernetes ツールで管理する場合に便利です。ONTAP および VMware vSphere 用の ONTAP ツールでサポートされています。

### データストアと **VM** 移行

別のストレージシステム上の既存のデータストアから ONTAP に VM を移行する際は、いくつか注意しておくべきプラクティスがあります。

- Storage vMotion を使用して、仮想マシンの大部分を ONTAP に移動します。このアプローチでは、実行中の VM を停止する必要がなくなるだけでなく、インラインの重複排除や圧縮などの ONTAP の Storage

Efficiency 機能を使用して、移行時にデータを処理できます。vCenter 機能を使用してインベントリリストから複数の VM を選択し、適切なタイミングで移行をスケジュール（ Ctrl キーを押しながら [ アクション ] をクリック）することを検討します。

- 適切なデスティネーションデータストアへの移行を慎重に計画することもできますが、多くの場合、一括で移行して必要に応じてあとから整理する方が簡単です。Snapshotスケジュールの変更など、データ保護に関する特定のニーズがある場合は、このアプローチを使用して別のデータストアに移行できます。
- ほとんどの VM とそのストレージは、実行中（ホット）に移行できますが、 ISO 、 LUN 、 NFS ボリュームなどの接続されたストレージ（データストア内にない）を別のストレージシステムから移行する場合は、コールドマイグレーションが必要になることがあります。
- より慎重な移行が必要な仮想マシンには、接続されたストレージを使用するデータベースやアプリケーションなどがあります。一般的に、移行を管理するためにアプリケーションのツールを使用することを検討してください。Oracle の場合は、 RMAN や ASM などの Oracle ツールを使用してデータベース・ファイルを移行することを検討してください。を参照してください "TR-4534" を参照してください。同様に、 SQL Server の場合は、 SQL Server Management Studio を使用するか、 SnapManager for SQL Server や SnapCenter などのネットアップのツールを使用することを検討します。

#### VMware vSphere 用の ONTAP ツール

ONTAP ソフトウェアを実行しているシステムで vSphere を使用する際に最も重要なベストプラクティスは、 VMware vSphere プラグイン（旧 Virtual Storage Console ）用の ONTAP ツールをインストールして使用することです。この vCenter プラグインは、 SAN と NAS のどちらを使用している場合でも、ストレージ管理を簡易化し、可用性を向上させ、ストレージコストと運用オーバーヘッドを削減します。データストアのプロビジョニングのベストプラクティスを使用して、マルチパスと HBA タイムアウト（これらは付録 B で説明）用の ESXi ホスト設定を最適化します。vCenterプラグインであるため、vCenterサーバに接続するすべてのvSphere Web Clientで使用できます。

このプラグインは、 vSphere 環境で他の ONTAP ツールを使用する場合にも役立ちます。NFS Plug-in for VMware VAAIをインストールできます。これにより、VMのクローニング処理、シック仮想ディスクファイルのスペースリザベーション、ONTAPスナップショットのオフロードのために、ONTAPへのコピーオフロードが可能になります。

VASA Provider for ONTAP の多くの機能を使用するための管理インターフェイスでもあり、 VVol でのストレージポリシーベースの管理がサポートされています。VMware vSphere 用の ONTAP ツールを登録したら、ストレージ機能プロファイルを作成してストレージにマッピングし、データストアがプロファイルに一定期間にわたって準拠していることを確認します。VASA Provider には、 VVol データストアの作成と管理を行うためのインターフェイスも用意されています。

一般に、 vCenter 内で VMware vSphere インターフェイス用の ONTAP ツールを使用して、従来のデータストアと VVol データストアをプロビジョニングし、ベストプラクティスに従っていることを確認することを推奨します。

#### 一般的なネットワーク

ONTAP ソフトウェアを実行しているシステムで vSphere を使用する場合のネットワーク設定の構成は簡単で、他のネットワーク構成と同様です。考慮すべき点をいくつか挙げます。

- ストレージネットワークのトラフィックを他のネットワークから分離します。専用の VLAN を使用するか、ストレージ用に別個のスイッチを使用することで、別のネットワークを実現できます。ストレージネットワークがアップリンクなどの物理パスを共有している場合は、十分な帯域幅を確保するために QoS または追加のアップリンクポートが必要になることがあります。ホストをストレージに直接接続しないでください。スイッチを使用して冗長パスを確保し、VMware HAが介入なしで機能できるようにします。を参照してください "直接接続ネットワーク" 追加情報 の場合。

- ジャンボフレームは、必要に応じてネットワークでサポートされていれば、特に iSCSI を使用している場合に使用できます。使用する場合は、ストレージと ESXi ホストの間のパスにあるすべてのネットワークデバイスや VLAN で設定が同じであることを確認してください。そうしないと、パフォーマンスや接続の問題が発生する可能性があります。MTU は、 ESXi 仮想スイッチ、 VMkernel ポート、および各 ONTAP ノードの物理ポートまたはインターフェイスグループでも同一の設定にする必要があります。
- ネットワークフロー制御は、 ONTAP クラスタ内のクラスタネットワークポートでのみ無効にすることを推奨します。データトラフィックに使用される残りのネットワークポートについては、推奨されるベストプラクティスはありません。必要に応じて有効または無効にしてください。を参照してください "TR-4182" を参照してください。
- ESXi および ONTAP ストレージアレイをイーサネットストレージネットワークに接続するときは、接続先のイーサネットポートを Rapid Spanning Tree Protocol （ RSTP ；高速スパニングツリープロトコル）のエッジポートとして設定するか、 Cisco の PortFast 機能を使用して設定することを推奨します。ネットアップでは、 Cisco の PortFast 機能を使用していて、 ESXi サーバまたは ONTAP ストレージアレイへの 802.1Q VLAN トランキングが有効になっている環境では、 Spanning-Tree PortFast trunk 機能を有効にすることを推奨します。
- リンクアグリゲーションのベストプラクティスとして次を推奨します。
  - CiscoのVirtual PortChannel（vPC）などのマルチシャーシリンクアグリゲーショングループアプローチを使用して、2つの別 々 のスイッチシャーシ上のポートのリンクアグリゲーションをサポートするスイッチを使用します。
  - LACPが設定されたdvSwitches 5.1以降を使用していない場合、ESXiに接続されているスイッチポートのLACPを無効にします。
  - LACPを使用して、ポートハッシュまたはIPハッシュを使用したダイナミックマルチモードインターフェイスグループを使用するONTAPストレージシステムのリンクアグリゲートを作成します。を参照してください "Network Management の略" を参照してください。
  - ESXiで静的リンクアグリゲーション（EtherChannelなど）と標準vSwitchを使用する場合、またはvSphere Distributed Switchを使用するLACPベースのリンクアグリゲーションを使用する場合は、IPハッシュチーミングポリシーを使用します。リンクアグリゲーションを使用しない場合は、代わりに[Route based on the originating virtual port ID]を使用します。

次の表に、ネットワーク設定項目とその適用先をまとめます。

| 項目 | **ESXi** | スイッチ | ノード | **SVM** |
|---|---|---|---|---|
| IP アドレス | VMkernel | いいえ ** | いいえ ** | はい。 |
| リンクアグリゲーション | 仮想スイッチ | はい。 | はい。 | いいえ * |
| VLAN | VMkernel と VM ポートグループ | はい。 | はい。 | いいえ * |
| フロー制御 | NIC | はい。 | はい。 | いいえ * |
| スパニングツリー | いいえ | はい。 | いいえ | いいえ |
| MTU （ジャンボフレーム用） | 仮想スイッチと VMkernel ポート（ 9000 ） | ○（最大に設定） | ○（ 9000 ） | いいえ * |
| フェイルオーバーグループ | いいえ | いいえ | ○（作成） | ○（選択） |

- SVM LIFは、VLANやMTUなどが設定されたポート、インターフェイスグループ、またはVLANインターフェイスに接続します。ただし、設定の管理はSVMレベルではありません。
  - これらのデバイスには管理用に独自の IP アドレスがありますが、 ESXi ストレージネットワークのコンテキストでは使用されません。

### SAN （ FC 、 FCoE 、 NVMe/FC 、 iSCSI ）、 RDM

NetApp ONTAPは、iSCSI、ファイバチャネルプロトコル（FCP、またはFC）、NVMe over Fabrics（NVMe-oF）を使用して、VMware vSphereにエンタープライズクラスのブロックストレージを提供します。vSphereとONTAPを使用してVMストレージにブロックプロトコルを実装する場合のベストプラクティスを次に示します。

vSphere では、ブロックストレージ LUN を 3 通りの方法で使用します。

- VMFS データストアを使用する場合
- raw デバイスマッピング（ RDM ）で使用
- ソフトウェアイニシエータがアクセスおよび制御する LUN として使用 VM ゲスト OS から作成します

VMFS は、共有ストレージプールであるデータストアを提供する、高性能なクラスタファイルシステムです。VMFSデータストアは、FC、iSCSI、FCoEを使用してアクセスするLUN、またはNVMe/FCまたはNVMe/TCPプロトコルを使用してアクセスするNVMeネームスペースで構成できます。VMFSを使用すると、クラスタ内のすべてのESXサーバから同時にストレージにアクセスできます。ONTAP 9.12.1P2以降（およびASAシステムの以前のバージョン）では、一般に最大LUNサイズは128TBです。したがって、単一のLUNを使用して、64TBの最大サイズのVMFS 5または6データストアを作成できます。

vSphere は、ストレージデバイスへの複数のパスを標準でサポートします。この機能はネイティブマルチパス（ NMP ）と呼ばれます。NMP は、サポートされるストレージシステムのストレージタイプを検出し、使用中のストレージシステムの機能をサポートするように NMP スタックを自動的に設定できます。

NMPとONTAPはどちらも、Asymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）による最適パスと非最適パスのネゴシエートをサポートします。ONTAP では、アクセス対象の LUN をホストするノード上のターゲットポートを使用する直接データパスが、 ALUA の最適パスとなります。ALUA は、 vSphere と ONTAP の両方でデフォルトで有効になっています。NMPはONTAPクラスタをALUAとして認識し、ALUAストレージアレイタイププラグインを使用します。（`VMW_SATP_ALUA`）を入力し、ラウンドロビンパス選択プラグインを選択します。（`VMW_PSP_RR`）。

ESXi 6 は、最大 256 個の LUN と、 LUN への最大 1 、 024 個の合計パスをサポートします。これらの制限を超えるLUNやパスはESXiで認識されません。最大数の LUN を使用した場合、 LUN あたりのパス数は最大 4 つです。大規模な ONTAP クラスタでは、 LUN 数の上限に達する前にパス数の制限に達する可能性があります。この制限に対処するため、 ONTAP では、リリース 8.3 以降の選択的 LUN マップ（ SLM ）がサポートされています。

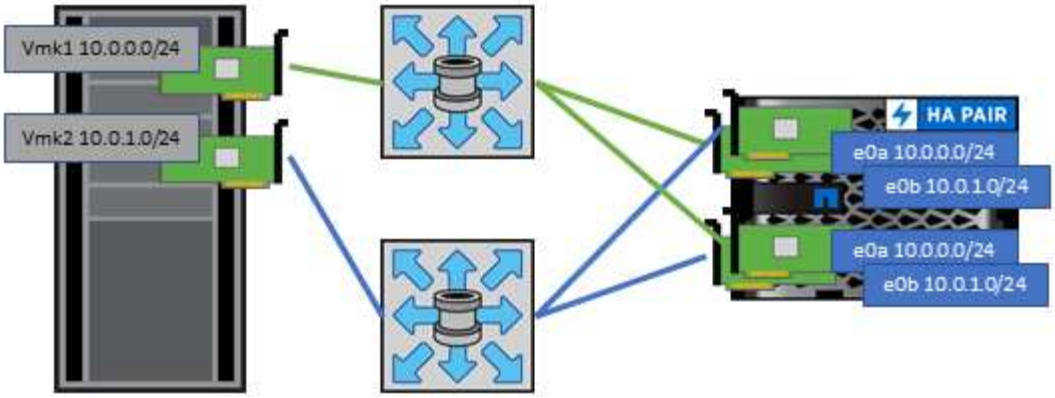
SLM は、特定の LUN へのパスをアドバタイズするノードを制限します。ネットアップのベストプラクティスでは、各 SVM のノードごとに少なくとも 1 つの LIF を配置し、 SLM を使用して、 LUN とその HA パートナーをホストするノードへのアドバタイズパスを制限することを推奨しています。他のパスは存在しますが、デフォルトではアドバタイズされません。SLM 内で、レポートノードの追加引数および削除引数を使用して通知されたパスを変更することができます。8.3 より前のリリースで作成された LUN ではすべてのパスがアドバタイズされるため、ホストしている HA ペアへのパスのみがアドバタイズされるように変更する必要があることに注意してください。SLM の詳細については、のセクション 5.9 を参照してください "TR-4080"。以前のポートセットの方式を使用すると、 LUN の使用可能なパスをさらに削減できます。ポートセットを使用すると、 igroup 内のイニシエータが LUN を認識する際に経由可能なパス数を減らすことができます。

- SLM はデフォルトでは有効になっています。ポートセットを使用しないかぎり、これ以上の設定は必要ありません。
- Data ONTAP 8.3より前のバージョンで作成したLUNの場合、次のコマンドを実行してSLMを手動で適用します。 `lun mapping remove-reporting-nodes` LUNレポートノードを削除し、LUNへのアクセスをLUNの所有者ノードとそのHAパートナーに制限するコマンド。

ブロックプロトコル（ iSCSI 、 FC 、 FCoE ）は、一意の名前に加え、 LUN ID とシリアル番号を使用して LUN にアクセスします。FC と FCoE は Worldwide Name （ WWNN および WWPN ）を使用し、 iSCSI は iSCSI Qualified Name （ IQN ）を使用します。ストレージ内での LUN へのパスはブロックプロトコルにとっては意味がないため、どこにも表示されません。したがって、 LUN のみが含まれるボリュームは内部でマウントする必要がなく、データストアで使用される LUN を含むボリュームのジャンクションパスも必要ありません。ONTAP の NVMe サブシステムも同様に機能します。

考慮すべきその他のベストプラクティス：

- 可用性と移動性を最大限に高めるために、 ONTAP クラスタ内の各ノード上の各 SVM に論理インターフェイス（ LIF ）が作成されていることを確認します。ONTAP SAN では、各ファブリックに対して 1 つずつ、ノードごとに 2 つの物理ポートと LIF を使用することを推奨します。ALUA を使用してパスが解析され、アクティブな最適化（直接）パスとアクティブな非最適化パスが特定されます。ALUA は FC 、 FCoE 、および iSCSI に使用されます。
- iSCSI ネットワークの場合、複数の仮想スイッチがある場合は、 NIC チーミングを使用して、異なるネットワークサブネット上の複数の VMkernel ネットワークインターフェイスを使用します。また、複数の物理スイッチに接続された複数の物理 NIC を使用して、 HA を実現し、スループットを向上させることもできます。次の図に、マルチパス接続の例を示します。ONTAP では、 2 つ以上のスイッチに接続された 2 つ以上のリンクでフェイルオーバーするシングルモードインターフェイスグループを設定するか、 LACP または他のリンクアグリゲーションテクノロジをマルチモードインターフェイスグループと併用して HA を実現し、リンクアグリゲーションのメリットを活かすことができます。
- ESXiでターゲット認証にチャレンジハンドシェイク認証プロトコル（CHAP）が使用されている場合は、CLIを使用してONTAPでもCHAPを設定する必要があります。（`vserver iscsi security create`）またはSystem Managerで（[ストレージ]>[SVM]>[SVM設定]>[プロトコル]>[iSCSI]で[イニシエータセキュリティ]を編集します）。
- LUN と igroup の作成と管理には、 VMware vSphere の ONTAP ツールを使用します。プラグインによってサーバの WWPN が自動的に判別され、適切な igroup が作成されます。また、ベストプラクティスに従って LUN を設定し、正しい igroup にマッピングします。
- RDMは管理が困難になる可能性があるため、使用には注意が必要です。また、前述したように制限されているパスも使用します。ONTAP LUN は両方をサポートします "物理互換モードと仮想互換モード" RDM ：
- vSphere 7.0 での NVMe/FC の使用については、以下を参照してください "ONTAP NVMe/FC Host Configuration Guide" および "TR-4684"次の図に、 vSphere ホストから ONTAP LUN へのマルチパス接続を示します。




**NFS**

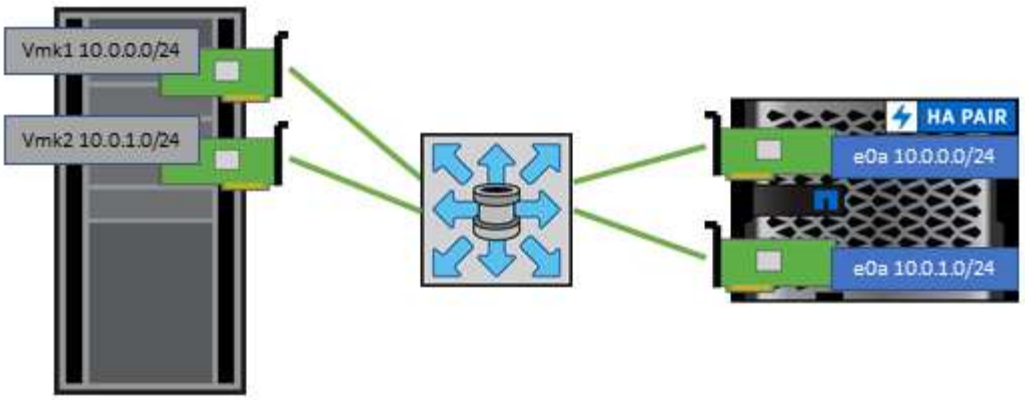
NetApp ONTAPは、とりわけエンタープライズクラスのスケールアウトNASアレイです。ONTAPは、VMware vSphereを強化し、多数のESXiホストからNFS接続データストアに同時にアクセスできるようにします。VMFSファイルシステムの制限をはるかに超えています。vSphereでNFSを使用すると、使いやすさとストレージ効率の可視化のメリットが得られます。詳細については、 "データストア" セクション。

vSphere で ONTAP NFS を使用する際に推奨されるベストプラクティスは次のとおりです。

- ONTAP クラスタ内の各ノードの各 SVM で、 1 つの論理インターフェイス（ LIF ）を使用します。データストアごとの LIF の過去の推奨事項は不要になりました。直接アクセス（同じノード上のLIFとデータストア）を推奨しますが、一般にパフォーマンスへの影響は最小限（マイクロ秒）であるため、間接アクセスについて心配する必要はありません。
- VMware は、 VMware Infrastructure 3 以降で NFSv3 をサポートしています。vSphere 6.0 では NFSv4.1 がサポートされるようになり、 Kerberos セキュリティなどの高度な機能が使用できるようになりました。NFSv3 ではクライアント側のロックが使用され、 NFSv4.1 ではサーバ側のロックが使用されます。ONTAP ボリュームは両方のプロトコルでエクスポートできますが、 ESXi は 1 つのプロトコルでしかマウントできません。この単一プロトコルのマウントにより、他の ESXi ホストが同じデータストアを別のバージョンでマウントすることができるわけではありません。すべてのホストが同じバージョン、つまり同じロック形式を使用するように、マウント時に使用するプロトコルバージョンを指定してください。NFS のバージョンをホスト間で混在させないでください。可能であれば、ホストプロファイルを使用して準拠しているかどうかを確認します
  - NFSv3 と NFSv4.1 間ではデータストアが自動変換されないため、新しい NFSv4.1 データストアを作成し、 Storage vMotion を使用して新しいデータストアに VM を移行します。
  - に記載されている NFS v4.1 と相互運用性に関する表の注を参照してください "NetApp Interoperability Matrix Tool で確認できます" をサポートするには、特定の ESXi パッチレベルが必要です。
  - vSphere 8.0U2以降では、VMwareでNFSv3でのnconnectがサポートされます。nconnectの詳細については、 "NetAppおよびVMwareでのNFSv3 nconnect機能"
- NFS エクスポートポリシーは、 vSphere ホストによるアクセスの制御に使用されます。複数のボリューム（データストア）で 1 つのポリシーを使用できます。NFSv3 では、 ESXi で sys （ UNIX ）セキュリティ形式が使用され、 VM を実行するためにルートマウントオプションが必要となります。ONTAP では、このオプションはスーパーユーザと呼ばれます。スーパーユーザオプションを使用する場合は、匿名ユーザ ID を指定する必要はありません。の値が異なるエクスポートポリシールールに注意してください `-anon` および `-allow-suid` 原因 SVM検出がONTAP ツールで問題を検出できるかどうか。ポリシーの例を次に示します。

- Access Protocol：nfs（nfs3とnfs4の両方を含む）
- クライアント一致仕様： 192.168.42.21
- RO アクセスルール： sys
- RWアクセスルール:sys
- 匿名UIDの形式です
- superuser ： sys

- NetApp NFS Plug-in for VMware VAAIを使用する場合は、プロトコルをに設定する必要があります。 `nfs` ではなく `nfs3` エクスポートポリシールールが作成または変更されたとき。VAAIコピーオフロード機能を使用するには、データプロトコルがNFSv3であっても、NFSv4プロトコルが機能する必要があります。フロトコルノシテイ `nfs` NFSv3とNFSv4の両方のバージョンが含まれます。
- NFS データストアのボリュームは SVM のルートボリュームからジャンクションされるため、 ESXi がデータストアボリュームに移動してマウントするためにはルートボリュームへのアクセス権も必要となります。ルートボリューム、およびデータストアボリュームのジャンクションがネストされているその他のボリュームのエクスポートポリシーには、ESXiサーバに読み取り専用アクセスを許可するルールが含まれている必要があります。VAAIプラグインを使用したルートボリュームのポリシーの例を次に示します。
  - Access Protocol：nfs（nfs3とnfs4の両方を含む）
  - クライアント一致仕様： 192.168.42.21
  - RO アクセスルール： sys
  - RW Access Rule：never（ルートボリュームに最適なセキュリティ）
  - 匿名UIDの形式です
  - superuser：sys（VAAIを使用するルートボリュームの場合も必要）
- VMware vSphere 用の ONTAP ツール（最も重要なベストプラクティス）を使用：
  - VMware vSphere 用の ONTAP ツールを使用してデータストアをプロビジョニングすると、エクスポートポリシーの自動管理が簡易化されます。
  - プラグインを使用してVMwareクラスタ用のデータストアを作成するときは、単一のESXサーバではなくクラスタを選択します。これにより、データストアがクラスタ内のすべてのホストに自動的にマウントされます。
  - プラグインのマウント機能を使用して、既存のデータストアを新しいサーバに適用します。
  - VMware vSphere 用の ONTAP ツールを使用しない場合は、すべてのサーバ、または追加のアクセス制御が必要なサーバクラスタごとに、 1 つのエクスポートポリシーを使用します。
- ONTAP にはフレキシブルボリュームのネームスペース構造が用意されており、ジャンクションを使用してボリュームをツリーにまとめることができますが、このアプローチは vSphere には価値がありません。ストレージのネームスペース階層に関係なく、データストアのルートに各 VM 用のディレクトリが作成されます。そのため、単に SVM のルートボリュームに vSphere のボリュームのジャンクションパスをマウントすることがベストプラクティスです。これは、 VMware vSphere 用の ONTAP ツールでデータストアをプロビジョニングする方法です。ジャンクションパスがネストされていないと、ルートボリューム以外のボリュームに依存しているボリュームがないこと、またボリュームをオフラインにするか破棄するかによって意図的に他のボリュームへのパスに影響が及ぶこともありません。
- NFS データストアの NTFS パーティションのブロックサイズは 4K で十分です。次の図は、 vSphere ホストから ONTAP NFS データストアへの接続を示しています。




次の表に、 NFS のバージョンとサポートされる機能を示します。

| **vSphere** の機能 | **NFSv3** | **NFSv4.1** |
|---|---|---|
| vMotion と Storage vMotion | はい。 | はい。 |
| 高可用性 | はい。 | はい。 |
| フォールトトレランス | はい。 | はい。 |
| DRS | はい。 | はい。 |
| ホストプロファイル | はい。 | はい。 |
| Storage DRS | はい。 | いいえ |
| ストレージ I/O の制御 | はい。 | いいえ |
| SRM の場合 | はい。 | いいえ |
| 仮想ボリューム | はい。 | いいえ |
| ハードウェアアクセラレーション（ VAAI ） | はい。 | はい。 |
| Kerberos 認証 | いいえ | ○（ vSphere 6.5 以降で拡張して、 AES 、 krb5i ） |
| マルチパスのサポート | いいえ | はい。 |

**FlexGroup** ボリューム

## VMware vSphereでONTAPボリュームとFlexGroupボリュームを使用すれば、ONTAPクラスタ全体の能力を最大限に活用できるシンプルで拡張性に優れたデータストアを構築できます。

ONTAP 9.8、ONTAP Tools for VMware vSphere 9.8、SnapCenterプラグインfor VMware 4.4リリースに加えて、vSphereでのFlexGroupボリュームベースデータストアのサポートが追加されました。FlexGroupボリュームは大規模なデータストアの作成を簡易化し、必要な分散コンスティチュエントボリュームをONTAPクラスタ全体に自動的に作成して、ONTAPシステムのパフォーマンスを最大限に引き出します。

FlexGroupボリュームに関する詳細情報 "『FlexCache and FlexGroup Volume Technical Report』を参照してください"。

ONTAPクラスタ全体の機能を備えた拡張性に優れた単一のvSphereデータストアが必要な場合や、非常に大規模なクローニングワークロードがあり、新しいFlexGroupクローニングメカニズムのメリットがある場合は、vSphereでFlexGroupボリュームを使用します。

コピーオフロード

ONTAP 9.8では、vSphereワークロードを使用した広範なシステムテストに加えて、FlexGroupデータストア用の新しいコピーオフロードメカニズムが追加されました。この新しいシステムでは、強化されたコピーエンジンを使用して、ソースとデスティネーションの両方へのアクセスを許可しながら、バックグラウンドでコンスティチュエント間でファイルをレプリケートします。このローカルキャッシュを使用して、VMクローンをオンデマンドで迅速にインスタンス化します。

FlexGroup最適化コピーオフロードを有効にする方法については、を参照してください。 "VAAIコピーオフロードを許可するようにONTAP FlexGroupを設定する方法"

VAAIクローニングを使用していても、キャッシュをウォームアップするのに十分なクローンを作成しないと、ホストベースのコピーよりも高速ではない場合があります。その場合は、必要に応じてキャッシュタイムアウトを調整できます。

次のシナリオを考えてみましょう。

- 8つのコンスティチュエントで新しいFlexGroupを作成しました
- 新しいFlexGroupのキャッシュタイムアウトが160分に設定されている

このシナリオでは、ローカルファイルクローンではなく、最初に完了する8つのクローンがフルコピーになります。160秒のタイムアウトが経過する前にそのVMをクローニングすると、各コンスティチュエント内のファイルクローンエンジンがラウンドロビン方式で使用され、コンスティチュエントボリューム間でほぼ瞬時に均等に分散されたコピーが作成されます。

ボリュームが新しいクローンジョブを受信するたびに、タイムアウトがリセットされます。この例のFlexGroup内のコンスティチュエントボリュームがタイムアウトまでにクローン要求を受信しなかった場合、そのVMのキャッシュはクリアされ、ボリュームに再度データを入力する必要があります。また、元のクローンのソースが変更された場合（テンプレートを更新した場合など）、競合を防ぐために各構成要素のローカルキャッシュが無効になります。前述したように、キャッシュは調整可能であり、環境のニーズに合わせて設定できます。

VAAIでFlexGroupを使用する方法の詳細については、次の技術情報アーティクルを参照してください。 "VAAI：FlexGroupボリュームでのキャッシュの仕組みを教えてください。"

FlexGroupキャッシュを十分に活用できないものの、ボリューム間での高速クローニングが必要な環境では、VVOLの使用を検討してください。VVolを使用したボリューム間クローニングは、従来のデータストアよりもはるかに高速で、キャッシュに依存しません。

**QoS**セツテイ

ONTAP System Managerまたはクラスタシェルを使用してFlexGroupレベルでQoSを設定することはサポートされていますが、VMに対応したりvCenterと統合したりすることはできません。

QoS（最大/最小IOPS）は、vCenter UIまたはREST APIを使用して、個 々 のVMまたはデータストア内のすべてのVMに対して設定できますONTAP。すべての VM に QoS を設定すると、 VM ごとに個別に設定する必要がなくなります。今後は、新規または移行された VM には適用されません。新しい VM に QoS を設定するか、データストア内のすべての VM に QoS を再適用してください。

VMware vSphereでは、NFSデータストアのすべてのIOがホストごとに単一のキューとして扱われるため、1つのVMでのQoS調整が、同じデータストア内の他のVMのパフォーマンスに影響する可能性があることに注意してください。これに対し、VVOLでは、別のデータストアに移行してもQoSポリシーの設定を維持でき、調整しても他のVMのIOに影響しません。

### 指標

また、ONTAP 9.8では、FlexGroupファイル用のファイルベースのパフォーマンス指標（IOPS、スループット、レイテンシ）が新たに追加され、これらの指標はONTAP tools for VMware vSphereのダッシュボードとVMレポートで確認できるようになりました。VMware vSphere プラグイン用の ONTAP ツールでは、最大 IOPS と最小 IOPS の組み合わせを使用してサービス品質（ QoS ）ルールを設定することもできます。これらは、データストア内のすべての VM に対して個別に設定することも、特定の VM に対して個別に設定することもできます。

### ベストプラクティス

- ONTAPツールを使用してFlexGroupデータストアを作成すると、FlexGroupが最適に作成され、vSphere環境に合わせてエクスポートポリシーが設定されます。ただし、ONTAP toolsを使用してFlexGroupボリュームを作成すると、vSphereクラスタ内のすべてのノードが1つのIPアドレスを使用してデータストアをマウントすることがわかります。その結果、ネットワークポートがボトルネックになる可能性があります。この問題を回避するには、データストアをアンマウントし、SVM上のLIF間でロードバランシングを行うラウンドロビンDNS名を使用して標準のvSphereデータストアウィザードを使用して再マウントします。再マウントが完了すると、ONTAP toolsは再びデータストアを管理できるようになります。ONTAP toolsを使用できない場合は、FlexGroupのデフォルト値を使用し、のガイドラインに従ってエクスポートポリシーを作成します。 "データストアとプロトコル- NFS"。
- FlexGroup データストアのサイジングを行う場合、 FlexVol は、より大容量のネームスペースを作成する複数の小さい FlexGroup で構成されることに注意してください。そのため、データストアのサイズは、最大のVMDKファイルのサイズの8倍以上（デフォルトのコンスティチュエントが8つの場合）、さらに10~20%の未使用のヘッドルームを使用して、リバランシングを柔軟に実行できるようにします。たとえば、環境に6TBのVMDKがある場合は、FlexGroupデータストアのサイズを52.8TB（6x8+10%）以上に設定します。
- ONTAP 9.14.1以降では、VMwareとNetAppでNFSv4.1セッショントランキングがサポートされます。特定のバージョンの詳細については、NetApp NFS 4.1のInteroperability Matrixの注意事項を参照してください。NFSv3では、ボリュームへの複数の物理パスはサポートされませんが、vSphere 8.0U2以降ではnconnectがサポートされます。nconnectの詳細については、 "NetAppおよびVMwareでのNFSv3 nconnect機能"。
- コピーオフロードには、 NFS Plug-in for VMware VAAI を使用します。前述したように、クローニングはFlexGroupデータストア内で強化されますが、FlexVolボリュームとFlexGroupボリュームの間でVMをコピーする場合、ONTAPはESXiホストのコピーに比べてパフォーマンス上の大きなメリットはありません。そのため、VAAIとFlexGroupのどちらを使用するかを決定する際は、ワークロードのクローニングを検討してください。コンスティチュエントボリュームの数の変更は、FlexGroupベースのクローニングを最適化する1つの方法です。前述のキャッシュタイムアウトの調整と同様に、
- ONTAP tools for VMware vSphere 9.8以降を使用して、ONTAP指標（ダッシュボードとVMレポート）を使用してFlexGroup VMのパフォーマンスを監視し、個 々 のVMのQoSを管理します。現時点では、これらの指標は ONTAP コマンドや API では使用できません。
- SnapCenter Plug-in for VMware vSphereリリース4.4以降では、プライマリストレージシステム上のFlexGroupデータストアのVMのバックアップとリカバリがサポートされます。SCV 4.6では、FlexGroupベースのデータストアに対するSnapMirrorのサポートが追加されています。アレイベースのスナップショットとレプリケーションを使用することは、データを保護する最も効率的な方法です。

## ネットワーク構成：

### ONTAP ソフトウェアを実行しているシステムで vSphere を使用する場合のネットワーク設定の構成は簡単で、他のネットワーク構成と同様です。

考慮すべき点をいくつか挙げます。

- ストレージネットワークのトラフィックを他のネットワークから分離します。専用の VLAN を使用するか、ストレージ用に別個のスイッチを使用することで、別のネットワークを実現できます。ストレージネットワークがアップリンクなどの物理パスを共有している場合は、十分な帯域幅を確保するために QoS または追加のアップリンクポートが必要になることがあります。ホストをストレージに直接接続しないでください。スイッチを使用して冗長パスを確保し、VMware HAが介入なしで機能できるようにします。を参照してください "直接接続ネットワーク" 追加情報 の場合。
- ジャンボフレームは、必要に応じてネットワークでサポートされていれば、特に iSCSI を使用している場合に使用できます。使用する場合は、ストレージと ESXi ホストの間のパスにあるすべてのネットワークデバイスや VLAN で設定が同じであることを確認してください。そうしないと、パフォーマンスや接続の問題が発生する可能性があります。MTU は、 ESXi 仮想スイッチ、 VMkernel ポート、および各 ONTAP ノードの物理ポートまたはインターフェイスグループでも同一の設定にする必要があります。
- ネットワークフロー制御は、 ONTAP クラスタ内のクラスタネットワークポートでのみ無効にすることを推奨します。データトラフィックに使用される残りのネットワークポートについては、推奨されるベストプラクティスはありません。必要に応じて有効または無効にする必要があります。を参照してください "TR-4182" を参照してください。
- ESXi および ONTAP ストレージアレイをイーサネットストレージネットワークに接続するときは、接続先のイーサネットポートを Rapid Spanning Tree Protocol （ RSTP ；高速スパニングツリープロトコル）のエッジポートとして設定するか、 Cisco の PortFast 機能を使用して設定することを推奨します。ネットアップでは、 Cisco の PortFast 機能を使用していて、 ESXi サーバまたは ONTAP ストレージアレイへの 802.1Q VLAN トランキングが有効になっている環境では、 Spanning-Tree PortFast trunk 機能を有効にすることを推奨します。
- リンクアグリゲーションのベストプラクティスとして次を推奨します。
  - CiscoのVirtual PortChannel（vPC）などのマルチシャーシリンクアグリゲーショングループアプローチを使用して、2つの別 々 のスイッチシャーシ上のポートのリンクアグリゲーションをサポートするスイッチを使用します。
  - LACPが設定されたdvSwitches 5.1以降を使用していない場合、ESXiに接続されているスイッチポートのLACPを無効にします。
  - LACPを使用して、IPハッシュを持つダイナミックマルチモードインターフェイスグループを持つONTAP ストレージシステムのリンクアグリゲートを作成します。
  - ESXiでIPハッシュチーミングポリシーを使用します。

次の表に、ネットワーク設定項目とその適用先をまとめます。

| 項目 | **ESXi** | スイッチ | ノード | **SVM** |
|---|---|---|---|---|
| IP アドレス | VMkernel | いいえ ** | いいえ ** | はい。 |
| リンクアグリゲーション | 仮想スイッチ | はい。 | はい。 | いいえ * |
| VLAN | VMkernel と VM ポートグループ | はい。 | はい。 | いいえ * |

| 項目 | **ESXi** | スイッチ | ノード | **SVM** |
|---|---|---|---|---|
| フロー制御 | NIC | はい。 | はい。 | いいえ * |
| スパニングツリー | いいえ | はい。 | いいえ | いいえ |
| MTU （ジャンボフレーム用） | 仮想スイッチと VMkernel ポート（ 9000 ） | ○（最大に設定） | ○（ 9000 ） | いいえ * |
| フェイルオーバーグループ | いいえ | いいえ | ○（作成） | ○（選択） |

- SVM LIFは、VLANやMTUなどが設定されたポート、インターフェイスグループ、またはVLANインターフェイスに接続します。ただし、設定の管理はSVMレベルではありません。
  - これらのデバイスには管理用に独自の IP アドレスがありますが、 ESXi ストレージネットワークのコンテキストでは使用されません。

**SAN （ FC 、 FCoE 、 NVMe/FC 、 iSCSI ）、 RDM**

vSphere では、ブロックストレージ LUN を 3 通りの方法で使用します。

- VMFS データストアを使用する場合
- raw デバイスマッピング（ RDM ）で使用
- ソフトウェアイニシエータがアクセスおよび制御する LUN として使用 VM ゲスト OS から作成します

VMFS は、共有ストレージプールであるデータストアを提供する、高性能なクラスタファイルシステムです。VMFS データストアは、 NVMe/FC プロトコルによってアクセスされる FC 、 iSCSI 、 FCoE 、または NVMe ネームスペースを使用してアクセスする LUN で構成できます。VMFS を使用すると、クラスタ内の各 ESX サーバから同時に従来型の LUN にアクセスすることができます。ONTAP の最大 LUN サイズは通常 16TB であるため、最大サイズの 64TB （このセクションの最初の表を参照）の VMFS 5 データストアは、 4 つの 16TB LUN を使用して作成されます（すべての SAN アレイシステムが最大 VMFS LUN サイズ 64TB をサポート）。ONTAP LUN アーキテクチャでは個々のキュー深度が小さくないため、 ONTAP の VMFS データストアは、比較的簡単な方法で従来のアレイアーキテクチャよりも大規模に拡張できます。

vSphere は、ストレージデバイスへの複数のパスを標準でサポートします。この機能はネイティブマルチパス（ NMP ）と呼ばれます。NMP は、サポートされるストレージシステムのストレージタイプを検出し、使用中のストレージシステムの機能をサポートするように NMP スタックを自動的に設定できます。

NMPとONTAPはどちらも、Asymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）による最適パスと非最適パスのネゴシエートをサポートします。ONTAP では、アクセス対象の LUN をホストするノード上のターゲットポートを使用する直接データパスが、 ALUA の最適パスとなります。ALUA は、 vSphere と ONTAP の両方でデフォルトで有効になっています。NMPはONTAPクラスタをALUAとして認識し、ALUAストレージアレイタイププラグインを使用します。（`VMW_SATP_ALUA`）を入力し、ラウンドロビンパス選択プラグインを選択します。（`VMW_PSP_RR`）。

ESXi 6 は、最大 256 個の LUN と、 LUN への最大 1 、 024 個の合計パスをサポートします。これらの制限を超える LUN やパスは、 ESXi で認識されません。最大数の LUN を使用した場合、 LUN あたりのパス数は最大 4 つです。大規模な ONTAP クラスタでは、 LUN 数の上限に達する前にパス数の制限に達する可能性があります。この制限に対処するため、 ONTAP では、リリース 8.3 以降の選択的 LUN マップ（ SLM ）がサポートされています。

SLM は、特定の LUN へのパスをアドバタイズするノードを制限します。ネットアップのベストプラクティス

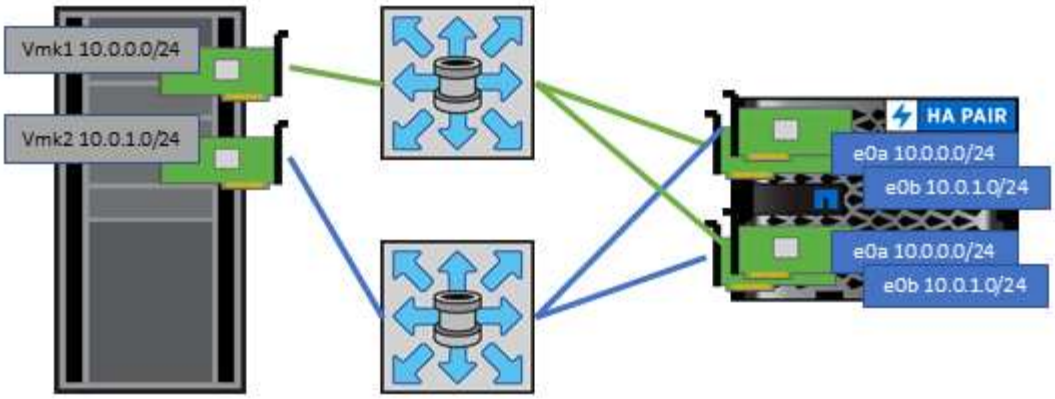
では、各 SVM のノードごとに少なくとも 1 つの LIF を配置し、 SLM を使用して、 LUN とその HA パートナーをホストするノードへのアドバタイズパスを制限することを推奨しています。他のパスは存在しますが、デフォルトではアドバタイズされません。SLM 内で、レポートノードの追加引数および削除引数を使用して通知されたパスを変更することができます。8.3より前のリリースで作成されたLUNではすべてのパスがアドバタイズされるため、ホストしているHAペアへのパスのみがアドバタイズされるように変更する必要があります。SLM の詳細については、のセクション 5.9 を参照してください "TR-4080"。以前のポートセットの方式を使用すると、 LUN の使用可能なパスをさらに削減できます。ポートセットを使用すると、 igroup 内のイニシエータが LUN を認識する際に経由可能なパス数を減らすことができます。

- SLM はデフォルトでは有効になっています。ポートセットを使用しないかぎり、これ以上の設定は必要ありません。
- Data ONTAP 8.3より前のバージョンで作成したLUNの場合、 `lun mapping remove-reporting-nodes` LUNレポートノードを削除し、LUNへのアクセスをLUNの所有者ノードとそのHAパートナーに制限するコマンド。

ブロックプロトコル（ iSCSI 、 FC 、 FCoE ）は、一意の名前に加え、 LUN ID とシリアル番号を使用して LUN にアクセスします。FC と FCoE は Worldwide Name （ WWNN および WWPN ）を使用し、 iSCSI は iSCSI Qualified Name （ IQN ）を使用します。ストレージ内での LUN へのパスはブロックプロトコルにとっては意味がないため、どこにも表示されません。したがって、 LUN のみが含まれるボリュームは内部でマウントする必要がなく、データストアで使用される LUN を含むボリュームのジャンクションパスも必要ありません。ONTAP の NVMe サブシステムも同様に機能します。

考慮すべきその他のベストプラクティス：

- 可用性と移動性を最大限に高めるために、 ONTAP クラスタ内の各ノード上の各 SVM に論理インターフェイス（ LIF ）が作成されていることを確認します。ONTAP SAN では、各ファブリックに対して 1 つずつ、ノードごとに 2 つの物理ポートと LIF を使用することを推奨します。ALUA を使用してパスが解析され、アクティブな最適化（直接）パスとアクティブな非最適化パスが特定されます。ALUA は FC 、 FCoE 、および iSCSI に使用されます。
- iSCSI ネットワークの場合、複数の仮想スイッチがある場合は、 NIC チーミングを使用して、異なるネットワークサブネット上の複数の VMkernel ネットワークインターフェイスを使用します。また、複数の物理スイッチに接続された複数の物理 NIC を使用して、 HA を実現し、スループットを向上させることもできます。次の図に、マルチパス接続の例を示します。ONTAPでは、高可用性とリンクアグリゲーションを実現するために、異なるスイッチへの複数のリンクを含むシングルモードインターフェイスグループを使用するか、マルチモードインターフェイスグループを使用したLACPを使用します。
- ESXiでターゲット認証にチャレンジハンドシェイク認証プロトコル（CHAP）が使用されている場合は、CLIを使用してONTAPでもCHAPを設定する必要があります。 (`vserver iscsi security create`）またはSystem Managerで（[ストレージ]>[SVM]>[SVM設定]>[プロトコル]>[iSCSI]で[イニシエータセキュリティ]を編集します）。
- LUN と igroup の作成と管理には、 VMware vSphere の ONTAP ツールを使用します。プラグインによってサーバの WWPN が自動的に判別され、適切な igroup が作成されます。また、ベストプラクティスに従って LUN を設定し、正しい igroup にマッピングします。
- RDMは管理が困難になる可能性があるため、使用には注意が必要です。また、前述したように制限されているパスも使用します。ONTAP LUN は両方をサポートします "物理互換モードと仮想互換モード" RDM ：
- vSphere 7.0 での NVMe/FC の使用については、以下を参照してください "ONTAP NVMe/FC Host Configuration Guide" および "TR-4684"。次の図は、vSphereホストからONTAP LUNへのマルチパス接続を示しています。




**NFS**

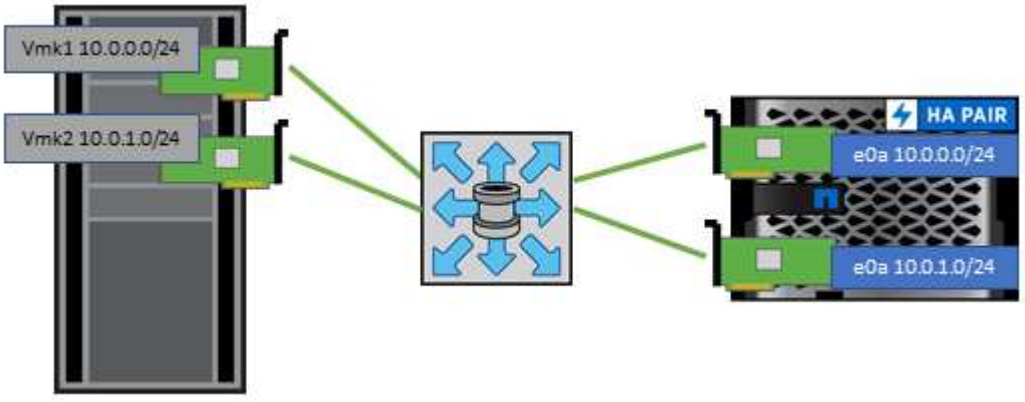
vSphere を使用すると、エンタープライズクラスの NFS アレイを使用して、 ESXi クラスタ内のすべてのノードへのデータストアへの同時アクセスを提供できます。データストアのセクションで説明したように、 vSphere で NFS を使用すると、使いやすさが向上し、ストレージ効率を可視化できるというメリットがあります。

vSphere で ONTAP NFS を使用する際に推奨されるベストプラクティスは次のとおりです。

- ONTAP クラスタ内の各ノードの各 SVM で、 1 つの論理インターフェイス（ LIF ）を使用します。データストアごとの LIF の過去の推奨事項は不要になりました。直接アクセス（LIFとデータストアが同じノード上にある場合）を推奨しますが、一般にパフォーマンスへの影響は最小限（マイクロ秒）であるため、間接アクセスについて心配する必要はありません。
- 現在サポートされているすべてのバージョンのVMware vSphereで、NFS v3とv4.1の両方を使用できます。nconnectの公式サポートは、NFS v3用のvSphere 8.0 Update 2に追加されました。NFS v4.1 のvSphereは、セッショントランキング、Kerberos認証、整合性を維持したKerberos認証を引き続きサポートします。セッショントランキングにはONTAP 9.14.1以降のバージョンが必要であることに注意してください。nconnect機能の詳細と、nconnect機能によってパフォーマンスがどのように向上するかについては、 "NetAppおよびVMwareでのNFSv3 nconnect機能"。

NFSv3とNFSv4.1では、異なるロックメカニズムが使用されていることに注目してください。NFSv3ではクライアント側ロックが使用され、NFSv4.1ではサーバ側ロックが使用されます。ONTAPボリュームは両方のプロトコルでエクスポートできますが、ESXiは1つのプロトコルでしかデータストアをマウントできません。ただしこれは、他のESXiホストが異なるバージョンを使用して同じデータストアをマウントできないという意味ではありません。問題を回避するには、マウント時に使用するプロトコルのバージョンを指定して、すべてのホストで同じバージョン、つまり同じロック形式を使用するようにする必要があります。NFSバージョンをホスト間で混在させないことが重要です。可能であれば、ホストプロファイルを使用して準拠を確認します。データストアは**NFSv3**と**NFSv4.1**の間で自動で変換されないため、新しい**NFSv4.1**データストアを作成し、**Storage vMotion**を使用して新しいデータストアに**VM**を移行します。
NFS v4.1の相互運用性の表を参照してください。 "NetApp Interoperability Matrix Tool で確認できます" をサポートするには、特定の ESXi パッチレベルが必要です。
* NFSエクスポートポリシーは、vSphereホストによるアクセスの制御に使用されます。複数のボリューム（データストア）で 1 つのポリシーを使用できます。NFSv3 では、 ESXi で sys （ UNIX ）セキュリティ形式が使用され、 VM を実行するためにルートマウントオプションが必要となります。ONTAP では、このオプションはスーパーユーザと呼ばれます。スーパーユーザオプションを使用する場合は、匿名ユーザ ID を指定する必要はありません。の値が異なるエクスポートポリシールールに注意してください `-anon` および `-allow -suid` 原因 SVM検出がONTAP ツールで問題を検出できるかどうか。ポリシーの例を次に示します。
アクセスプロトコル：**NFS3**
クライアント一致仕様：192.168.42.21

**RO**アクセスルール**: sys**
RWアクセスルール: sys
匿名**UID**
スーパーユーザ: sys
* NetApp NFS Plug-in for VMware VAAIを使用する場合、プロトコルは次のように設定する必要があります。 `nfs` エクスポートポリシールールが作成または変更されたとき。VAAIコピーオフロードが機能するためには、次のように指定してNFSv4プロトコルが必要です。 `nfs` NFSv3とNFSv4の両方のバージョンが自動的に含まれます。
* NFSデータストアボリュームはSVMのルートボリュームからジャンクションされるため、ESXiがデータストアボリュームに移動してマウントするには、ルートボリュームへのアクセスも必要です。ルートボリューム、およびデータストアボリュームのジャンクションがネストされているその他のボリュームのエクスポートポリシーには、ESXiサーバに読み取り専用アクセスを許可するルールが含まれている必要があります。VAAIプラグインを使用したルートボリュームのポリシーの例を次に示します。
アクセスプロトコル：**NFS**（**NFS3**と**nfs4**の両方を含む）
クライアント一致仕様：192.168.42.21
**RO**アクセスルール**: sys**
RW Access Rule：never（ルートボリュームに最適なセキュリティ）
匿名**UID**
Superuser：sys（VAAIを使用するルートボリュームにも必要）
* ONTAP Tools for VMware vSphere（最も重要なベストプラクティス）を使用します。
**ONTAP Tools for VMware vSphere**を使用すると、エクスポートポリシーの管理が自動的に簡素化されるため、データストアをプロビジョニングできます。
プラグインを使用してVMwareクラスタ用のデータストアを作成する場合は、単一のESXサーバではなくクラスタを選択します。これにより、データストアがクラスタ内のすべてのホストに自動的にマウントされます。既存のデータストアを新しいサーバに適用するには、プラグインマウント機能を使用します。
ONTAP Tools for VMware vSphereを使用しない場合は、すべてのサーバ、または追加のアクセス制御が必要なサーバのクラスタごとに1つのエクスポートポリシーを使用します。
* ONTAPは柔軟なボリュームネームスペース構造を提供し、ジャンクションを使用してボリュームをツリーにまとめることができますが、このアプローチはvSphereには意味がありません。ストレージのネームスペース階層に関係なく、データストアのルートに各 VM 用のディレクトリが作成されます。そのため、単に SVM のルートボリュームに vSphere のボリュームのジャンクションパスをマウントすることがベストプラクティスです。これは、 VMware vSphere 用の ONTAP ツールでデータストアをプロビジョニングする方法です。ジャンクションパスがネストされていないと、ルートボリューム以外のボリュームに依存しているボリュームがないこと、またボリュームをオフラインにするか破棄するかによって意図的に他のボリュームへのパスに影響が及ぶこともありません。
* NFSデータストア上のNTFSパーティションでは、ブロックサイズを4Kに設定しても問題ありません。次の図は、 vSphere ホストから ONTAP NFS データストアへの接続を示しています。




次の表に、 NFS のバージョンとサポートされる機能を示します。

| vSphere の機能 | NFSv3 | NFSv4.1 |
| --- | --- | --- |
| vMotion と Storage vMotion | はい。 | はい。 |
| 高可用性 | はい。 | はい。 |
| フォールトトレランス | はい。 | はい。 |
| DRS | はい。 | はい。 |
| ホストプロファイル | はい。 | はい。 |
| Storage DRS | はい。 | いいえ |
| ストレージ I/O の制御 | はい。 | いいえ |
| SRM の場合 | はい。 | いいえ |
| 仮想ボリューム | はい。 | いいえ |
| ハードウェアアクセラレーション（ VAAI ） | はい。 | はい。 |
| Kerberos 認証 | いいえ | ○（ vSphere 6.5 以降で拡張して、 AES 、 krb5i ） |
| マルチパスのサポート | いいえ | ○（ONTAP 9.14.1） |

直接接続ネットワーク

ストレージ管理者は、構成からネットワークスイッチを削除してインフラを簡易化したいと考える場合があります。これは一部のシナリオでサポートされます。

#### iSCSIとNVMe/TCP

iSCSIまたはNVMe/TCPを使用するホストは、ストレージシステムに直接接続して正常に動作することができます。その理由はパス設定です。2つの異なるストレージコントローラに直接接続すると、データフローが2つの独立したパスになります。パス、ポート、またはコントローラが失われても、他のパスの使用が妨げられることはありません。

#### NFS

直接接続されたNFSストレージも使用できますが、フェイルオーバーには大きな制限があります。スクリプト作成にはお客様の責任が伴います。

直接接続されたNFSストレージで無停止フェイルオーバーが複雑になるのは、ローカルOSで発生するルーティングが原因です。たとえば、ホストのIPアドレスが192.168.1.1/24で、IPアドレスが192.168.1.50/24のONTAPコントローラに直接接続されているとします。フェールオーバー中、192.168.1.50アドレスはもう一方のコントローラにフェールオーバーでき、ホストが使用できるようになりますが、ホストはそのアドレスの存在をどのように検出しますか。元の192.168.1.1アドレスは、動作中のシステムに接続されていないホストNICに残っています。192.168.1.50宛てのトラフィックは、動作不能なネットワークポートに引き続き送信されます。

2番目のOS NICは19に設定できます。 2.168.1.2およびは、192.168.1.50経由でフェールオーバーされたアドレスと通信できますが、ローカルルーティングテーブルのデフォルトでは、192.168.1.0/24サブネットと通信するために1つの*および1つの*アドレスのみを使用することになります。システム管理者は、失敗したネットワーク接続を検出し、ローカルルーティングテーブルを変更したり、インターフェイスをアップ/ダウンしたりするスクリプトフレームワークを作成できます。正確な手順は、使用しているOSによって異なります。

実際にはNetAppを使用していますが、通常はフェイルオーバー中のIO一時停止が許容されるワークロードのみが対象です。ハードマウントを使用する場合は、一時停止中にIOエラーが発生しないようにしてください。ホスト上のNIC間でIPアドレスを移動するためのフェイルバックまたは手動操作によって、サービスが復元されるまでIOはハングします。

#### FC直接接続

FCプロトコルを使用してホストをONTAPストレージシステムに直接接続することはできません。その理由はNPIVの使用です。FCネットワークへのONTAP FCポートを識別するWWNは、NPIVと呼ばれる仮想化タイプを使用します。ONTAPシステムに接続されているすべてのデバイスがNPIV WWNを認識できる必要があります。現在、NPIVターゲットをサポートできるホストにインストールできるHBAを提供しているHBAベンダーはありません。

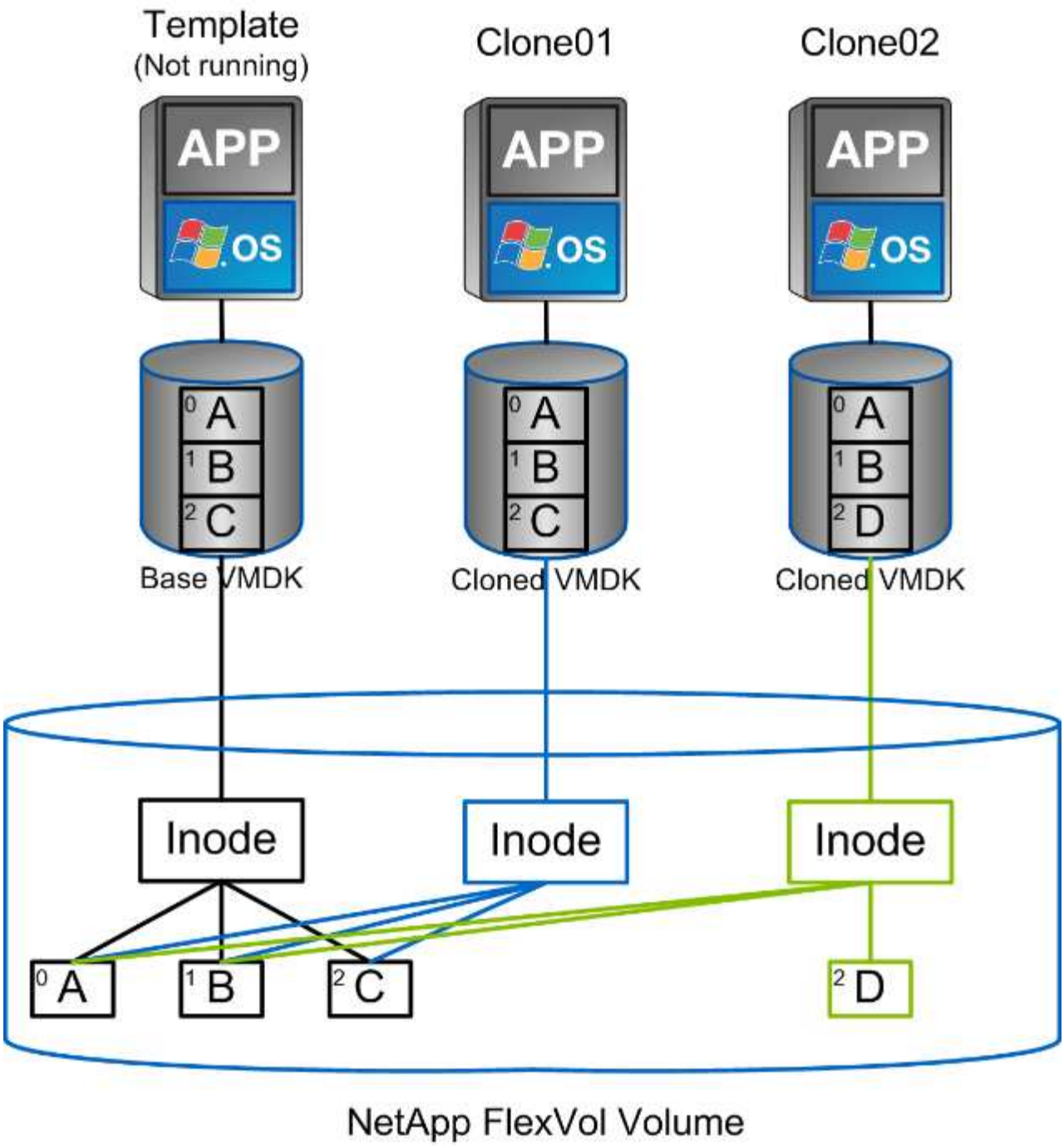
## VM とデータストアのクローニング

ストレージオブジェクトをクローニングすると、追加の VM のプロビジョニングやバックアップ / リカバリ処理などの用途に使用できるコピーを簡単に作成できます。

vSphere では、 VM 、仮想ディスク、 VVOL 、またはデータストアをクローニングできます。クローニングされたオブジェクトは、多くの場合、自動化されたプロセスによってさらにカスタマイズできます。vSphereでは、フルコピークローンとリンククローンの両方がサポートされます。リンククローンでは、元のオブジェクトとは別に変更が追跡されます。

リンククローンはスペースを節約するのに適していますが、 vSphere が VM に対して処理する I/O 量が増えるため、その VM のパフォーマンスや場合によってはホスト全体のパフォーマンスに影響します。そのため、NetAppのお客様は、ストレージシステムベースのクローンを使用して、ストレージの効率的な使用とパフォーマンスの向上という2つのメリットを活用することがよくあります。

次の図は、 ONTAP クローニングを示しています。




クローニングは、 ONTAP ソフトウェアを実行するシステムに複数のメカニズムを使用してオフロードできます。通常は、 VM 、 VVol 、データストアのレベルでオフロードします。これには次のものが含まれます。

- NetApp vSphere APIs for Storage Awareness （ VASA ） Provider を使用した VVol のクローニング。vCenterで管理されるVVol Snapshotをサポートするために、ONTAPクローンを使用します。VVol Snapshotの作成や削除によるI/Oへの影響は最小限で、スペース効率に優れています。 VM のクローニングは vCenter を使用して行うこともでき、 1 つのデータストア / ボリューム内かデータストア / ボリューム間かに関係なく、 ONTAP にオフロードされます。
- vSphere APIs – Array Integration （ VAAI ）を使用した vSphere のクローニングと移行：SAN 環境と NAS 環境の両方で、 VM のクローニング処理を ONTAP にオフロードできます（ネットアップでは、 NFS 用の VAAI を有効にするために ESXi プラグインを提供しています）。 vSphere は、 NAS データストア内のコールド（電源オフ） VM にのみオフロードします。一方、ホット VM （クローニングと

Storage vMotion ）の処理も SAN にオフロードされます。ONTAP では、ソース、デスティネーション、インストールされている製品ライセンスに基づいて最も効率的なアプローチを採用しています。この機能は VMware Horizon View でも使用されています。

- SRA （ VMware Site Recovery Manager で使用）。ここでは、クローンを使用して、 DR レプリカのリカバリを無停止でテストします。
- SnapCenter などのネットアップのツールを使用したバックアップとリカバリVM クローンは、バックアップ処理の検証や VM バックアップのマウントに使用され、個々のファイルをコピーできるようにします。

ONTAP オフロードクローニングは、 VMware 、ネットアップ、サードパーティのツールから実行できます。ONTAP にオフロードされたクローンには、いくつかのメリットがあります。ほとんどの場合、スペース効率に優れており、オブジェクトの変更にのみ対応するストレージが必要です。読み取りや書き込みのパフォーマンスには影響しません。また、高速キャッシュでブロックを共有することでパフォーマンスが向上する場合もあります。また、 CPU サイクルとネットワーク I/O も ESXi サーバからオフロードされます。FlexVol を使用する従来のデータストア内でのコピーオフロードは、 FlexClone ライセンスを使用すると高速かつ効率的ですが、 FlexVol 間のコピーの方が低速になる可能性があります。VM テンプレートをクローンのソースとして管理する場合は、スペース効率に優れた高速クローンを作成するために、テンプレートをデータストアボリューム内に配置することを検討してください（フォルダやコンテンツライブラリを使用してテンプレートを整理します）。

ONTAP 内で直接ボリュームまたは LUN をクローニングして、データストアをクローニングすることもできます。NFS データストアの場合は、 FlexClone テクノロジでボリューム全体をクローニングし、 ONTAP からクローンをエクスポートして、別のデータストアとして ESXi にマウントできます。VMFS データストアの場合は、ボリューム内の LUN 、または 1 つ以上の LUN を含むボリューム全体を ONTAP でクローニングできます。VMFS を含む LUN を通常のデータストアとしてマウントして使用するためには、 LUN を ESXi igroup にマッピングし、 ESXi から再署名を受ける必要があります。ただし一部の一時的なユースケースでは、クローニングされた VMFS を再署名なしでマウントすることができます。クローニングしたデータストア内の VM は、個別にクローニングした VM と同様に登録、再設定、およびカスタマイズすることができます。

バックアップや FlexClone 用の SnapRestore など、追加のライセンス機能を使用してクローニングを強化できる場合があります。これらのライセンスは、追加コストなしでライセンスバンドルに含まれていることがよくあります。FlexCloneライセンスは、VVolのクローニング処理や、VVolの管理対象Snapshot（ハイパーバイザーからONTAPにオフロードされる）をサポートするために必要です。FlexClone をデータストア / ボリューム内で使用すると、特定の VAAI ベースのクローンの品質を向上させることもできます（ブロックコピーではなく、スペース効率に優れたコピーが瞬時に作成されます）。 また、 DR レプリカのリカバリをテストする際に SRA で使用され、クローニング処理用に SnapCenter でバックアップコピーを参照して個々のファイルをリストアする際にも使用されます。

## データ保護

### VM のバックアップと迅速なリカバリは、 ONTAP for vSphere の大きな特長の 1 つです。この機能は、 SnapCenter Plug-in for VMware vSphere を使用して vCenter 内で簡単に管理できます。

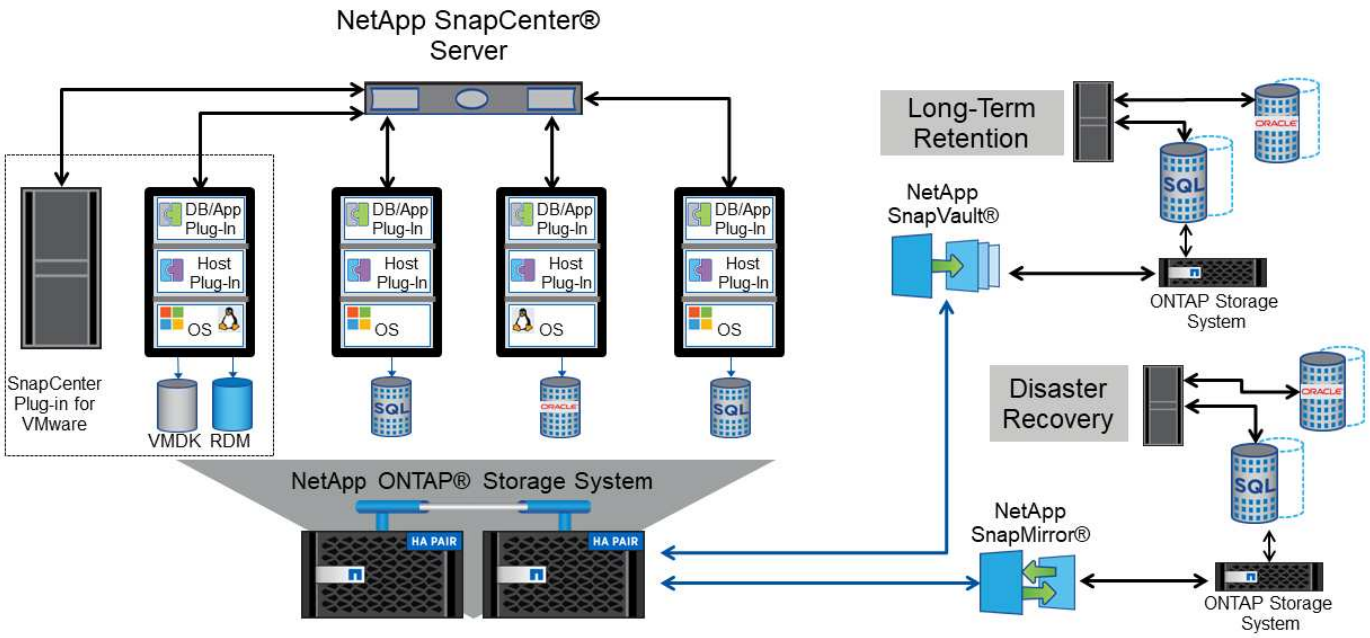
Snapshotを使用すると、パフォーマンスに影響を与えずにVMやデータストアのコピーをすばやく作成でき、SnapMirrorを使用してセカンダリシステムに送信することで、オフサイトでの長期的なデータ保護を実現できます。このアプローチでは、変更された情報のみを格納することで、ストレージスペースとネットワーク帯域幅を最小限に抑えます。

SnapCenter では、複数のジョブに適用可能なバックアップポリシーを作成できます。これらのポリシーでは、スケジュール、保持、レプリケーションなどの機能を定義できます。VMwareスナップショットを作成す

る前にI/Oを休止するハイパーバイザーの機能を活用して、VM整合性スナップショットをオプションで選択できます。ただし、 VMware スナップショットはパフォーマンスへの影響があるため、ゲストファイルシステムを休止する必要がないかぎり、一般には推奨されません。代わりに、スナップショットを使用して一般的な保護を行い、SnapCenterプラグインなどのアプリケーションツールを使用してSQL ServerやOracleなどのトランザクションデータを保護します。これらのスナップショットはVMware（整合性）スナップショットとは異なり、長期的な保護に適しています。 VMware スナップショットはのみです "（推奨）" パフォーマンスやその他の影響があるため、短期的な使用に適しています。

これらのプラグインは、物理環境と仮想環境の両方でデータベースを保護する拡張機能を提供します。vSphere では、これらのプロトコルを使用して、 RDM LUN 、ゲスト OS に直接接続された iSCSI LUN 、 VMFS または NFS データストア上の VMDK ファイルにデータが格納されている SQL Server または Oracle データベースを保護できます。プラグインでは、さまざまなタイプのデータベースバックアップを指定し、オンラインまたはオフラインのバックアップをサポートし、ログファイルとともにデータベースファイルを保護できます。プラグインは、バックアップとリカバリに加えて、開発やテスト目的でのデータベースのクローニングにも対応しています。

次の図は、 SnapCenter の導入例を示しています。




ディザスタリカバリ機能を強化するには、 ONTAP 用 NetApp SRA と VMware Site Recovery Manager の使用を検討してください。DR サイトへのデータストアのレプリケーションをサポートするだけでなく、レプリケートしたデータストアをクローニングすることで DR 環境を無停止でテストすることもできます。SRA に組み込まれている自動化機能を使用すると、災害からのリカバリや、システム停止が解決したあとの本番環境の再保護も簡単に実行できます。

最後に、最高レベルのデータ保護を実現するために、 NetApp MetroCluster を使用した VMware vSphere Metro Storage Cluster （ vMSC ）設定を検討してください。vMSC は、同期レプリケーションとアレイベースのクラスタリングを組み合わせた VMware 認定の解決策です。高可用性クラスタと同じメリットを提供しますが、複数のサイトに分散してサイト障害から保護します。NetApp MetroCluster は、同期レプリケーション向けの対費用効果の高い構成を提供します。ストレージコンポーネントのあらゆる単一障害から透過的にリカバリでき、サイト障害時にコマンド 1 つでリカバリできます。vMSC の詳細については、を参照してください "TR-4128"。

## サービス品質（ **QoS** ）

ONTAP ソフトウェアを実行するシステムでは、 ONTAP ストレージ QoS 機能を使用して、ファイル、 LUN 、ボリューム、 SVM 全体などの異なるストレージオブジェクトに対するスループットを MBps や IOPS （ 1 秒あたりの I/O 数）で制限できます。

スループット制限は、他のワークロードに影響しないように、導入前に未知のワークロードやテストワークロードを制御するのに役立ちます。また、 Bully ワークロードが特定された場合に、この 2 つを使用して抑制することもできます。ONTAP 9.2 では SAN オブジェクトに、 ONTAP 9.3 では NAS オブジェクトに一貫したパフォーマンスを提供するために、 IOPS に基づく最小サービスレベルもサポートされています。

NFS データストアの場合は、 QoS ポリシーを FlexVol 全体またはボリューム内の個々の VMDK ファイルに適用できます。ONTAP LUN を使用する VMFS データストアでは、 LUN を含む FlexVol ボリュームには QoS ポリシーを適用できますが、 ONTAP が VMFS ファイルシステムを認識しないため、個々の VMDK ファイルには適用できません。VVol を使用する場合は、ストレージ機能プロファイルと VM ストレージポリシーを使用して、個々の VM に最小 QoS と最大 QoS を設定できます。

オブジェクトに対する QoS の最大スループット制限は、 MBps と IOPS のいずれかまたは両方で設定できます。両方を使用する場合は、最初に到達した制限が ONTAP によって適用されます。ワークロードには複数のオブジェクトを含めることができ、 QoS ポリシーは 1 つ以上のワークロードに適用できます。ポリシーを複数のワークロードに適用した場合は、ポリシーの制限はワークロード全体に適用されます。ネストされたオブジェクトはサポートされません（たとえば、ボリューム内のファイルには個別のポリシーを設定することはできません）。QoS の最小値は IOPS 単位でのみ設定できます。

ONTAP QoS ポリシーの管理とオブジェクトへの適用に現在使用できるツールは次のとおりです。

- ONTAP CLI
- ONTAP システムマネージャ
- OnCommand Workflow Automation のサポートを利用できます
- Active IQ Unified Manager
- NetApp PowerShell Toolkit for ONTAP
- VMware vSphere VASA Provider 用の ONTAP ツール

NFS 上の VMDK に QoS ポリシーを割り当てる場合は、次のガイドラインに注意してください。

- ポリシーは、 `vmname- flat.vmdk` ではなく、実際の仮想ディスクイメージが含まれています。 `vmname.vmdk` （仮想ディスク記述ファイル）または `vmname.vmx` （VM記述ファイル）。
- 仮想スワップファイルなど、他のVMファイルにポリシーを適用しない (`vmname.vswp`）。
- vSphere Web Clientを使用してファイルパスを検索する場合（[Datastore]>[Files]）は、 `- flat.vmdk` および `. vmdk` 1つのファイルが表示されます。このファイルには、 `. vmdk` しかしその大きさは `- flat.vmdk`。追加（ Add ） `-flat` ファイル名に入力して、正しいパスを取得します。

VMFS と RDM 、 ONTAP SVM （ SVM として表示）、 LUN パス、シリアル番号などの LUN に QoS ポリシーを割り当てるには、 ONTAP Tools for VMware vSphere のホームページのストレージシステムメニューから QoS ポリシーを取得します。ストレージシステム（SVM）を選択し、[Related Objects]>[SAN]を選択します。 この方法は、いずれかの ONTAP ツールを使用して QoS を指定する場合に使用します。

VVol ベースの VM には、 VMware vSphere または Virtual Storage Console 7.1 以降の ONTAP ツールを使用して、最大 QoS と最小 QoS を簡単に割り当てることができます。VVolコンテナのストレージ機能プロファ

イルを作成するときは、パフォーマンス機能で最大IOPSと最小IOPSの値を指定し、このSCPをVMのストレージポリシーで参照します。このポリシーは VM を作成するときに使用するか、ポリシーを既存の VM に適用します。

FlexGroup データストアでは、 ONTAP ツールを VMware vSphere 9.8 以降で使用する場合に、 QoS 機能が強化されています。QoS は、データストア内のすべての VM 、または特定の VM に簡単に設定できます。詳細については、本レポートの「 FlexGroup 」セクションを参照してください。

### ONTAP の QoS と VMware の SIOC

ONTAP の QoS と VMware vSphere の Storage I/O Control （ SIOC ）は、 vSphere 管理者とストレージ管理者が組み合わせて、 ONTAP ソフトウェアを実行するシステムでホストされる vSphere VM のパフォーマンスを管理できる、相互に補完するテクノロジです。各ツールには、次の表に示すようにそれぞれの長所があります。VMware vCenter と ONTAP ではスコープが異なるため、一部のオブジェクトは一方のシステムで認識および管理でき、もう一方のシステムではできません。

| プロパティ（ **Property** ） | **ONTAP QoS** | **VMware SIOC** |
|---|---|---|
| アクティブになっている場合 | ポリシーは常にアクティブです | 競合が発生している（データストアのレイテンシがしきい値を超えている）場合 |
| 単位のタイプ | IOPS 、 MBps | IOPS 、共有数 |
| 対象となる vCenter またはアプリケーション | 複数の vCenter 環境、その他のハイパーバイザーとアプリケーションがあります | 単一の vCenter サーバ |
| VM に QoS を設定？ | NFS 上の VMDK のみ | NFS 上または VMFS 上の VMDK です |
| LUN （ RDM ）で QoS を設定？ | はい。 | いいえ |
| LUN （ VMFS ）への QoS の設定 | はい。 | いいえ |
| ボリューム（ NFS データストア）への QoS の設定 | はい。 | いいえ |
| SVM （テナント）に QoS を設定？ | はい。 | いいえ |
| ポリシーベースのアプローチ | はい。ポリシー内のすべてのワークロードで共有することも、ポリシー内の各ワークロードにフルに適用することもできます。 | はい。 vSphere 6.5 以降が必要です。 |
| ライセンスが必要です | ONTAP に付属しています | Enterprise Plus |

### VMware Storage Distributed Resource Scheduler の略

VMware Storage Distributed Resource Scheduler （ SDRS ）は、現在の I/O レイテンシとスペース使用量に基づいて VM をストレージに配置する vSphere の機能です。その後、 VM や VMDK の配置先として最適なデータストアをデータストアクラスタ内から選択し、システムを停止することなくデータストアクラスタ（ポッドとも呼ばれます）内のデータストア間で VM や VMDK を移動します。データストアクラスタは、類似するデータストアをvSphere管理者から見た単一の消費単位に集約したものです。

SDRSとONTAP tools for VMware vSphereを使用する場合は、まずプラグインを使用してデータストアを作成し、vCenterを使用してデータストアクラスタを作成してから、そのデータストアにデータストアを追加する

必要があります。データストアクラスタを作成したら、プロビジョニングウィザードの詳細ページからデータストアクラスタにデータストアを直接追加できます。

SDRS に関するその他の ONTAP のベストプラクティスは、次のとおりです。

- クラスタ内のすべてのデータストアで同じタイプのストレージ（ SAS 、 SATA 、 SSD など）を使用し、すべて VMFS データストアまたは NFS データストアとし、レプリケーションと保護の設定を同じにします。
- デフォルト（手動）モードでは SDRS の使用を検討してください。このアプローチでは、推奨事項を確認し、適用するかどうかを決定できます。VMDK の移行による影響を次に示します。
  - SDRS がデータストア間で VMDK を移動すると、 ONTAP のクローニングや重複排除によるスペース削減効果は失われます。重複排除機能を再実行すれば、削減効果を取り戻すことができます。
  - NetAppでは、VMDKを移動したあとに、移動したVMによってスペースがロックされるため、ソースデータストアでSnapshotを再作成することを推奨しています。
  - 同じアグリゲート上のデータストア間で VMDK を移動してもメリットはほとんどなく、 SDRS はアグリゲートを共有する可能性のある他のワークロードを可視化できません。

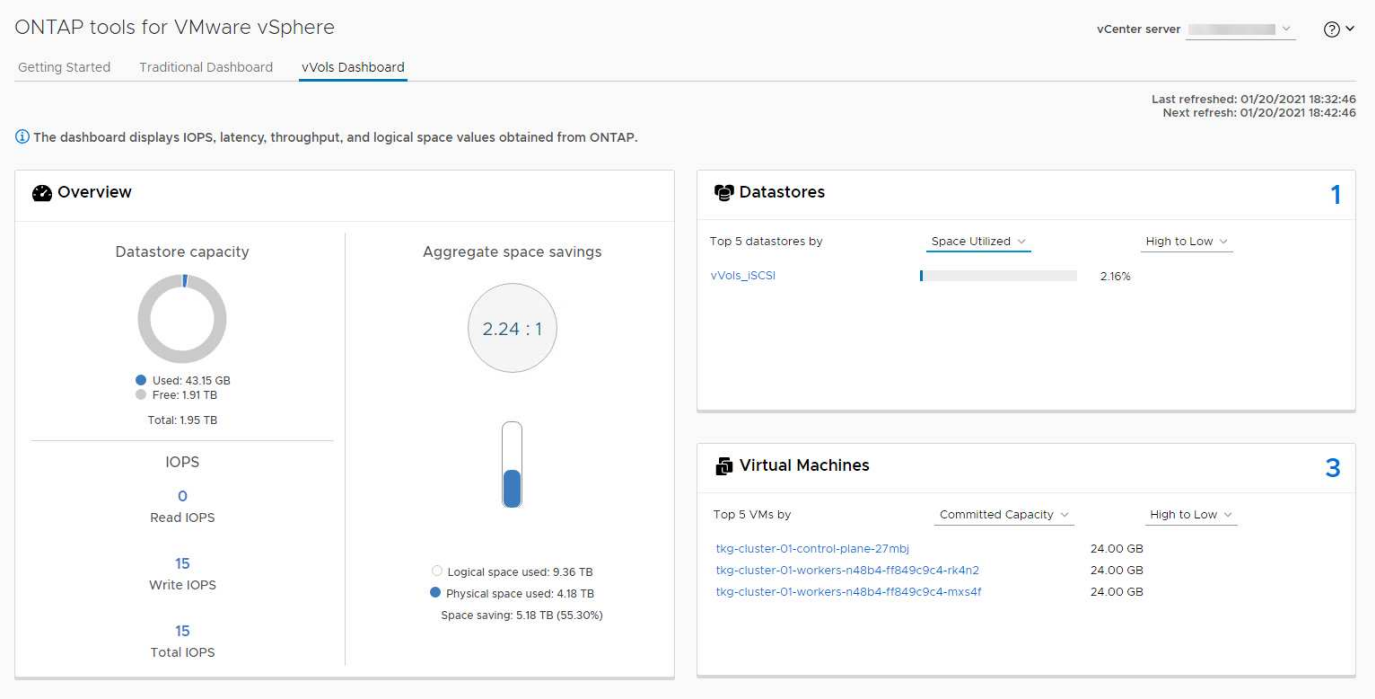
ストレージポリシーベースの管理と**VVOL**

VMware vSphere APIs for Storage Awareness （ VASA ）を使用すると、ストレージ管理者は、明確に定義された機能を使用してデータストアを簡単に設定でき、 VM 管理者は、相互にやり取りすることなく、いつでも VM をプロビジョニングするためのこれらの機能を使用できます。このアプローチを見て、仮想化ストレージの運用を合理化し、単純な作業の多くを回避する方法を確認することをお勧めします。

VASA が導入される前は、 VM 管理者が VM ストレージポリシーを定義することもできましたが、適切なデータストアを特定するには、多くの場合、ドキュメントや命名規則を使用する必要がありました。VASA を使用すると、ストレージ管理者は、パフォーマンス、階層化、暗号化、レプリケーションなど、さまざまなストレージ機能を定義できます。1 つのボリュームまたはボリュームセットの一連の機能を、ストレージ機能プロファイル（ SCP ）と呼びます。

SCPでは、VMのデータVVOLに対して最小または最大のQoSがサポートされます。最小 QoS は AFF システムでのみサポートされます。VMware vSphere 用の ONTAP ツールには、 ONTAP システム上の VVOL の VM の詳細なパフォーマンスと論理容量を表示するダッシュボードがあります。

次の図は、 VMware vSphere 9.8 VVol ダッシュボード用の ONTAP ツールを示しています。




ストレージ機能プロファイルを定義したら、そのプロファイルを使用して要件を定義するストレージポリシーを使用して VM をプロビジョニングできます。vCenter では、 VM ストレージポリシーとデータストアストレージ機能プロファイルのマッピングに基づいて、互換性があるデータストアのリストを選択対象として表示できます。このアプローチは、ストレージポリシーベースの管理と呼ばれます。

VASA は、ストレージを照会して一連のストレージ機能を vCenter に返すためのテクノロジを提供します。VASA ベンダープロバイダは、ストレージシステムの API およびコンストラクトと、 vCenter が認識可能な VMware API との間の変換機能を提供します。ネットアップのVASA Provider for ONTAPは、ONTAP Tools for VMware vSphereアプライアンスVMの一部として提供されます。vCenterプラグインは、VVOLデータストアをプロビジョニングおよび管理するためのインターフェイスと、ストレージ機能プロファイル（SCP）を定義する機能を提供します。

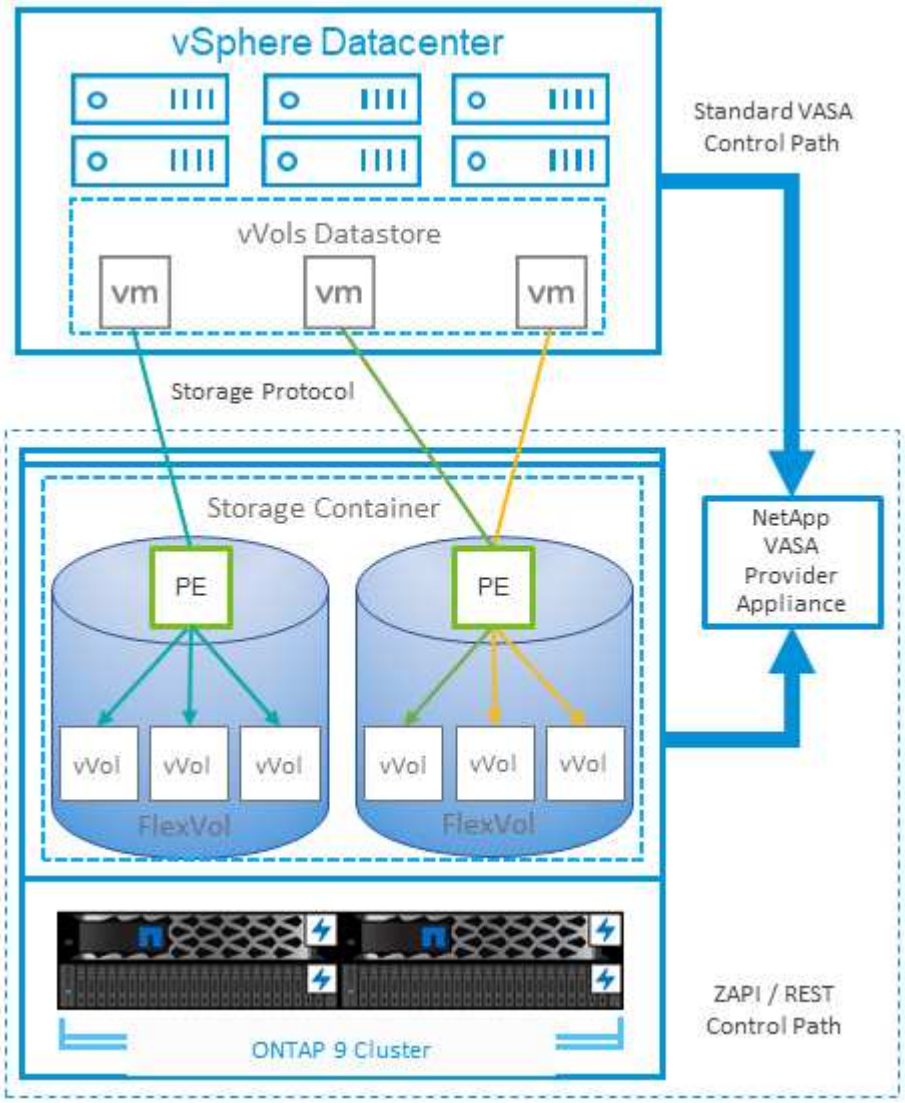
ONTAP は、 VMFS データストアと NFS データストアの両方をサポートしています。SAN データストアで VVOL を使用すると、 VM レベルのきめ細かさなど、 NFS のメリットの一部を活用できます。ここでは考慮すべきベストプラクティスをいくつか示します。また、追加情報はにあります "TR-4400"：

- VVOL データストアは、複数のクラスタノードにある複数の FlexVol で構成できます。ボリュームごとに機能が異なる場合でも、最もシンプルなアプローチは 1 つのデータストアです。SPBM により、互換性のあるボリュームが VM に使用されています。ただし、すべてのボリュームが 1 つの ONTAP SVM に含まれていて、単一のプロトコルでアクセスできる必要があります。各プロトコルでノードごとに 1 つの LIF で十分です。1 つの VVOL データストアで複数の ONTAP リリースを使用することは避けてください。リリースによってストレージ機能が異なる場合があります。
- VVol データストアの作成と管理には、 VMware vSphere プラグインの ONTAP ツールを使用します。データストアとそのプロファイルの管理に加え、必要に応じて、 VVOL にアクセスするためのプロトコルエンドポイントが自動的に作成されます。LUN を使用する場合、 LUN PE は 300 以上の LUN ID を使用してマッピングされます。ESXiホストの詳細なシステム設定を確認する `Disk.MaxLUN` 300を超えるLUN ID番号を許可します（デフォルトは1、024）。そのためには、vCenterでESXiホストを選択し、[Configure]タブで `Disk.MaxLUN` をクリックします。
- VASA Provider 、 vCenter Server （アプライアンスまたは Windows ベース）、または VMware vSphere 用の ONTAP ツールは相互に依存するため、 VVOL データストアにインストールしたり移行したりしないでください。これらのツールは、停電やその他のデータセンターの停止が発生した場合に管理しなくなる

ためです。

- VASA Provider VM を定期的にバックアップします。VASA Providerが格納された従来のデータストアのSnapshotを少なくとも1時間ごとに作成してください。VASA Provider の保護とリカバリの詳細については、こちらを参照してください "こちらの技術情報アーティクル"。

次の図は、 VVOL のコンポーネントを示しています。




クラウドへの移行とバックアップ

ONTAP のもう 1 つの強みは、ハイブリッドクラウドを幅広くサポートすることで、オンプレミスのプライベートクラウドのシステムとパブリッククラウドの機能を統合できることです。vSphere と組み合わせて使用できるネットアップのクラウドソリューションには、次のものがあります。

- * Cloud Volumes。* NetApp Cloud Volumes Service for Amazon Web ServicesまたはGoogle Cloud PlatformとAzure NetApp Files for ANFは、主要なパブリッククラウド環境でハイパフォーマンスなマルチプロトコルマネージドストレージサービスを提供します。VMware Cloud VM ゲストで直接使用できます。
- * Cloud Volumes ONTAP 。 * NetApp Cloud Volumes ONTAP データ管理ソフトウェアは、お客様が選択したクラウド上のデータを管理、保護、柔軟性、効率性で保護します。Cloud Volumes ONTAP は、ONTAPストレージ上に構築されたクラウドネイティブのデータ管理ソフトウェアです。Cloud

Volumes ONTAP インスタンスをオンプレミスの ONTAP システムと一緒に導入、管理する際には、Cloud Manager と組み合わせて使用できます。NASおよびiSCSI SANの高度な機能と、スナップショットやSnapMirrorレプリケーションなどの統合データ管理機能を活用できます。

- * Cloud Backup Service * 。クラウドサービスまたは SnapMirror クラウドを使用して、パブリッククラウドストレージを使用してオンプレミスシステムからデータを保護します。Cloud Sync を使用すると、NAS 、オブジェクトストア、 Cloud Volumes Service ストレージ間でデータを移行し、同期を維持できます。
- * ONTAP * FabricPool は、 FabricPool データの階層化を迅速かつ容易にします。コールドブロックは、パブリッククラウドまたはStorageGRIDのプライベートオブジェクトストアにあるオブジェクトストアに移行でき、ONTAPデータが再度アクセスされると自動的にリコールされます。または、 SnapVault ですでに管理されているデータの第 3 レベルの保護としてオブジェクト階層を使用することもできます。この方法を使用すると、を実行できます "VMのより多くのスナップショットを保存" プライマリおよびセカンダリ ONTAP ストレージシステム。
- * ONTAP Select * 。ネットアップの Software-Defined Storage を使用して、インターネット経由でプライベートクラウドをリモートの施設やオフィスに拡張できます。 ONTAP Select を使用すれば、ブロックサービスやファイルサービスのほか、エンタープライズデータセンターと同じ vSphere データ管理機能をサポートできます。

VM ベースのアプリケーションを設計する際は、将来のクラウドのモビリティを考慮してください。たとえば、アプリケーションファイルとデータファイルを一緒に配置するのではなく、データ用に別の LUN または NFS エクスポートを使用します。これにより、 VM とデータを別々にクラウドサービスに移行できます。

**vSphere** データの暗号化

現在、保管データを暗号化で保護する必要性はますます高まっています。当初は財務情報や医療情報に重点が置かれていましたが'ファイル'データベース'その他のデータタイプに保存されているかどうかにかかわらず'すべての情報を保護することへの関心が高まっています

ONTAP ソフトウェアを実行するシステムでは、保存データの暗号化を使用してあらゆるデータを簡単に保護できます。NetApp Storage Encryption （ NSE ）は、 ONTAP を備えた自己暗号化ディスクドライブを使用して、 SAN と NAS のデータを保護します。また、 NetApp Volume Encryption と NetApp Aggregate Encryption も、シンプルなソフトウェアベースの手法として、ディスクドライブ上のボリュームを暗号化します。このソフトウェア暗号化では、特別なディスクドライブや外部キー管理ツールは必要ありません。ONTAPのお客様は追加料金なしで利用できます。クライアントやアプリケーションを停止することなくアップグレードして使用を開始でき、オンボードキーマネージャなどの FIPS 140-2 レベル 1 標準で検証されます。

VMware vSphere 上で実行される仮想アプリケーションのデータを保護する方法はいくつかあります。1 つは、 VM 内のソフトウェアをゲスト OS レベルで使用してデータを保護する方法です。別の方法として、vSphere 6.5 などの新しいハイパーバイザーでは VM レベルの暗号化がサポートされるようになりました。ただし、ネットアップのソフトウェア暗号化はシンプルで使いやすく、次のようなメリットがあります。

- * 仮想サーバの CPU には影響しません。 * 仮想サーバ環境によっては、アプリケーションに使用可能なすべての CPU サイクルが必要ですが、ハイパーバイザーレベルの暗号化では最大 5 倍の CPU リソースが必要です。暗号化ソフトウェアがインテルのAES-NI命令セットをサポートして暗号化ワークロードをオフロードしていても（NetAppソフトウェア暗号化がサポートしているように）、古いサーバーと互換性のない新しいCPUが必要なため、このアプローチは実現できない可能性があります。
- * オンボードキーマネージャを含む。 * ネットアップのソフトウェア暗号化機能には、追加料金なしでオンボードキーマネージャが含まれているため、購入や使用が複雑な高可用性キー管理サーバなしで簡単に利用を開始できます。
- * ストレージ効率への影響はありません。 * 重複排除や圧縮などの Storage Efficiency テクノロジは現在広

く使用されており、フラッシュディスクメディアをコスト効率よく使用する上で鍵となります。ただし、一般に、暗号化されたデータは重複排除も圧縮もできません。ネットアップのハードウェアとストレージの暗号化は下位レベルで動作し、他のアプローチとは異なり、業界をリードするネットアップの Storage Efficiency 機能を最大限に活用できます。

- * データストアのきめ細かい暗号化が容易。 * NetApp Volume Encryption を使用すると、各ボリュームに専用の AES 256 ビットキーが設定されます。変更が必要な場合は、 1 つのコマンドで変更できます。このアプローチは、テナントが複数ある場合や、さまざまな部門やアプリケーションに対して個別に暗号化を証明する必要がある場合に適しています。この暗号化はデータストアレベルで管理されるため、個々の VM の管理よりもはるかに簡単です。

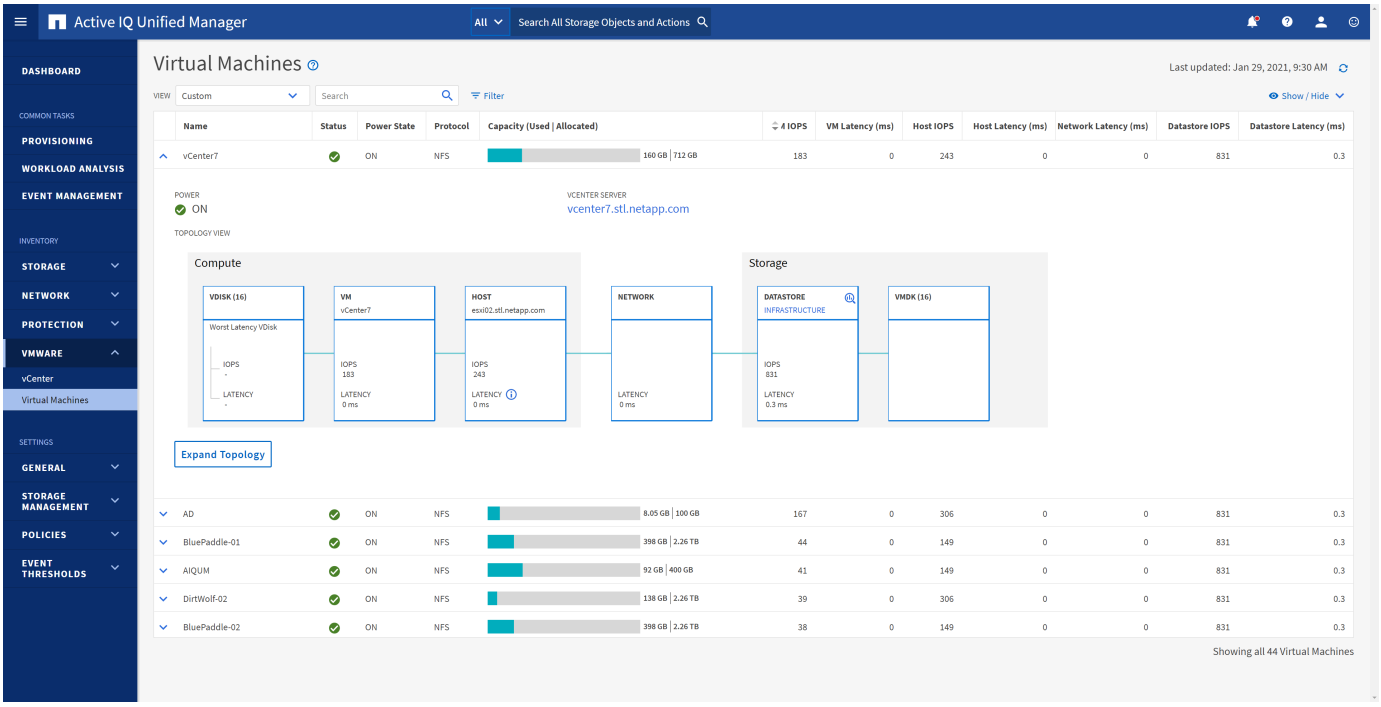
ソフトウェア暗号化を開始するのは簡単です。ライセンスのインストールが完了したら、パスフレーズを指定してオンボードキーマネージャを設定し、新しいボリュームを作成するかストレージ側のボリューム移動を実行して暗号化を有効にします。ネットアップでは、 VMware ツールの今後のリリースで、暗号化機能のサポートをさらに統合する予定です。

### Active IQ Unified Manager

Active IQ Unified Manager を使用すると、仮想インフラ内の VM を可視化し、仮想環境内のストレージやパフォーマンスの問題を監視してトラブルシューティングすることができます。

ONTAP の一般的な仮想インフラ環境には、さまざまなコンポーネントがコンピューティングレイヤ、ネットワークレイヤ、ストレージレイヤに分散して配置されています。VM アプリケーションのパフォーマンス低下は、各レイヤのさまざまなコンポーネントでレイテンシが生じていることが原因である可能性があります。

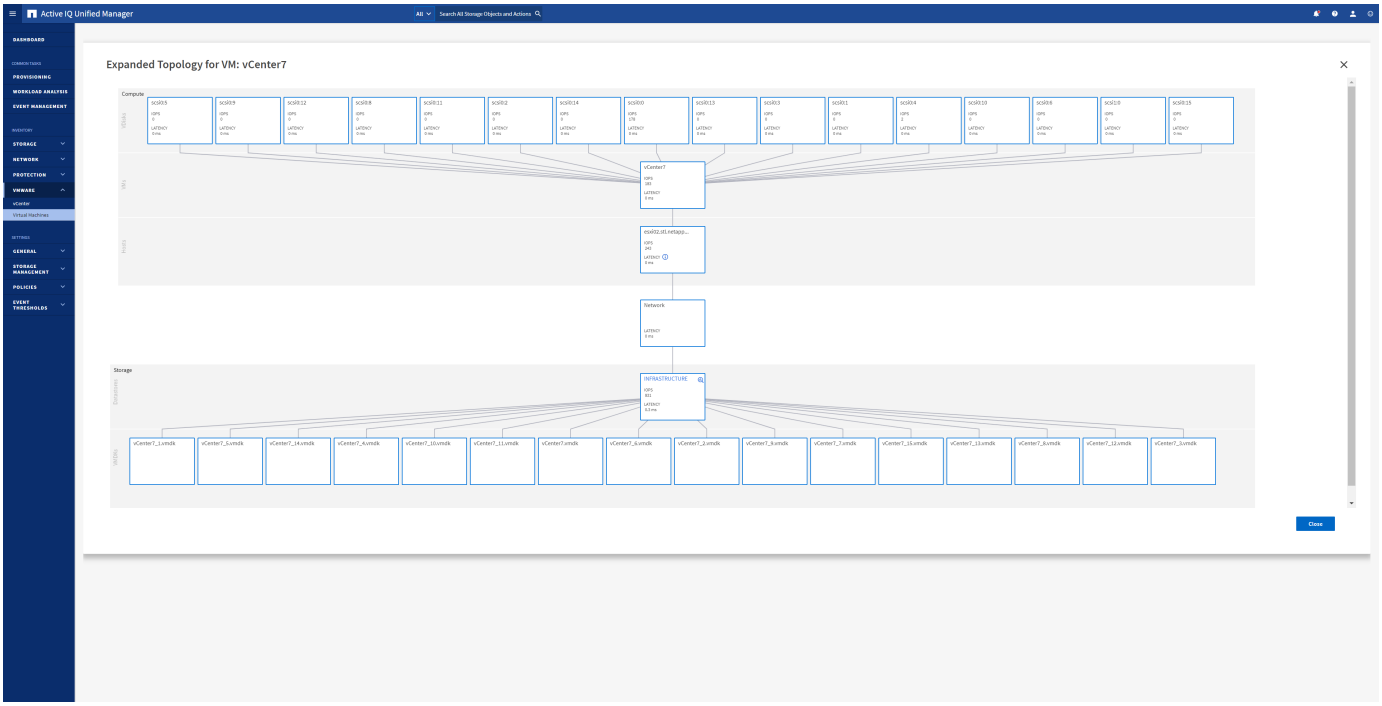
次のスクリーンショットは、 Active IQ Unified Manager の仮想マシンビューを示しています。



ビュー"]

Unified Manager のトポロジビューには、仮想環境の基盤となるサブシステムが表示され、コンピューティングノード、ネットワーク、またはストレージでレイテンシ問題が発生したかどうかが確認されます。また、修復手順を実行して基盤となる問題に対応するために、パフォーマンス低下の原因となっているオブジェクトが強調表示されます。

次のスクリーンショットは、 AIQUM の拡張トポロジを示しています。




## ストレージポリシーベースの管理と**VVOL**

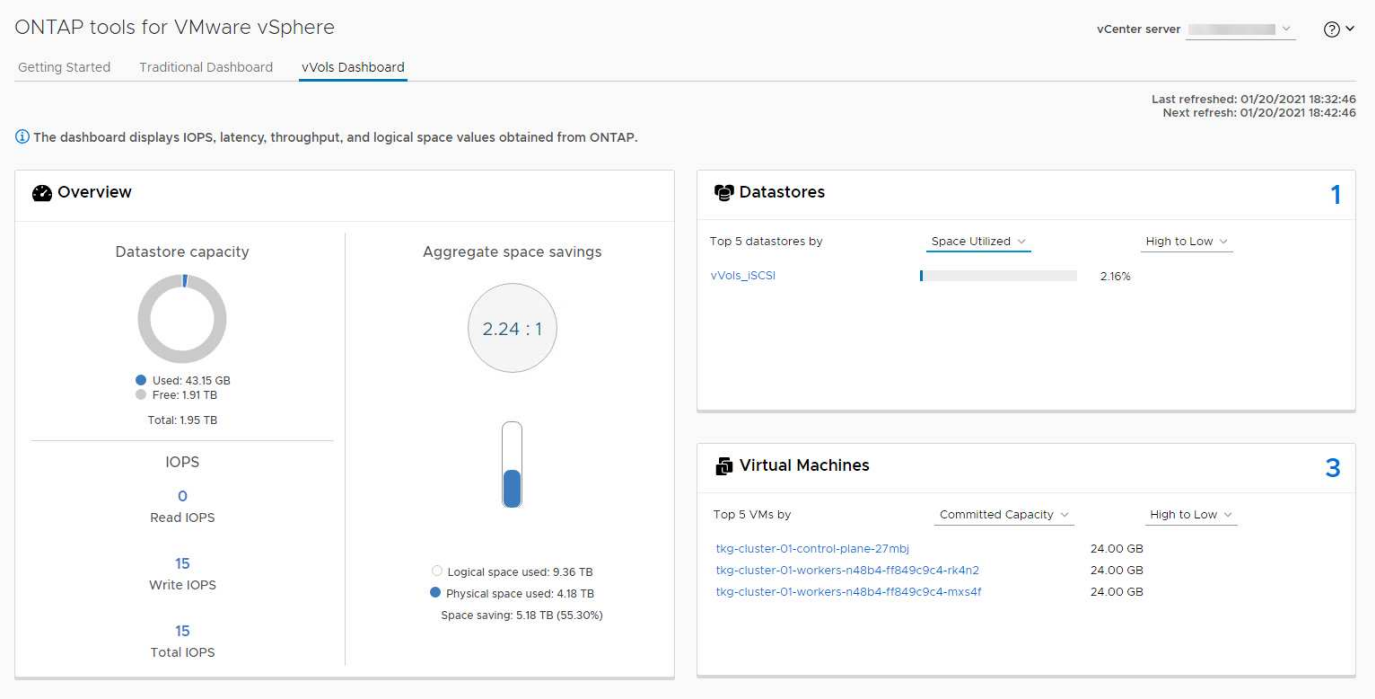
VMware vSphere APIs for Storage Awareness （ VASA ）を使用すると、ストレージ管理者は、明確に定義された機能を使用してデータストアを簡単に設定でき、 VM 管理者は、相互にやり取りすることなく、いつでも VM をプロビジョニングするためのこれらの機能を使用できます。

このアプローチを見て、仮想化ストレージの運用を合理化し、単純な作業の多くを回避する方法を確認することをお勧めします。

VASA が導入される前は、 VM 管理者が VM ストレージポリシーを定義することもできましたが、適切なデータストアを特定するには、多くの場合、ドキュメントや命名規則を使用する必要がありました。VASA を使用すると、ストレージ管理者は、パフォーマンス、階層化、暗号化、レプリケーションなど、さまざまなストレージ機能を定義できます。1 つのボリュームまたはボリュームセットの一連の機能を、ストレージ機能プロファイル（ SCP ）と呼びます。

SCPでは、VMのデータVVOLに対して最小または最大のQoSがサポートされます。最小 QoS は AFF システムでのみサポートされます。VMware vSphere 用の ONTAP ツールには、 ONTAP システム上の VVOL の VM の詳細なパフォーマンスと論理容量を表示するダッシュボードがあります。

次の図は、 VMware vSphere 9.8 VVol ダッシュボード用の ONTAP ツールを示しています。




ストレージ機能プロファイルを定義したら、そのプロファイルを使用して要件を定義するストレージポリシーを使用して VM をプロビジョニングできます。vCenter では、 VM ストレージポリシーとデータストアストレージ機能プロファイルのマッピングに基づいて、互換性があるデータストアのリストを選択対象として表示できます。このアプローチは、ストレージポリシーベースの管理と呼ばれます。

VASA は、ストレージを照会して一連のストレージ機能を vCenter に返すためのテクノロジを提供します。VASA ベンダープロバイダは、ストレージシステムの API およびコンストラクトと、 vCenter が認識可能な VMware API との間の変換機能を提供します。ネットアップのVASA Provider for ONTAPは、ONTAP Tools for VMware vSphereアプライアンスVMの一部として提供されます。vCenterプラグインは、VVOLデータストアをプロビジョニングおよび管理するためのインターフェイスと、ストレージ機能プロファイル（SCP）を定義する機能を提供します。

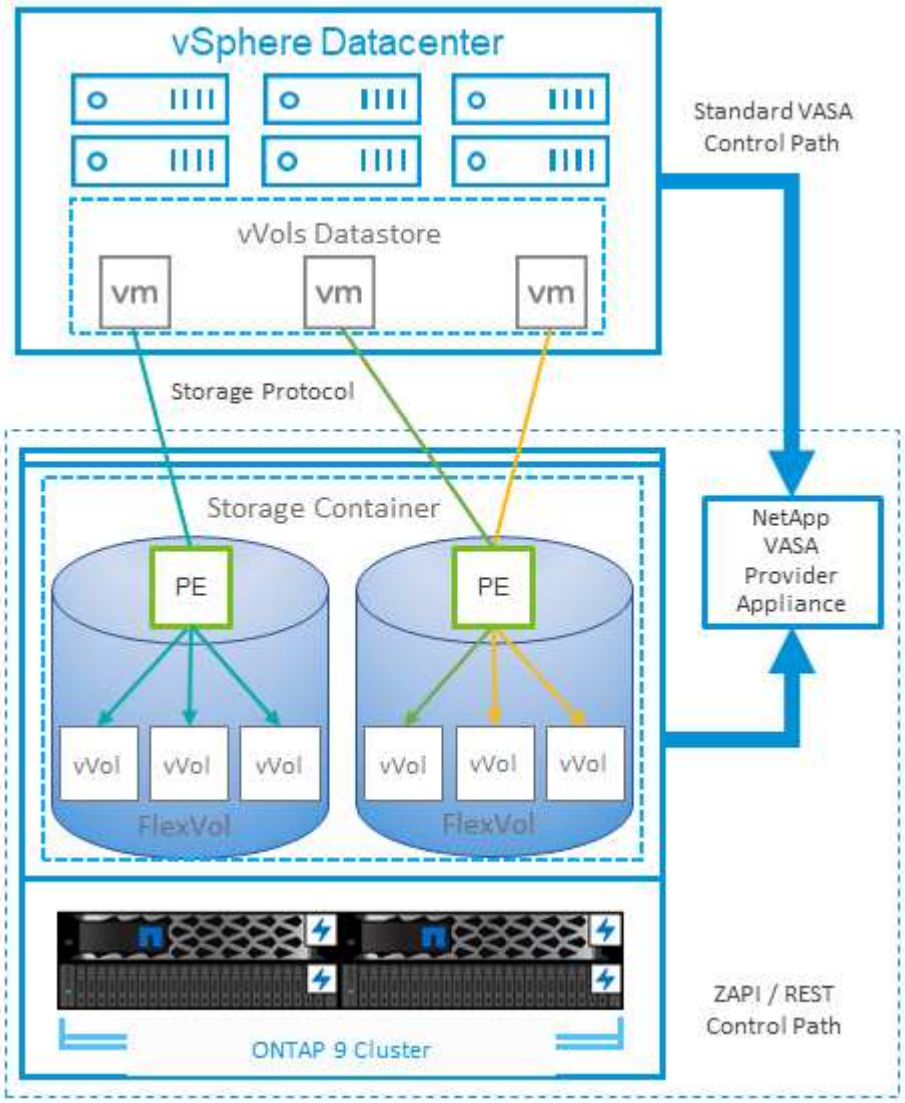
ONTAP は、 VMFS データストアと NFS データストアの両方をサポートしています。SAN データストアで VVOL を使用すると、 VM レベルのきめ細かさなど、 NFS のメリットの一部を活用できます。ここでは考慮すべきベストプラクティスをいくつか示します。また、追加情報はにあります "TR-4400"：

- VVOL データストアは、複数のクラスタノードにある複数の FlexVol で構成できます。ボリュームごとに機能が異なる場合でも、最もシンプルなアプローチは 1 つのデータストアです。SPBM により、互換性のあるボリュームが VM に使用されています。ただし、すべてのボリュームが 1 つの ONTAP SVM に含まれていて、単一のプロトコルでアクセスできる必要があります。各プロトコルでノードごとに 1 つの LIF で十分です。1 つの VVOL データストアで複数の ONTAP リリースを使用することは避けてください。リリースによってストレージ機能が異なる場合があります。
- VVol データストアの作成と管理には、 VMware vSphere プラグインの ONTAP ツールを使用します。データストアとそのプロファイルの管理に加え、必要に応じて、 VVOL にアクセスするためのプロトコルエンドポイントが自動的に作成されます。LUN を使用する場合、 LUN PE は 300 以上の LUN ID を使用してマッピングされます。ESXiホストの詳細なシステム設定を確認する `Disk.MaxLUN` 300を超えるLUN ID番号を許可します（デフォルトは1、024）。そのためには、vCenterでESXiホストを選択し、[Configure]タブで `Disk.MaxLUN` をクリックします。
- VASA Provider 、 vCenter Server （アプライアンスまたは Windows ベース）、または VMware vSphere 用の ONTAP ツールは相互に依存するため、 VVOL データストアにインストールしたり移行したりしないでください。これらのツールは、停電やその他のデータセンターの停止が発生した場合に管理しなくなる

ためです。

- VASA Provider VM を定期的にバックアップします。VASA Providerが格納された従来のデータストアのSnapshotを少なくとも1時間ごとに作成してください。VASA Provider の保護とリカバリの詳細については、こちらを参照してください "こちらの技術情報アーティクル"。

次の図は、 VVOL のコンポーネントを示しています。




## VMware Storage Distributed Resource Scheduler の略

VMware Storage Distributed Resource Scheduler （ SDRS ）は、現在の I/O レイテンシとスペース使用量に基づいて VM をストレージに配置する vSphere の機能です。

その後、 VM や VMDK の配置先として最適なデータストアをデータストアクラスタ内から選択し、システムを停止することなくデータストアクラスタ（ポッドとも呼ばれます）内のデータストア間で VM や VMDK を移動します。データストアクラスタは、類似するデータストアをvSphere管理者から見た単一の消費単位に集約したものです。

SDRSとONTAP tools for VMware vSphereを使用する場合は、まずプラグインを使用してデータストアを作成し、vCenterを使用してデータストアクラスタを作成してから、そのデータストアにデータストアを追加する

必要があります。データストアクラスタを作成したら、プロビジョニングウィザードの詳細ページからデータストアクラスタにデータストアを直接追加できます。

SDRS に関するその他の ONTAP のベストプラクティスは、次のとおりです。

- クラスタ内のすべてのデータストアで同じタイプのストレージ（ SAS 、 SATA 、 SSD など）を使用し、すべて VMFS データストアまたは NFS データストアとし、レプリケーションと保護の設定を同じにします。
- デフォルト（手動）モードでは SDRS の使用を検討してください。このアプローチでは、推奨事項を確認し、適用するかどうかを決定できます。VMDK の移行による影響を次に示します。
  - SDRS がデータストア間で VMDK を移動すると、 ONTAP のクローニングや重複排除によるスペース削減効果は失われます。重複排除機能を再実行すれば、削減効果を取り戻すことができます。
  - NetAppでは、VMDKを移動したあとに、移動したVMによってスペースがロックされるため、ソースデータストアでSnapshotを再作成することを推奨しています。
  - 同じアグリゲート上のデータストア間で VMDK を移動してもメリットはほとんどなく、 SDRS はアグリゲートを共有する可能性のある他のワークロードを可視化できません。

## 推奨される **ESXi** ホストとその他の **ONTAP** 設定

NetAppは、NFSプロトコルとブロックプロトコルの両方に最適なESXiホスト設定を開発しました。また、NetAppとVMwareの内部テストに基づいて、ONTAPで適切に動作するようにマルチパスとHBAタイムアウトを設定するための具体的なガイダンスも提供されます。

これらの値は、ONTAP tools for VMware vSphereを使用して簡単に設定できます。[Summary]ダッシュボードで、[Host Systems]ポートレットの[Edit Settings]をクリックするか、vCenterでホストを右クリックし、ONTAP tools]>[Set Recommended Values]に移動します。

ここでは、9.8~9.13リリースで推奨されるホスト設定を示します。

| ホスト設定 | ネットアップが推奨する値 | 再起動が必要です |
|---|---|---|
| * ESXi Advanced Configuration * | | |
| VMFS3.HardwareAcceleratedLocking | デフォルトのまま（1） | いいえ |
| VMFS3.EnableBlockDelete の 2 つのオプションがあります | デフォルト（0）のままにしますが、必要に応じて変更できます。詳細については、を参照してください "VMware KB 2007427" | いいえ |
| VMFS3.EnableVMFS6Unmap | デフォルトのまま（1）<br>詳細については、を参照してください "VMware vSphere API：アレイ統合（VAAI）" | いいえ |
| * NFS設定* | | |
| Net.TcpipHeapSize の場合 | vSphere 6.0 以降： 32 に設定<br>他のすべてのNFS設定の場合は、30に設定されます | はい。 |

| | | |
|---|---|---|
| Net.TcpipHeapMax | vSphere 6.Xのほとんどのリリースでは512 MBに設定されています。6.5U3、6.7U3、7.0以降の場合は、1024MBに設定します。 | はい。 |
| NFS.MaxVolumes の場合 | vSphere 6.0以降：256に設定その他のNFS構成はすべて64に設定されます。 | いいえ |
| NFS41.MaxVolumes | vSphere 6.0 以降では、 256 に設定されます。 | いいえ |
| NFS.MaxQueueDepth^1 ^ | vSphere 6.0以降では、128に設定されます | はい。 |
| NFS.HeartbeatMaxFailures の略 | すべてのNFS設定について、10に設定されます | いいえ |
| nfs.HeartbeatFrequency | すべてのNFS構成で12に設定 | いいえ |
| nfs.HeartbeatTimeout | すべてのNFS構成で5に設定されます。 | いいえ |
| SunRPC.MaxConnPerIP | vSphere 7.0 以降では 128 に設定されます。 | いいえ |
| * FC / FCoE 設定 * | | |
| パス選択ポリシー | FC パスの ALUA を使用する場合は、 RR （ラウンドロビン）に設定されます。それ以外の構成では、すべて FIXED に設定されます。<br>この値を RR に設定すると、最適化されたすべてのアクティブなパスで負荷を分散できます。<br>FIXED は、 ALUA に対応していない従来の構成用の値で、プロキシ I/O を防止できますつまり、Data ONTAP 7-Modeを実行する環境でハイアベイラビリティ（HA）ペアの他方のノードにI/Oが送られないようにすることができます | いいえ |
| Disk.QFullSampleSize | すべての構成で 32 に設定されます。<br>この値を設定すると、 I/O エラーの防止に役立ちます。 | いいえ |
| Disk.qFullThreshold | すべての構成で 8 に設定します。<br>この値を設定すると、 I/O エラーの防止に役立ちます。 | いいえ |
| Emulex FC HBA タイムアウト | デフォルト値を使用します。 | いいえ |
| QLogic FC HBA タイムアウト | デフォルト値を使用します。 | いいえ |
| * iSCSI 設定 * | | |

| | | |
|---|---|---|
| パス選択ポリシー | すべての iSCSI パスで RR （ラウンドロビン）に設定されます。<br>この値を RR に設定すると、最適化されたすべてのアクティブなパスで負荷を分散できます。 | いいえ |
| Disk.QFullSampleSize | すべての構成で 32 に設定されます。<br>この値を設定すると、I/Oエラーの防止に役立ちます | いいえ |
| Disk.qFullThreshold | すべての構成で 8 に設定します。<br>この値を設定すると、 I/O エラーの防止に役立ちます。 | いいえ |

VMware vSphere ESXi 7.0.1およびVMware vSphere ESXi 7.0.2を使用する場合、1-NFSの高度な設定オプションMaxQueueDepthが想定どおりに機能しないことがあります。参照してください "VMware KB 86331" を参照してください。

ONTAP ツールでは、 ONTAP FlexVol および LUN の作成時に特定のデフォルト設定も指定されます。

| * ONTAP ツール* | デフォルト設定 |
|---|---|
| Snapshot リザーブ（ -percent-snapshot-space ） | 0 |
| フラクショナルリザーブ（ -fractional-reserve ） | 0 |
| アクセス時間の更新（ -atime-update ） | いいえ |
| 最小限の先読み（ -min-readahead ） | いいえ |
| スケジュールされたSnapshot | なし |
| ストレージ効率 | 有効 |
| ボリュームギャランティ | なし（シンプロビジョニング） |
| ボリュームのオートサイズ | grow_shrink |
| LUN のスペースリザベーション | 無効 |
| LUN スペースの割り当て | 有効 |

ハフオマンスノマルチハスセツテイ

現在使用可能なONTAPツールでは設定されていませんが、NetAppでは次の設定オプションを推奨しています。

- ハイパフォーマンスな環境で、または単一の LUN データストアでパフォーマンスをテストする場合は、ラウンドロビン（ VMW_PSP_RR ）パス選択ポリシー（ PSP ）の負荷分散設定をデフォルトの IOPS 設定 1000 から 1 に変更することを検討します。VMware の技術情報を参照 "2069356" 詳細については、
- vSphere 6.7 Update 1 では、 VMware がラウンドロビン PSP 用に新しいレイテンシの負荷分散メカニズムを導入しました。新しいオプションでは、 I/O に最適なパスを選択する際に、 I/O 帯域幅とパスレイテンシが考慮されますパス接続が異なる環境（あるパスのネットワークホップ数が別のパスよりも多い場合など）や、NetAppオールSANアレイシステムを使用している場合など、パス接続が同等でない環境で使用するとメリットがあります。を参照してください "パス選択プラグインとポリシー" を参照してください。

その他のドキュメント

vSphere 7を使用するFCPおよびiSCSIの詳細については、を参照してください。 "VMware vSphere 7.xとONTAPの併用"
vSphere 8を使用するFCPおよびiSCSIの詳細については、を参照してください。 "VMware vSphere 8.xとONTAPの併用"
vSphere 7を使用したNVMe-oFの詳細については、を参照してください。 "NVMe-oFの詳細については、「NVMe-oFホスト構成（ESXi 7.x with ONTAP）」を参照してください。"
vSphere 8を使用したNVMe-oFの詳細については、を参照してください。 "NVMe-oFの詳細については、「NVMe-oFホスト構成（ESXi 8.x with ONTAP）」を参照してください。"

# ONTAPを備えた仮想ボリューム（VVOL）

## 概要

ONTAPは、20年以上にわたって業界をリードするVMware vSphere環境向けストレージ解決策であり、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。

本ドキュメントでは、VMware vSphere Virtual Volumes（VVOL）向けのONTAP 機能について説明します。最新の製品情報やユースケース、導入を合理化してエラーを削減するためのベストプラクティスなどを紹介します。

このドキュメントは、これまでに公開されていたテクニカルレポート_TR-4400：『VMware vSphere Virtual Volumes（vVol）with ONTAP _』を差し替えます。

ベストプラクティスは、ガイドや互換性リストなどの他のドキュメントを補うものです。ラボテストに基づいて開発されており、ネットアップのエンジニアやお客様は広範な現場経験を積んでいます。効果的またはサポートされている唯一の手法ではないかもしれませんが、一般的には、ほとんどのお客様のニーズを満たす最もシンプルなソリューションです。

本ドキュメントが更新され、vSphere 8.0 Update 1に搭載された新しいvVol機能がONTAP tools 9.12リリースでサポートされるようになりました。

### Virtual Volumes（VVol）の概要

ネットアップは2012年にVMwareとの連携を開始し、vSphere APIs for Storage Awareness（VASA）for vSphere 5のサポートを開始しました。この初期のVASA Providerでは、プロファイルにストレージ機能を定義することができました。このプロファイルを使用すると、プロビジョニング時やポリシーへの準拠状況の確認時にデータストアをフィルタリングできます。時間の経過とともに、プロビジョニングの自動化を可能にする新しい機能が追加されたり、仮想ボリューム（VVol）が追加されたりして、個 々 のストレージオブジェクトが仮想マシンファイルと仮想ディスクに使用されたりします。これらのオブジェクトにはLUN、ファイルなどが含まれます。vSphere 8 - NVMe namespaces.NetAppは、2015年にvSphere 6でリリースされたVVOLのリファレンスパートナーとして、またvSphere 8でNVMe over Fabricsを使用したVVOLの設計パートナーとして、VMwareと緊密に連携しています。ネットアップでは、ONTAP の最新機能を活用できるように、VVOLの機能を継続的に強化しています。

注意が必要なコンポーネントは次のとおりです。

| * VASA Provider * |
| --- |

| |
|---|
| VMware vSphereとストレージシステムの間の通信を処理するソフトウェアコンポーネントです。ONTAP の場合、VASA ProviderはONTAP Tools for VMware vSphere（ONTAP tools for VMware vSphere）と呼ばれるアプライアンスで実行されます。ONTAP toolsには、vCenterプラグイン、VMware Site Recovery Manager用のStorage Replication Adapter（SRA）、独自の自動化を構築するためのREST APIサーバも含まれています。ONTAP toolsを設定してvCenterに登録すると、ONTAP システムを直接操作する必要はほとんどなくなります。これは、必要なストレージのほぼすべてをvCenter UIから直接、またはREST APIによる自動化を通じて管理できるためです。 |
| プロトコルエンドポイント（**PE**） |
| プロトコルエンドポイントは、ESXiホストとVVOLデータストアの間のI/Oのプロキシです。ONTAP VASA Providerは、VVOLデータストアのFlexVolごとに1つのプロトコルエンドポイントLUN（サイズ4MB）、またはデータストア内のFlexVolボリュームをホストしているストレージノードのNFSインターフェイス（LIF）ごとに1つのNFSマウントポイントを自動的に作成します。ESXiホストでは、これらのプロトコルエンドポイントは、個 々 のVVOL LUNや仮想ディスクファイルではなく直接マウントされます。プロトコルエンドポイントは、必要なインターフェイスグループやエクスポートポリシーとともにVASA Providerによって自動的に作成、マウント、アンマウント、および削除されるため、管理する必要はありません。 |
| 仮想プロトコルエンドポイント（**VPE**） |
| vSphere 8の新機能では、VVOLでNVMe over Fabrics（NVMe-oF）を使用する場合、プロトコルエンドポイントの概念はONTAP には関係ありません。代わりに、最初のVMの電源がオンになるとすぐに、各ANAグループのESXiホストによって仮想PEが自動的にインスタンス化されます。ONTAP では、データストアで使用されるFlexVol ボリュームごとにANAグループが自動的に作成されます。<br><br>VVOLにNVMe-oFを使用するもう1つの利点は、VASA Providerでバインド要求が不要であることです。代わりに、VVOLバインド機能はVPEに基づいてESXiホストが内部的に処理します。これにより、VVolのバインドストームがサービスに影響する可能性が低くなります。<br><br>詳細については、を参照してください "NVMeと仮想ボリューム" オン "VMware.com" |
| 仮想ボリュームデータストア |
| 仮想ボリュームデータストアは、VASA Providerで作成および管理されるVVolコンテナを表す論理データストアです。コンテナは、VASA Providerで管理されるストレージシステムからプロビジョニングされたストレージ容量のプールを表します。ONTAP toolsでは、1つのvVolデータストアに複数のFlexVol ボリューム（バッキングボリューム）を割り当てることができます。これらのvVolデータストアは、機能の異なるフラッシュシステムとハイブリッドシステムを組み合わせることで、ONTAP クラスタ内の複数のノードにまたがることができます。管理者は、プロビジョニングウィザードまたはREST APIを使用して新しいFlexVol ボリュームを作成できます。また、作成済みのFlexVol ボリュームがある場合は、元のストレージ用に選択できます。 |
| 仮想ボリューム（**VVol**） |
| VVOLは、VVOLデータストアに格納される実際の仮想マシンのファイルとディスクです。VVOL（単一）という用語は、単一の特定のファイル、LUN、またはネームスペースを指します。ONTAP は、データストアが使用するプロトコルに応じて、NVMeネームスペース、LUN、またはファイルを作成します。VVOLにはいくつかの異なるタイプがあり、最も一般的なものは、Config（メタデータファイル）、Data（仮想ディスクまたはVMDK）、Swap（VMの電源投入時に作成）です。VMware VM暗号化で保護されるvVolのタイプはOTHERになります。VMware VMの暗号化とONTAP ボリュームまたはアグリゲートの暗号化を混同しないでください。 |

ポリシーベースの管理

VMware vSphere APIs for Storage Awareness（VASA）を使用すると、VM管理者は、ストレージチームとやり取りすることなく、VMのプロビジョニングに必要なストレージ機能を簡単に使用できます。VASAがリリー

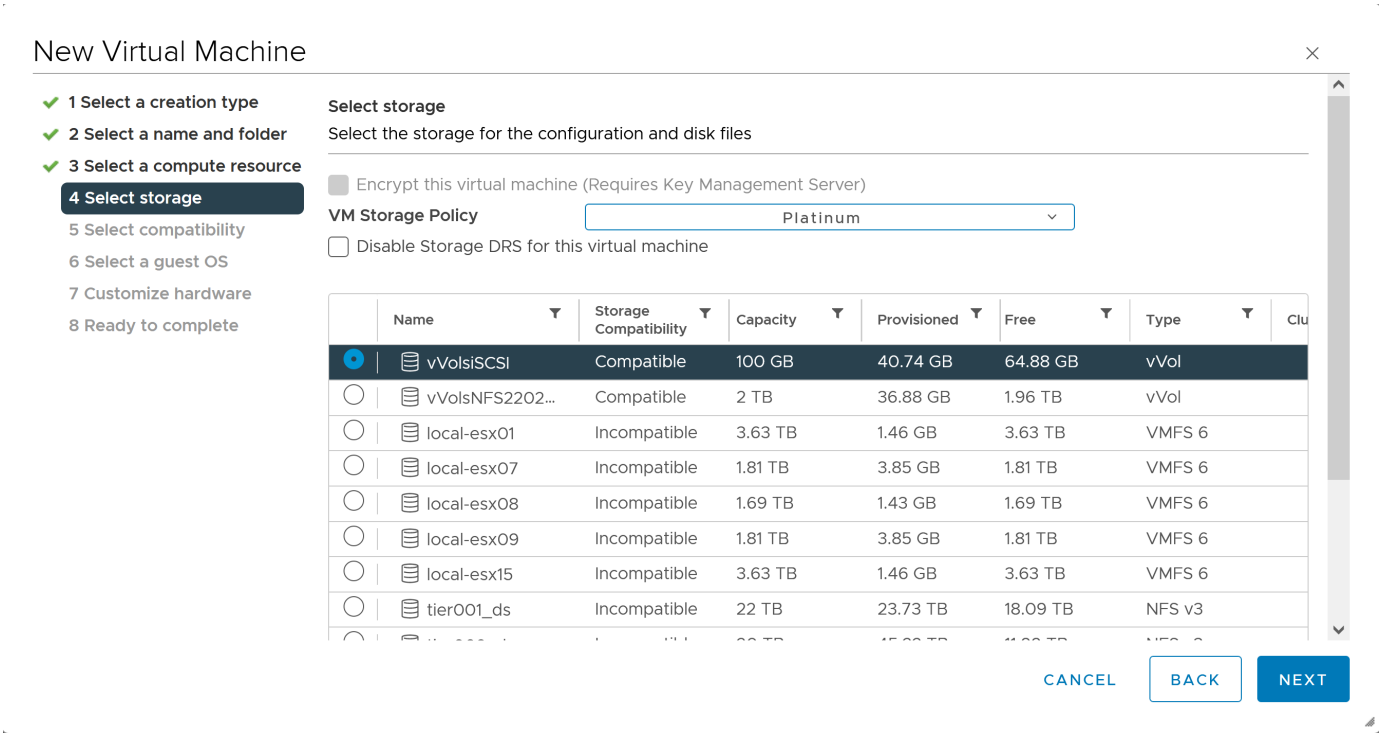
スされるまではVM管理者はVMストレージポリシーを定義できましたが、適切なデータストアを特定するためにはストレージ管理者と協力しなければなりませんでした。多くの場合、ドキュメントや命名規則を使用していました。VASAを使用すると、適切な権限を持つvCenter管理者は、vCenterユーザがVMのプロビジョニングに使用できる一連のストレージ機能を定義できます。VMストレージポリシーとデータストアストレージ機能プロファイルのマッピングにより、vCenterで互換性のあるデータストアのリストを表示して選択できるほか、ARIA（旧vRealize）AutomationやTanzu Kubernetes Gridなどの他のテクノロジを有効にして、割り当てられたポリシーからストレージを自動的に選択できます。このアプローチは、ストレージポリシーベースの管理と呼ばれます。ストレージ機能プロファイルとポリシーは従来のデータストアでも使用できますが、ここではVVOLデータストアに焦点を当てます。

次の2つの要素があります。

| ストレージ機能プロファイル（**SCP**） |
| --- |
| ストレージ機能プロファイル（SCP）は、ストレージテンプレートの形式です。これを使用すると、vCenterの管理者は、ONTAP でのそれらの機能の管理方法を実際に理解していなくても、必要なストレージ機能を定義できます。テンプレート形式のアプローチを採用することで、管理者は一貫した予測可能な方法でストレージサービスを簡単に提供できます。SCPで説明される機能には、パフォーマンス、プロトコル、Storage Efficiencyなどがあります。特定の機能はバージョンによって異なります。vCenter UIのONTAP Tools for VMware vSphereメニューを使用して作成します。REST APIを使用してSCPを作成することもできます。個々 の機能を選択して手動で作成することも、既存の（従来の）データストアから自動的に生成することもできます。 |
| * VMストレージポリシー* |
| 仮想マシンストレージポリシーは、vCenterの[Policies and Profiles]に作成されます。VVOLの場合は、NetApp VVOLストレージタイププロバイダから提供されるルールを使用してルールセットを作成します。ONTAP ツールを使用すると、個別のルールを強制的に指定するのではなく、SCPを選択するだけでシンプルなアプローチが可能になります。 |

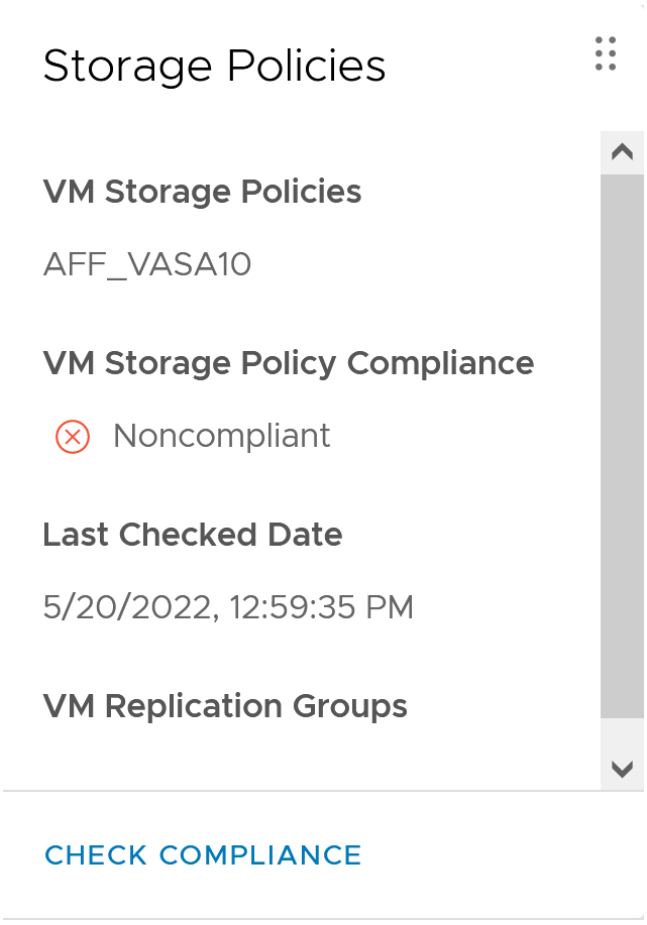
前述したように、ポリシーを使用すると、ボリュームのプロビジョニングタスクを合理化できます。適切なポリシーを選択するだけで、そのポリシーをサポートするvVolデータストアがVASA Providerに表示され、準拠している個 々 のFlexVol にvVolが配置されます（図1）。

ストレージポリシーを使用して**VM**を導入します




VMのプロビジョニングが完了すると、VASA Providerは準拠状況を継続的にチェックし、元のボリュームがポリシーに準拠しなくなったときにvCenterでアラームを生成してVM管理者に通知します（図2）。

**VM**ストレージポリシーへの準拠



## NetApp VVOLのサポート

ONTAPは、2012年の最初のリリースからVASA仕様をサポートしています。他のネットアップストレージシステムがVASAをサポートしている場合もありますが、本ドキュメントでは、現在サポートされているONTAP 9のリリースを中心に説明します。

### ONTAP

NetAppは、AFF、ASA、FASシステムでのONTAP 9に加えて、ONTAP SelectでのVMwareワークロード、VMware Cloud on AWSでのAmazon FSx for NetApp、Azure VMware解決策でのNetApp、Google Cloud VMware EngineでのCloud Volumes Service、EquinixでのAzure NetApp Filesプライベートストレージをサポートしています。 ただし、特定の機能は、サービスプロバイダーおよび使用可能なネットワーク接続によって異なる場合があります。vSphereゲストから、これらの構成に格納されたデータやCloud Volumes ONTAPにアクセスすることもできます。

本書の発行時点では、ハイパースケーラ環境は従来のNFS v3データストアに限定されているため、VVOLは、オンプレミスのONTAP システム、または世界中のネットアップパートナーやサービスプロバイダがホストするオンプレミスシステムのすべての機能を提供するクラウド接続システムでのみ使用できます。

ONTAP の詳細については、を参照してください "ONTAP 製品ドキュメント"_

ONTAP およびVMware vSphereのベストプラクティスの詳細については、を参照してください "TR-4597"_

## ONTAPでVVOLを使用するメリット

2015年にVMwareがVASA 2.0でVVOLをサポートするようになったとき、VMwareは「外付けストレージ（SAN / NAS）の新しい運用モデルを提供する統合管理フレームワーク」と表現しました。 この運用モデルには、ONTAP ストレージと組み合わせるメリットがいくつかあります。

#### ポリシーベースの管理

セクション1.2で説明したように、ポリシーベースの管理では、事前定義されたポリシーを使用してVMをプロビジョニングし、その後管理できます。これは、次のようなさまざまな方法でITの運用に役立ちます。

- 高速化。 ONTAP ツールにより、vCenter管理者がストレージプロビジョニング作業のためにストレージチームとチケットをオープンする必要がなくなります。ただし、vCenterとONTAP システムのONTAP tools RBACロールでは、必要に応じて特定の機能へのアクセスを制限することで、独立したチーム（ストレージチームなど）や同じチームによる独立したアクティビティを許可できます。
- *よりスマートなプロビジョニング。*ストレージシステムの機能をVASA APIを通じて公開できるため、VM管理者がストレージシステムの管理方法を理解しなくても、プロビジョニングワークフローで高度な機能を活用できます。
- プロビジョニングの高速化。 1つのデータストアでさまざまなストレージ機能をサポートし、VMポリシーに基づいてVMに応じて自動的に選択できます。
- *間違いを避けてください。*ストレージとVMのポリシーは事前に開発され、必要に応じて適用されます。VMをプロビジョニングするたびにストレージをカスタマイズする必要はありません。コンプライアンスアラームは、定義されたポリシーからストレージ機能が逸脱すると生成されます。前述したように、SCPは初期プロビジョニングを予測可能かつ反復可能にし、SCPに基づいてVMストレージポリシーを設定することで正確な配置を保証します。
- 容量管理の向上。 VASAおよびONTAP ツールを使用すると、必要に応じてストレージ容量を業界単位のアグリゲートレベルまで表示し、容量が不足し始めた場合に複数のレイヤからアラートを受け取ることができます。

### 最新の**SAN**で**VM**をきめ細かく管理

VMwareでは、ファイバチャネルとiSCSIを使用するSANストレージシステムが最初にESX向けにサポートされましたが、ストレージシステムから個 々 のVMファイルとディスクを管理する機能はありませんでした。代わりに、LUNがプロビジョニングされ、VMFSが個 々 のファイルを管理します。そのため、個 々 のVMストレージのパフォーマンス、クローニング、保護をストレージシステムで直接管理することは困難です。VVOLは、ONTAP の堅牢でパフォーマンスに優れたSAN機能により、NFSストレージを使用しているお客様がすでに利用しているストレージをきめ細かく制御します。

現在、vSphere 8とONTAP Tools for VMware vSphere 9.12以降では、従来のSCSIベースのプロトコルにVVOLで使用されていたきめ細かな制御機能が、NVMe over Fabricsを使用した最新のファイバチャネルSANで利用できるようになり、大規模環境でのパフォーマンスをさらに向上させることができます。vSphere 8.0 Update 1では、ハイパーバイザーストレージスタックでI/O変換を行うことなく、VVOLを使用して完全なエンドツーエンドのNVMe解決策 を導入できるようになりました。

### 優れたストレージオフロード機能

VAAIにはさまざまな処理がストレージにオフロードされますが、VASA Providerで対処できるギャップがいくつかあります。SAN VAAIでは、VMwareが管理するスナップショットをストレージシステムにオフロードできません。NFS VAAIはVM管理スナップショットをオフロードできますが、ストレージネイティブスナップショットを持つVMには制限事項があります。VVOLでは、個 々 のLUN、ネームスペース、または仮想マシンディスク用のファイルが使用されるため、ONTAP ではファイルやLUNのクローンを迅速かつ効率的に作成し、差分ファイルが不要になったVM単位のSnapshotを作成できます。NFS VAAIは、Storage vMotionのホット（電源をオンにした）移行用のクローン処理のオフロードもサポートしていません。従来のNFSデータストアでVAAIを使用する場合は、VMの電源をオフにして移行のオフロードを可能にする必要があります。ONTAPツールのVASA Providerを使用すると、ストレージ効率に優れたクローンをほぼ瞬時にホットデータとコールドデータの移行に使用できます。また、ほぼ瞬時にコピーを作成してVVOLのボリュームをまたがって移行することもできます。Storage Efficiencyにはこれらの大きなメリットがあるため、でVVOLワークロードを最大限に活用できる場合があります "容量削減保証" プログラム。同様に、VAAIを使用したボリューム間クローンで要件を満たせない場合は、VVOLでのコピー操作の向上により、ビジネス上の課題を解決できる可能性があります。

### **VVOL**の一般的なユースケース

これらのメリットに加えて、VVOLストレージの一般的なユースケースを次に示します。

- 仮想マシンのオンデマンドプロビジョニング
  - プライベートクラウドまたはサービスプロバイダのIaaS：
  - ARIA（旧称vRealize）スイートやOpenStackなどによる自動化とオーケストレーションを活用できます
- ファーストクラスディスク（**FCD**）
  - VMware Tanzu Kubernetes Grid [TKG]の永続ボリューム。
  - 独立したVMDKライフサイクル管理を通じてAmazon EBSに似たサービスを提供
- 一時**VM**のオンデマンドプロビジョニング
  - テスト/開発ラボ
  - トレーニング環境

#### VVOLの一般的なメリット

VVOLを最大限に活用すると（上記のユースケースなど）、具体的に次のような機能強化が実現します。

- クローンは、1つのボリューム内またはONTAP クラスタ内の複数のボリューム間ですばやく作成されます。これは、VAAIが有効な従来のクローンと比較して有利です。また、ストレージ効率にも優れています。ボリューム内のクローンには、ONTAPファイルクローンが使用されます。FlexCloneボリュームと同様に、ソースのVVOLファイル/ LUN /ネームスペースからの変更のみが格納されます。本番環境やその他のアプリケーションを目的とした長期的なVMを短時間で作成し、最小限のスペースでVMレベルの保護（VMware vSphere向けNetApp SnapCenter プラグイン、VMware管理スナップショットまたはVADPバックアップを使用）とパフォーマンス管理（ONTAP QoSを使用）を実現できます。
- VVOLは、vSphere CSIでTKGを使用する場合に理想的なストレージテクノロジであり、vCenter管理者が管理する個別のストレージクラスと容量を提供します。
- Amazon EBSに似たサービスは、FCDを介して提供できます。FCD VMDKは、その名前が示すように、vSphereのファーストクラスの市民であり、ライフサイクルが割り当てられているVMとは別に個別に管理できるためです。

## ONTAP でVVOLを使用する

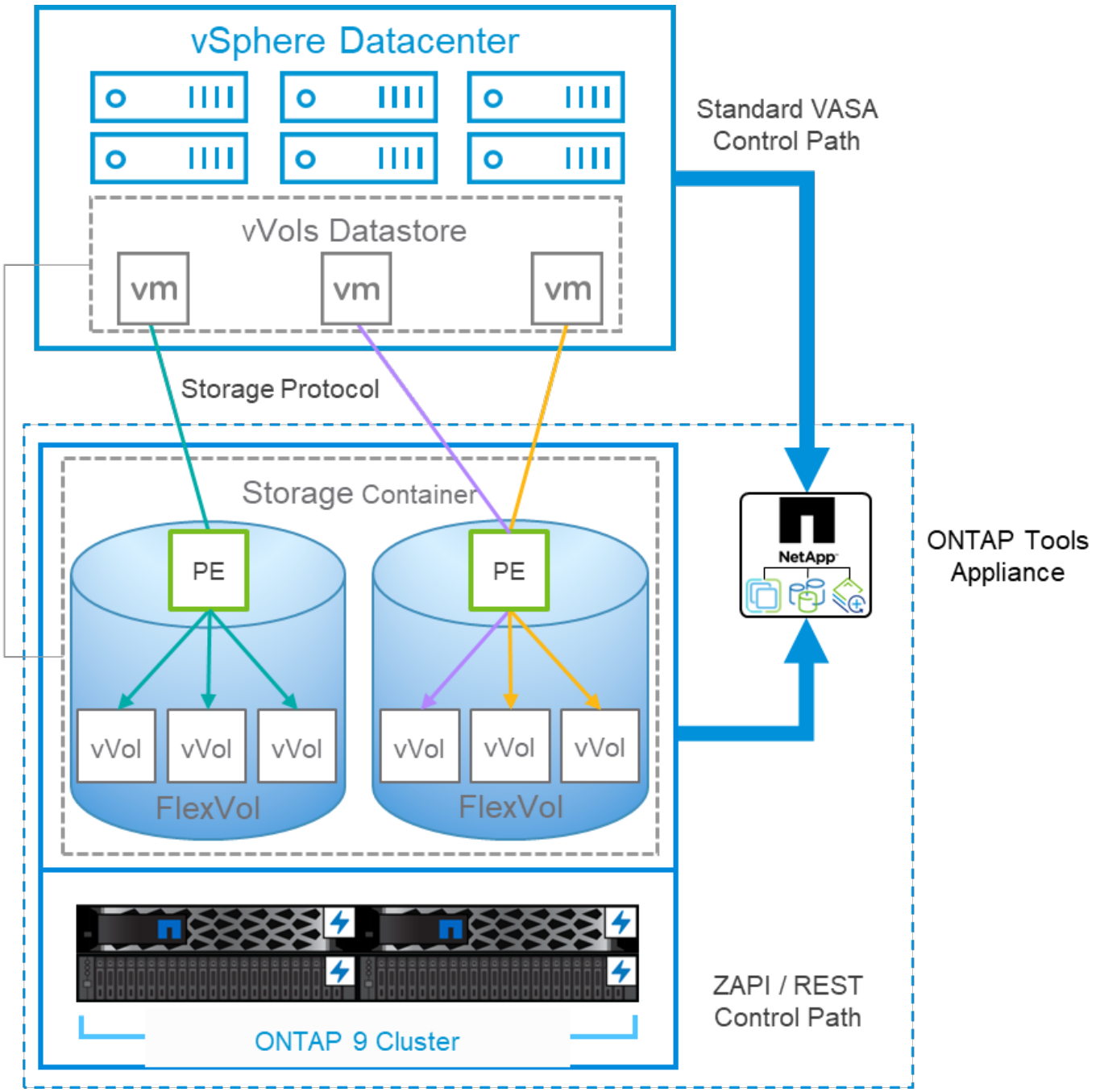
### VVOLをONTAP で使用するための鍵は、ONTAP Tools for VMware vSphere仮想アプライアンスに含まれているVASA Providerソフトウェアです。

ONTAP ツールには、vCenter UI拡張機能、REST APIサーバ、Storage Replication Adapter for VMware Site Recovery Manager、Monitoring and Host構成ツール、VMware環境の管理に役立つ一連のレポートも含まれています。

#### 製品およびドキュメント

ONTAPでVVOLを使用するために必要な追加製品は、ONTAP Oneに付属のONTAP FlexCloneライセンスとONTAP toolsアプライアンスだけです。最近リリースされたONTAP toolsは、ESXi上で動作する単一の統合アプライアンスとして提供され、これまで3種類のアプライアンスとサーバの機能を提供します。VVOLの場合、vSphereのONTAP 機能の一般的な管理ツールおよびユーザインターフェイスとして、ONTAP toolsのvCenter UI拡張機能またはREST APIを、特定のVVOL機能を提供するVASA Providerとともに使用することが重要です。SRAコンポーネントは従来のデータストアに含まれていますが、VMware Site Recovery ManagerはvVolにSRAを使用せず、代わりにvVolレプリケーションにVASAプロバイダを利用する新しいサービスをSRM 8.3以降に実装します。

#### iSCSIまたはFCPを使用する場合のONTAP tools VASA Providerのアーキテクチャ




製品のインストール

新規インストールの場合は、仮想アプライアンスをvSphere環境に導入します。現在のリリースのONTAP toolsは自動的にvCenterに登録され、VASA Providerがデフォルトで有効になります。ESXiホストとvCenter Serverの情報に加えて、アプライアンスのIPアドレス設定の詳細も必要です。前述したように、VVOLに使用するすべてのONTAP クラスタには、ONTAP FlexCloneライセンスがあらかじめインストールされている必要があります。アプライアンスには可用性を確保するためのwatchdogが組み込まれています。ベストプラクティスとして、VMwareの高可用性機能とオプションのフォールトトレランス機能を使用して設定する必要があります。詳細については、セクション4.1を参照してください。ONTAP toolsアプライアンスまたはvCenter Serverアプライアンス（vCSA）をvVolストレージにインストールしたり移動したりしないでください。アプライアンスが再起動しない可能性があります。

ONTAP ツールのインプレースアップグレードは、NetApp Support Site （NSS）からダウンロードできるアップグレードISOファイルを使用してサポートされます。導入およびセットアップガイドの手順に従って、アプ

ライアンスをアップグレードします。

仮想アプライアンスのサイジングと構成の制限については、次のナレッジベースの記事を参照してください。
"『Sizing Guide for ONTAP tools for VMware vSphere』を参照してください"

製品ドキュメント

ONTAP ツールの導入に役立つ次のドキュメントを参照してください。

"完全なドキュメントリポジトリについては、次のリンクを参照してください。docs.netapp.com"

はじめに

- "リリースノート"
- "ONTAP Tools for VMware vSphereについて説明します"
- "ONTAP ツールクイックスタート"
- "ONTAP ツールを導入"
- "ONTAP ツールをアップグレードする"

**ONTAP** ツールを使用する

- "従来のデータストアをプロビジョニングする"
- "vVol データストアをプロビジョニングする"
- "ロールベースアクセス制御を設定する"
- "リモート診断を設定します"
- "ハイアベイラビリティを設定する"

データストアの保護と管理

- "従来のデータストアを保護" SRMを使用
- "VVOLベースの仮想マシンを保護" SRMを使用
- "従来のデータストアと仮想マシンを監視する"
- "VVol データストアと仮想マシンを監視する"

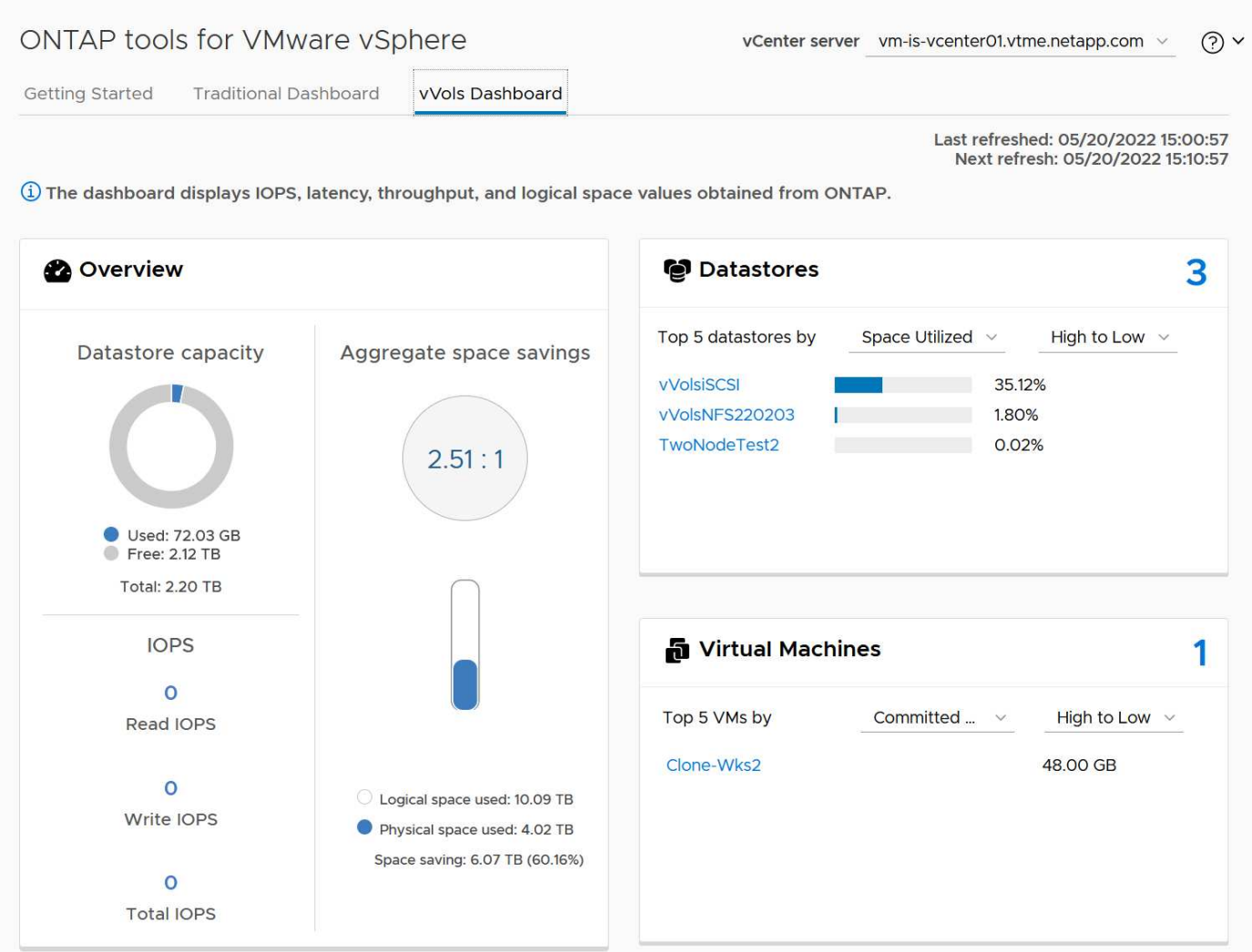
製品ドキュメント以外にも、役立つサポート技術情報アーティクルがあります。

- "『How to perform a VASA Provider Disaster Recovery - Resolution Guide』"

**VASA Provider**ダッシュボード

VASA Providerには、個 々 のvVol VMのパフォーマンスと容量の情報が表示されたダッシュボードがあります。この情報は、VVOLファイルおよびLUNのONTAP から直接取得されます。上位5つのVMのレイテンシ、IOPS、スループット、アップタイム、上位5つのデータストアのレイテンシとIOPSなどが含まれます。ONTAP 9.7以降を使用している場合はデフォルトで有効になります。初期データが取得されてダッシュボードに表示されるまで、最大で30分かかることがあります。

**ONTAP tools vVolダッシュボード**




ベストプラクティス

vSphereでONTAP vVolを使用するのは簡単で、公開されているvSphereのメソッドに従います（使用しているバージョンのESXiに対応するVMwareのドキュメントの「vSphere Storage」の「Working with Virtual Volumes」を参照してください）。ここでは、ONTAP と併せて考慮すべき追加のプラクティスをいくつか紹介します。

制限

一般に、ONTAP でサポートされるVVOLの制限は、VMwareで定義されています（公開されているを参照） "構成の最大値"）。次の表は、ONTAP 固有のVVOLのサイズと数の制限をまとめたものです。必ずをチェックしてください "NetApp Hardware Universe の略" LUNとファイルの数とサイズの制限を更新

- ONTAP vVolの制限*

| 容量 / 機能 | **SAN（SCSIまたはNVMe-oF）** | **NFS** |
|---|---|---|
| vVolの最大サイズ | 62TiB * | 62TiB * |
| FlexVol あたりの最大VVol数 | 一、〇 二四 | 20億です |

| 容量 / 機能 | **SAN（SCSI**または**NVMe-oF）** | **NFS** |
| --- | --- | --- |
| ONTAP ノードあたりの最大VVol数 | 最大12,288 ** | 500億です |
| ONTAP ペアあたりの最大VVol数 | 最大24,576 ** | 500億です |
| ONTAP クラスタあたりの最大VVol数 | 最大98,304 ** | 特定のクラスタ制限はありません |
| 最大QoSオブジェクト（共有ポリシーグループと個 々 のvVolサービスレベル） | ONTAP 9.3では12、000、ONTAP 9.4以降では40、000 | |

- サイズ制限はASA システム、またはONTAP 9.12.1P2以降を実行するAFF およびFAS システムによって異なります。
  - SAN vVol（NVMeネームスペースまたはLUN）の数はプラットフォームによって異なります。必ずをチェックしてください "NetApp Hardware Universe の略" LUNとファイルの数とサイズの制限を更新
- ONTAP ツールfor VMware vSphereのUI拡張機能またはREST APIを使用して、VVOLデータストア*およびプロトコルエンドポイントをプロビジョニングします。*

VVOLデータストアは一般的なvSphereインターフェイスを使用して作成することもできますが、ONTAPツールを使用すると、必要に応じてプロトコルエンドポイントが自動的に作成されます。また、ONTAPのベストプラクティスに従って、定義されたストレージ機能プロファイルに準拠したFlexVolボリュームが作成されます。ホスト/クラスタ/データセンターを右クリックし、ONTAP tools_and_Provision datastores_を選択します。ウィザードで目的のvVolオプションを選択するだけです。

- ONTAP Toolsアプライアンスまたはv Center Server Appliance（vCSA）は、管理対象のVVOLデータストアには絶対に保存しないでください。*

その結果、アプライアンスのリブートが必要になった場合、リブート中に自身のVVOLを再バインドできないため、アプライアンスのリブートが必要になることがあります。これらのデータは、別のONTAP ツールとvCenter環境で管理されるvVolデータストアに格納できます。

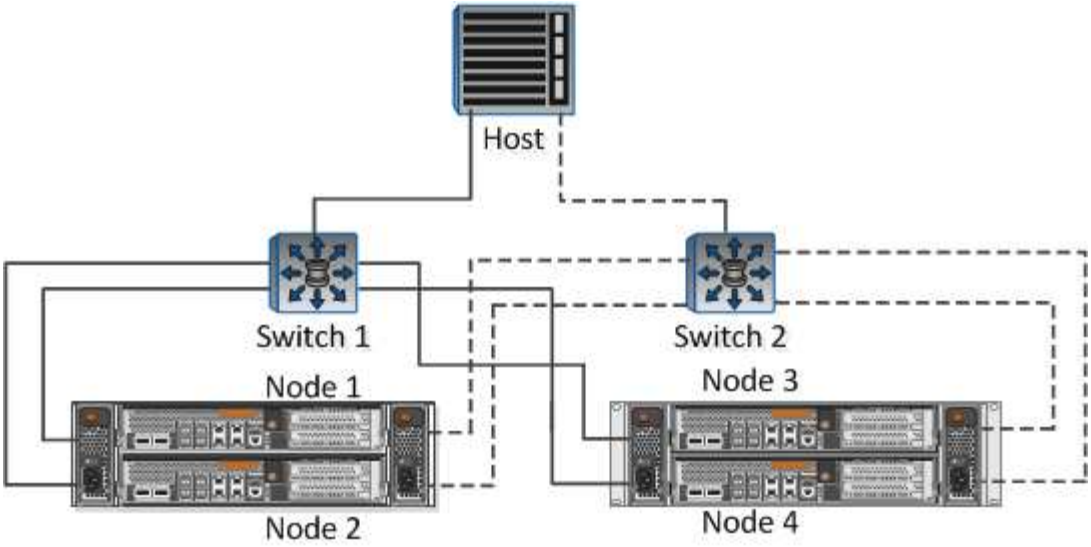
異なる**ONTAP** リリース間での**VVOL**処理は避けてください。

サポートされるストレージ機能（QoS、パーソナリティなど）はVASA Providerのリリースによって変更され、一部はONTAP リリースに依存します。ONTAP クラスタで異なるリリースを使用したり、リリースの異なるクラスタ間でVVolを移動したりすると、予期しない動作やコンプライアンスアラームが発生する可能性があります。

- VVOLにNVMe/FCまたはFCPを使用する前に、ファイバチャネルファブリックのゾーニングを設定してください。*

ONTAP tools VASAプロバイダは、管理対象のESXiホストで検出されたイニシエータに基づいて、FCPおよびiSCSI igroup、およびONTAP 内のNVMeサブシステムを管理します。ただし、ゾーニングを管理するためにファイバチャネルスイッチと統合することはできません。プロビジョニングを実行する前に、ベストプラクティスに従ってゾーニングを実行する必要があります。次に、4つのONTAPシステムに対する単一イニシエータゾーニングの例を示します。

単一イニシエータのゾーニング：




ベストプラクティスの詳細については、次のドキュメントを参照してください。

"_TR-4080『Best Practices for Modern SAN ONTAP 9』を参照してください"

"_TR-4684『Implementing and Configuring Modern SANs with NVMe-oF』を参照してください"

あなたの必要性に応じてあなたのバッキング**FlexVol**を計画しなさい。

VVOLデータストアに元のボリュームをいくつか追加して、ONTAP クラスタ全体にワークロードを分散したり、さまざまなポリシーオプションをサポートしたり、許可するLUNやファイルの数を増やしたりすることができます。ただし、最大限のストレージ効率が必要な場合は、すべてのバッキングボリュームを1つのアグリゲートに配置してください。また、クローニングのパフォーマンスを最大限に高める必要がある場合は、単一のFlexVol ボリュームを使用し、テンプレートまたはコンテンツライブラリを同じボリューム内に維持することを検討してください。VASA Providerは、移行、クローニング、Snapshotなど、多くのVVOLストレージ処理をONTAP にオフロードします。単一のFlexVol ボリューム内で実行すると、スペース効率に優れたファイルクローンが使用され、ほぼ瞬時に使用できます。この処理をFlexVol ボリューム間で実行すると、コピーをすぐに使用でき、インラインの重複排除と圧縮が使用されます。ただし、バックグラウンドの重複排除と圧縮を使用するボリュームでバックグラウンドジョブが実行されるまで、最大限のストレージ効率が回復されることはありません。ソースとデスティネーションによっては、一部の効率が低下する場合があります。

ストレージ機能プロファイル（**SCP**）はシンプルに。

必要のない機能は、anyに設定して指定しないでください。これにより、FlexVol ボリュームを選択または作成する際の問題を最小限に抑えることができます。たとえば、VASA Provider 7.1以前では、圧縮がデフォルトのSCP設定の[いいえ]のままになっていると、AFF システムであっても圧縮を無効にしようとします。

デフォルトの**SCP**をサンプルテンプレートとして使用して、独自の**SCP**を作成します。

付属のSCPはほとんどの汎用用途に適していますが、要件が異なる場合があります。

最大**IOPS**を使用して不明な**VM**やテスト**VM**を制御することを検討してください。

最大IOPSを使用すると、不明なワークロードのIOPSを特定のVVolに制限して、他の重要度の高いワークロードへの影響を回避できます。パフォーマンス管理の詳細については、表4を参照してください。

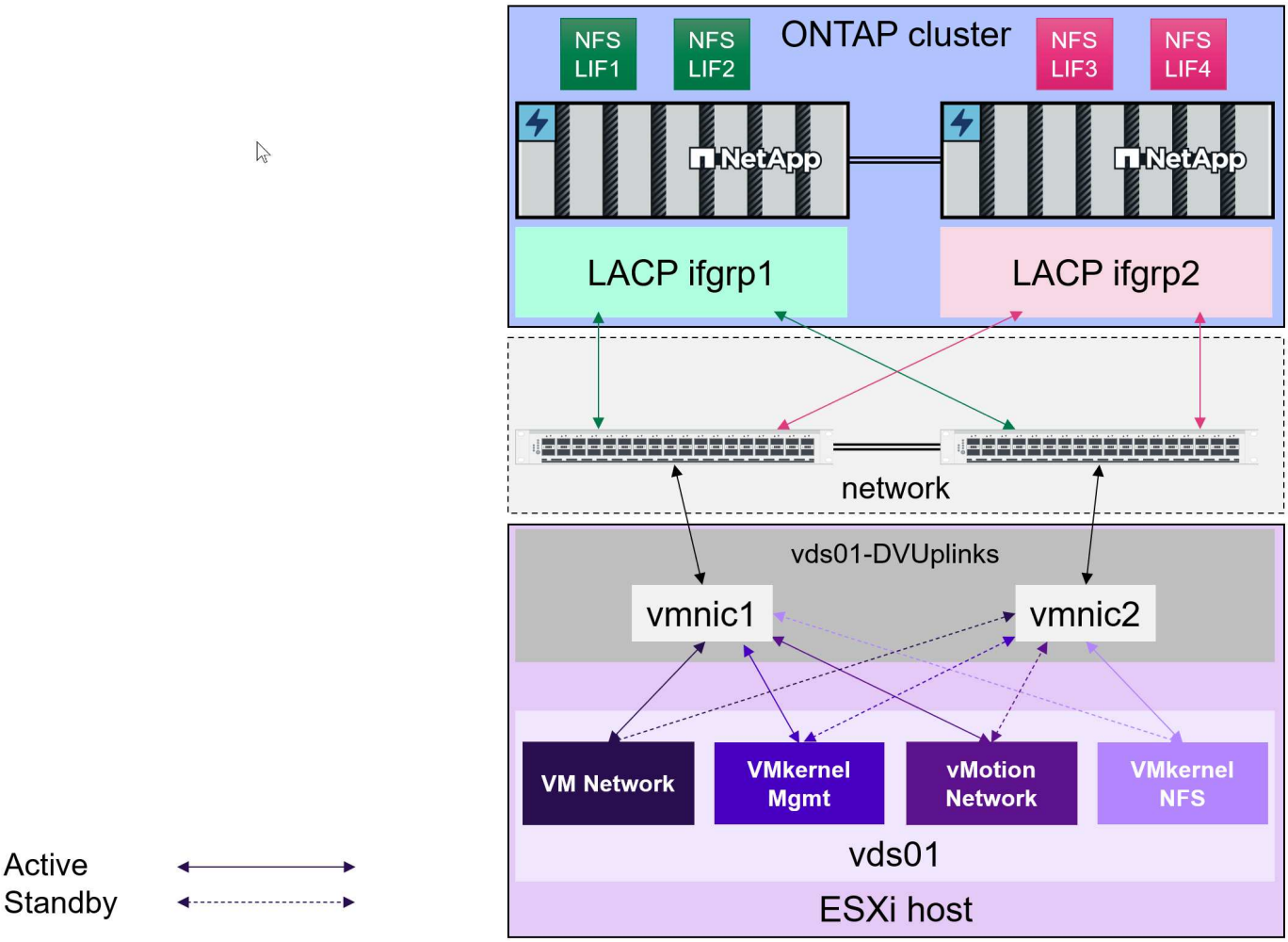
十分な数のデータ**LIF**があることを確認してください。
各HAペアのノードごとに少なくとも2つのLIFを作成します。ワークロードに応じて、さらに多くの処理が必

要になる場合があります。

すべてのプロトコルのベストプラクティスに従ってください。

選択したプロトコルに固有のNetAppおよびVMwareのその他のベストプラクティスガイドを参照してください。一般的に、上記以外の変更はありません。

- NFS v3経由でVVOLを使用したネットワーク構成の例*




## vVolストレージの導入

### VM用のVVOLストレージを作成するには、いくつかの手順を実行します。

従来のデータストアにONTAP を使用する既存のvSphere環境では、最初の2つの手順は必要ない場合があります。VMFSまたは従来のNFSベースのストレージの管理、自動化、レポート作成に、すでにONTAPツールを使用している場合があります。これらの手順については、次のセクションで詳しく説明します。

1. Storage Virtual Machine（SVM）とそのプロトコル設定を作成します。[NVMe/FC]、[NFSv3]、[NFSv4.1]、[iSCSI]、[FCP]、 またはそれらのオプションの組み合わせ。ONTAPのSystem Managerウィザードまたはクラスタシェルコマンドラインを使用できます。
   - スイッチ/ファブリック接続ごとにノードごとに少なくとも1つのLIFが必要です。FCP、iSCSI、またはNVMeベースのプロトコルを使用する場合は、ノードごとに2つ以上を作成することを推奨します。

- この時点でボリュームを作成することもできますが、_Provision Datastore_wizardで作成する方が簡単です。ただし、VMware Site Recovery ManagerでvVolレプリケーションを使用する場合は例外です。この方法を使用すると、既存のSnapMirror関係が設定された既存のFlexVol を使用した方が簡単です。QoSはSPBMとONTAP ツールで管理するため、VVOLに使用するボリュームでは有効にしないでください。

2. NetApp Support Site からダウンロードしたOVAを使用して、ONTAP Tools for VMware vSphereを導入します。
3. 環境に合わせてONTAP toolsを設定します。
   - ONTAP toolsの_Storage Systems_にONTAP クラスタを追加します
     - ONTAP toolsとSRAはクラスタレベルとSVMレベルの両方のクレデンシャルをサポートしますが、VASA Providerではストレージシステムのクラスタレベルのクレデンシャルのみがサポートされます。これは、VVOLに使用されるAPIの多くがクラスタレベルでしか使用できないためです。そのため、VVOLを使用する場合は、クラスタを対象としたクレデンシャルを使用してONTAPクラスタを追加する必要があります。
   - ONTAP データLIFがVMkernelアダプタとは異なるサブネットにある場合は、ONTAP toolsの設定メニューで、[Selected Subnets]リストにVMkernelアダプタのサブネットを追加する必要があります。デフォルトでは、ONTAP toolsはローカルサブネットへのアクセスのみを許可することでストレージトラフィックを保護します。
   - ONTAPツールには、事前定義されたポリシーがいくつか用意されています。これらのポリシーは、 ポリシーによるVMの管理 を参照してください。
4. vCenterの_Provision ONTAP tools_menuを使用して、_Provision datastore_wizardを起動します。
5. わかりやすい名前を指定し、目的のプロトコルを選択します。データストアの概要 も指定できます。
6. vVolデータストアでサポートするSCPを1つ以上選択します。これにより、プロファイルに一致しないONTAP システムがすべて除外されます。表示されたリストから、目的のクラスタとSVMを選択します。
7. ウィザードを使用して、指定したSCPごとに新しいFlexVol ボリュームを作成するか、適切なラジオボタンを選択して既存のボリュームを使用します。
8. vCenter UIの_PoliciesとProfiles_menuから、データストアで使用する各SCPのVMポリシーを作成します。
9. 「NetApp.clustered.Data.ONTAP.VP.vvol」ストレージルールセットを選択します。「NetApp.clustered.Data.ONTAP.VP.VASA10」ストレージルールセットは、vVol以外のデータストアでのSPBMサポート用です
10. ストレージ機能プロファイルは、VMストレージポリシーを作成するときに名前で指定します。この手順では、[replication]タブを使用してSnapMirrorポリシーの照合を設定し、[Tags]タブを使用してタグベースの照合を設定することもできます。選択できるようにするには、タグがすでに作成されている必要があります。
11. [Select storage]でVMストレージポリシーと互換性があるデータストアを選択して、VMを作成します。

### 従来のデータストアから**VVOL**への**VM**の移行

従来のデータストアからvVolデータストアへのVMの移行は、従来のデータストア間でVMを移動するだけです。VMを選択し、[Actions]リストから[Migrate]を選択し、移行タイプとして[*change storage only*]を選択します。移行コピー処理はvSphere 6.0以降ではSAN VMFSからVVOLへの移行でオフロードされますが、NAS VMDKからVVOLへの移行ではオフロードされません。

## ポリシーによるVMの管理

ポリシーベースの管理でストレージプロビジョニングを自動化するには、次のことが必要です。

- ストレージ機能プロファイル（SCP）を使用して、ストレージ（ONTAP ノードとFlexVol ボリューム）の機能を定義します。
- 定義済みのSCPに対応するVMストレージポリシーを作成します。

VASA Provider 7.2以降では、機能とマッピングが簡易化され、以降のバージョンで継続的に改善されています。このセクションでは、この新しいアプローチに焦点を当てます。以前のリリースではサポートされていた機能の数が増え、個 々 にストレージポリシーにマッピングすることができましたが、このアプローチはサポートされなくなりました。

ストレージ機能プロファイルONTAP toolsリリース別の機能

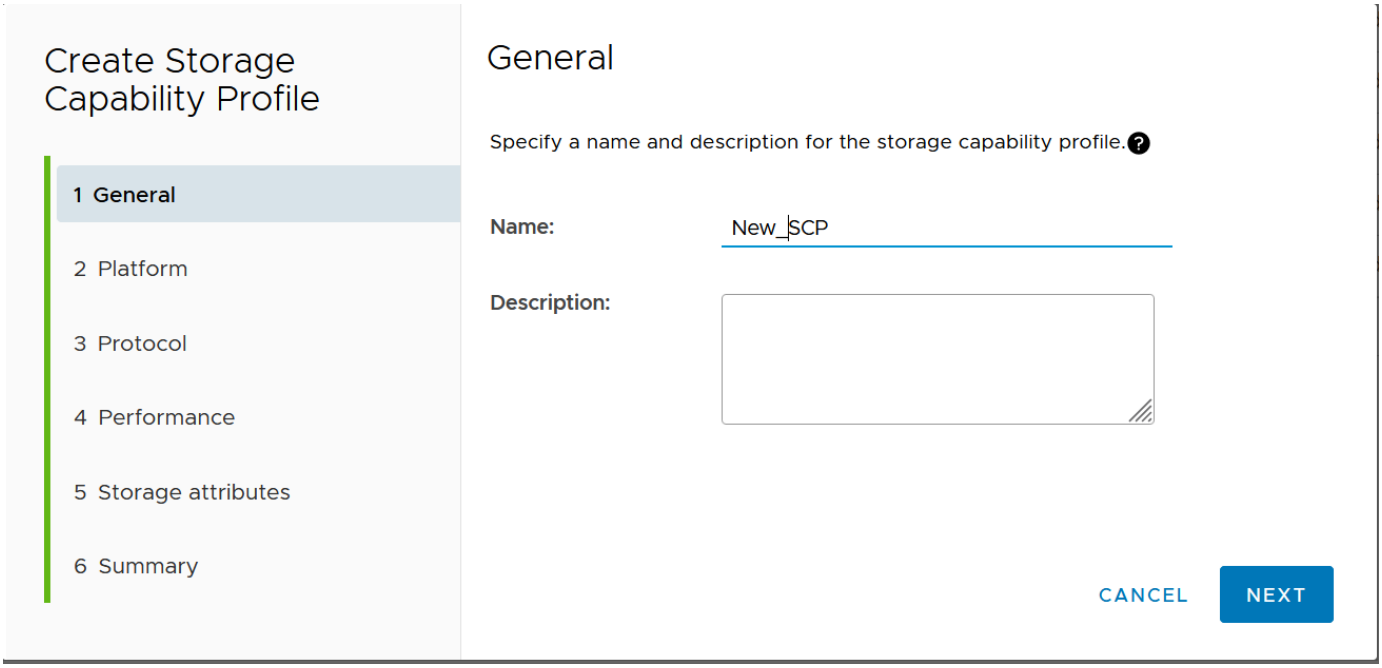
| * SCP機能* | 機能値 | サポートされているリリース | * メモ * |
|---|---|---|---|
| * 圧縮 * | はい、いいえ、任意 | すべて | 7.2以降のAFF では必須です。 |
| * 重複排除 * | はい、いいえ、任意 | すべて | 7.2以降のAFF では必須です。 |
| * 暗号化 * | はい、いいえ、任意 | 7.2以降 | 暗号化されたFlexVol ボリュームを選択または作成します。ONTAP ライセンスが必要です。 |
| * 最大 IOPS * | <number> | 7.1以降ですが、違いがあります | 7.2以降のQoSポリシーグループに表示されます。を参照してください ONTAP tools 9.10以降によるパフォーマンス管理 を参照してください。 |
| パーソナリティ | 略称はFAS | 7.2以降 | FAS には、ONTAP Select など、AFF以外のシステムも含まれます。AFF にはASA が含まれます。 |
| プロトコル | NFS、NFS 4.1、iSCSI 、FCP、NVMe/FC、 任意 | 7.1以前、9.10以降 | 7.2-9.8は実質的に「任意」です。9.10以降では、NFS 4.1とNVMe/FC が元のリストに追加されました。 |
| スペースリザベーション（シンプロビジョニング） | Thin（シン）、Thick（シック）、（任意） | すべて、違いを除いて | 7.1以前ではシンプロビジョニングと呼ばれ、anyの値も使用できました。7.2ではスペースリザベーションと呼ばれていますすべてのリリースのデフォルトはシンです。 |

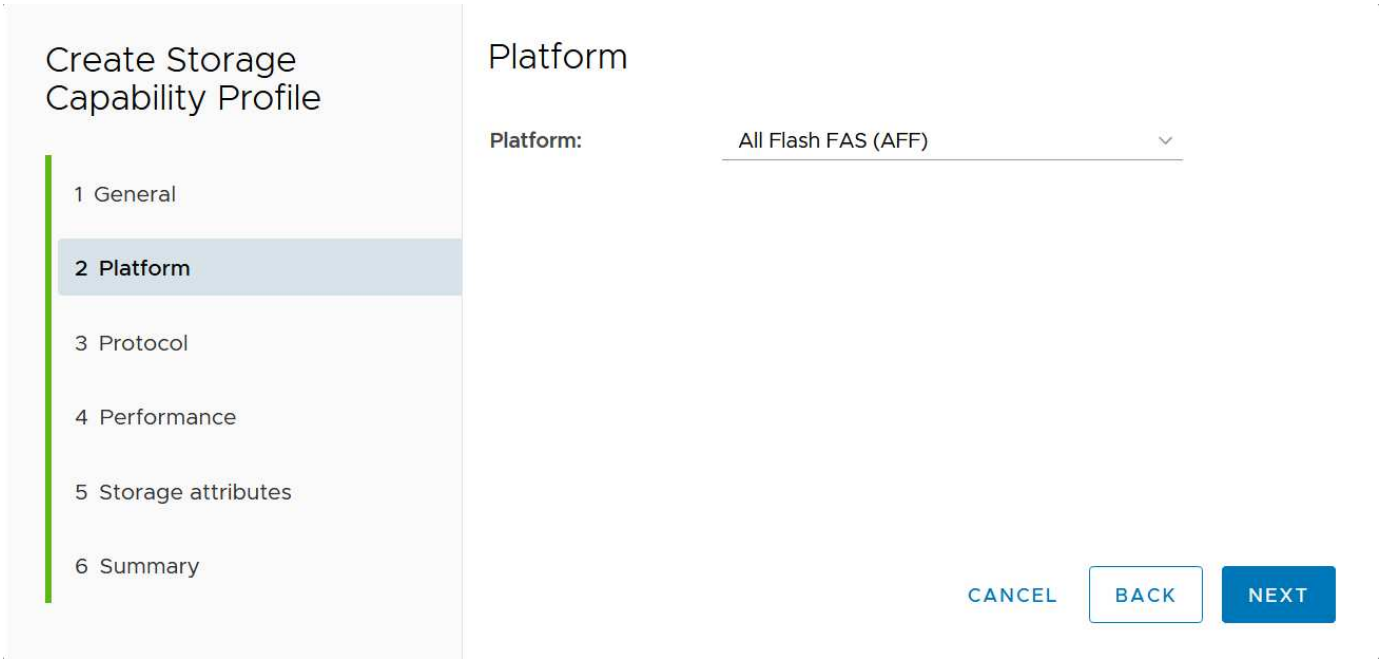
| * SCP機能* | 機能値 | サポートされているリリース | * メモ * |
| --- | --- | --- | --- |
| * 階層化ポリシー * | [任意]、[なし]、[スナップショット]、[自動] | 7.2以降 | FabricPoolに使用- ONTAP 9.4以降を搭載したAFFまたはASAが必要です。NetApp StorageGRIDのようなオンプレミスのS3解決策 を使用しないかぎり、Snapshotのみが推奨されます。 |

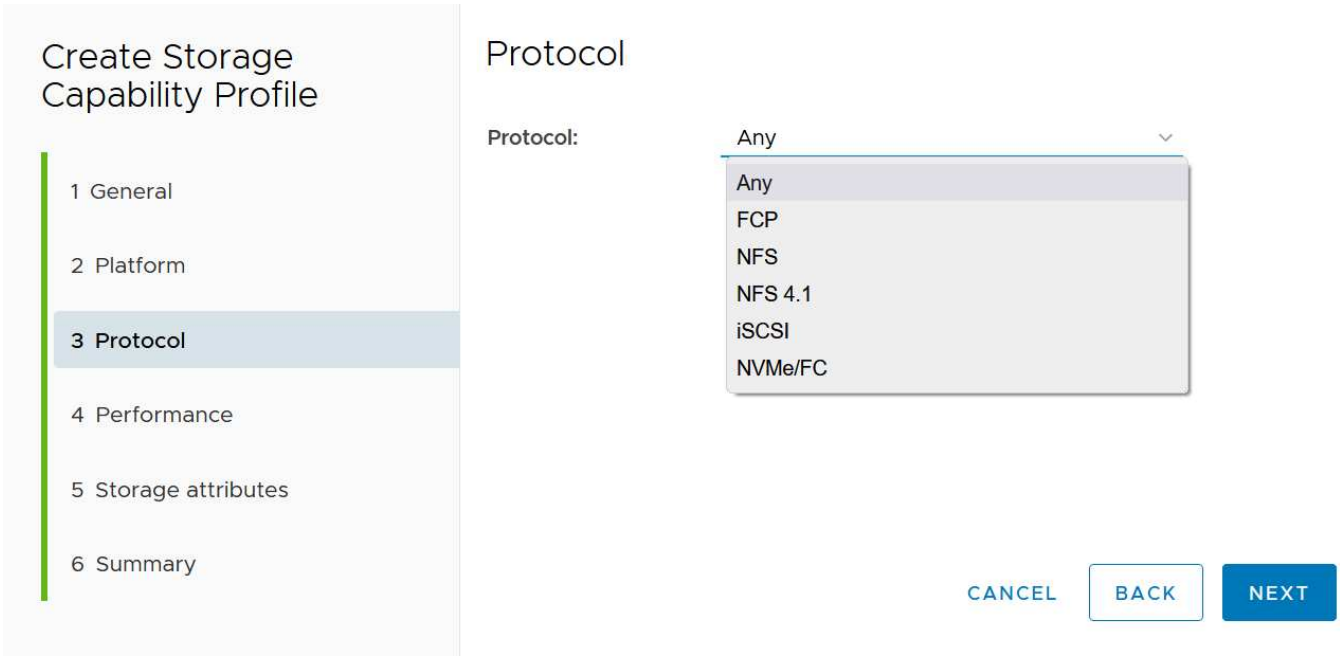
ストレージ機能プロファイルの作成

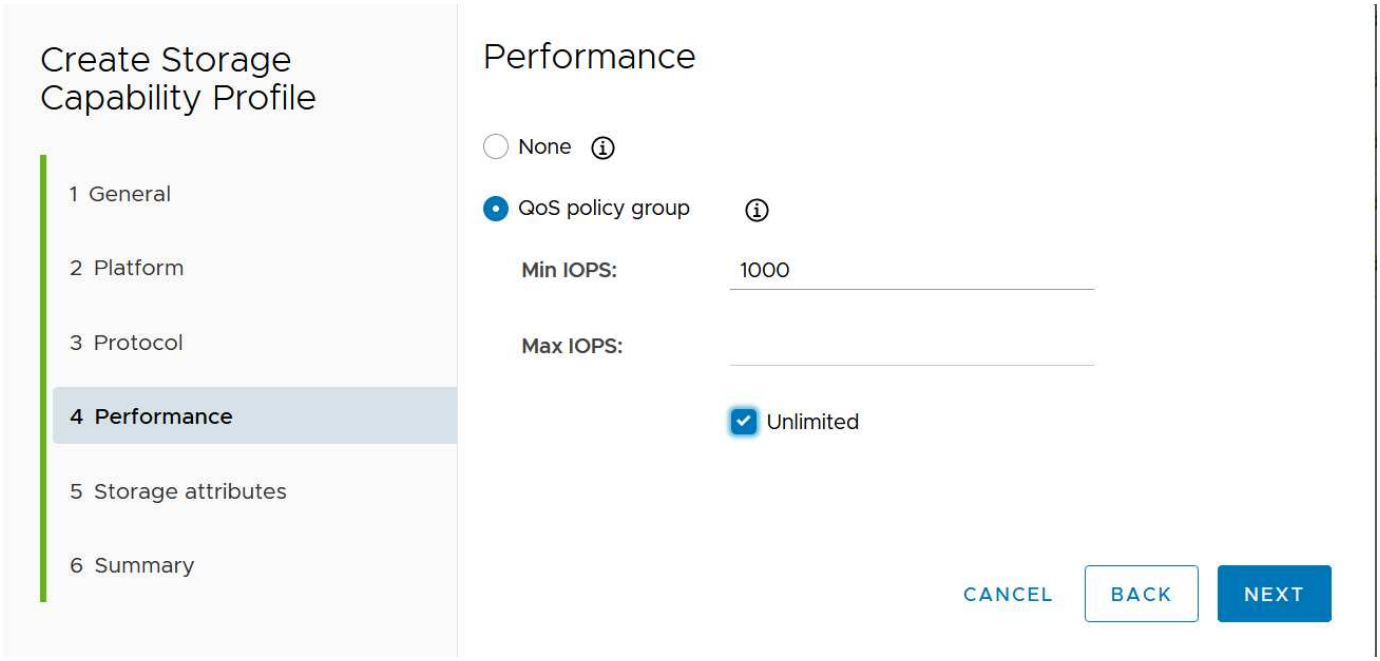
NetApp VASA Providerには、いくつかのSCPが事前定義されています。新しいSCPは、vCenter UIを使用して手動で作成することも、REST APIを使用した自動化を通じて作成することもできます。新しいプロファイルで機能を指定するか、既存のプロファイルをクローニングするか、既存の従来のデータストアからプロファイルを自動生成します。これは、ONTAP ツールのメニューを使用して行います。ストレージ機能プロファイル_を使用してプロファイルを作成またはクローニングし、ストレージマッピング_を使用してプロファイルを自動生成します。

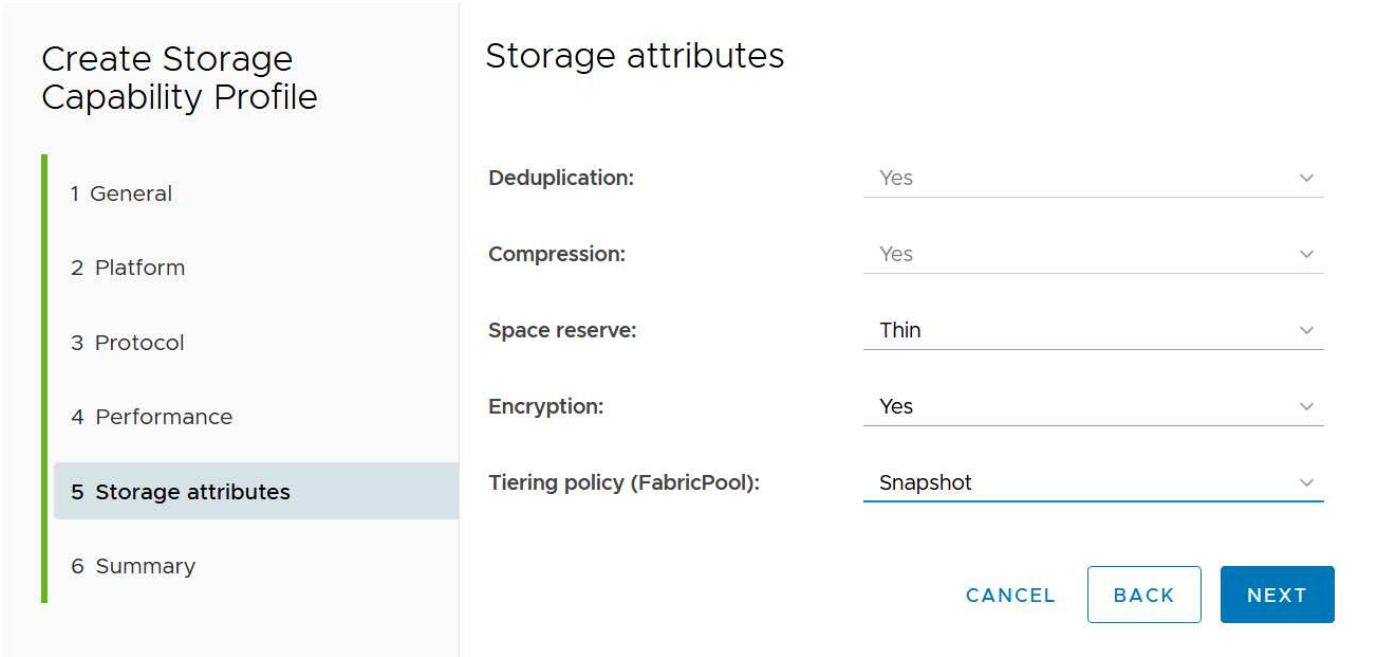
**ONTAP tools 9.10**以降のストレージ機能

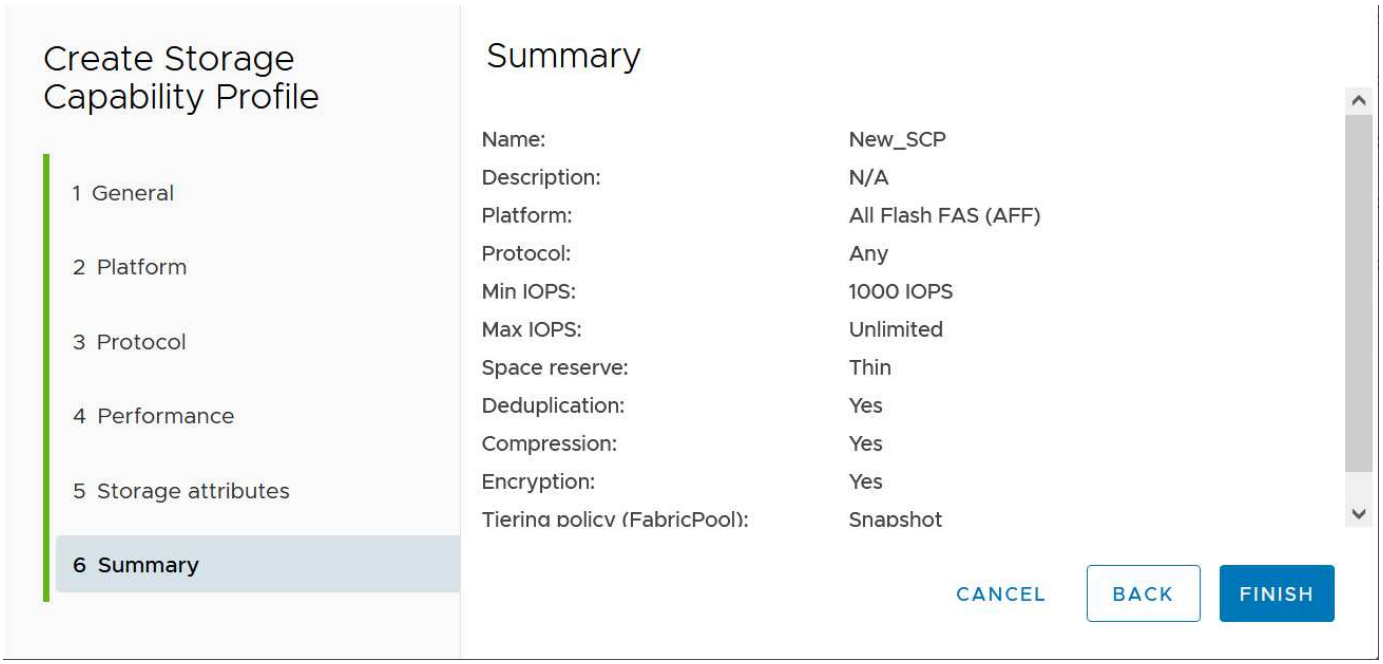



Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Platform
Platform:
All Flash FAS (AFF)
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Protocol
Protocol:
Any
Any
FCP
NFS
NFS 4.1
iSCSI
NVMe/FC
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Performance
None
QoS policy group
Min IOPS:
1000
Max IOPS:
Unlimited
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Storage attributes
Deduplication:
Yes
Compression:
Yes
Space reserve:
Thin
Encryption:
Yes
Tiering policy (FabricPool):
Snapshot
CANCEL
BACK
NEXT




- vVolデータストアを作成しています*
  必要なSCPを作成したら、そのSCPを使用してVVOLデータストア（および必要に応じてデータストア用のFlexVol ボリューム）を作成できます。ONTAP データストアを作成するホスト、クラスタ、またはデータセンターを右クリックし、_vVol tools>>_Provision Datastore_を選択します。データストアでサポートするSCPを1つ以上選択し、既存のFlexVol ボリュームから選択するか、データストア用に新しいFlexVol ボリュームをプロビジョニングします。最後に、データストアのデフォルトのSCPを指定します。このSCPは、ポリシーで指定されたSCPが設定されていないVMやスワップVVOL（ハイパフォーマンスなストレージは必要ありません）に使用されます。

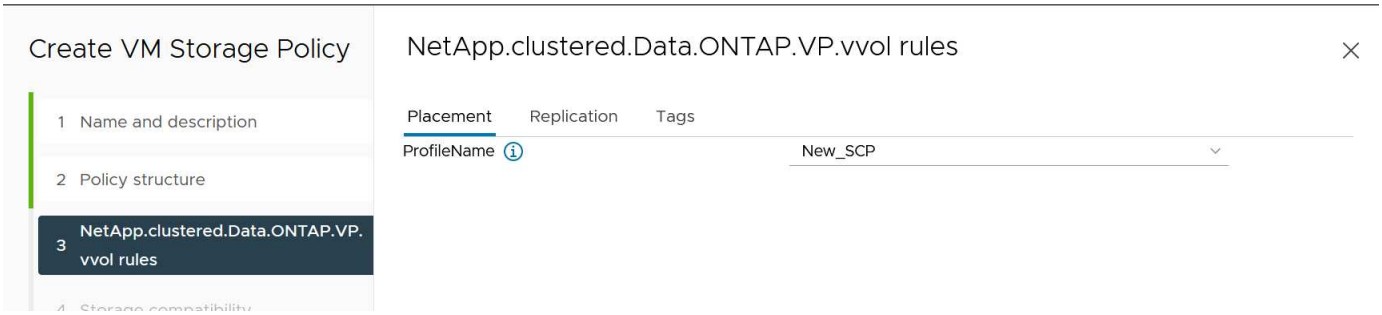
仮想マシンストレージポリシーを作成しています

仮想マシンストレージポリシーは、Storage I/O ControlやvSphere Encryptionなどのオプション機能を管理するためにvSphereで使用されます。また、VVOLでも使用され、特定のストレージ機能をVMに適用します。ポリシーを使用して特定のSCPをVMに適用するには、「NetApp.clustered.Data.ONTAP.VP.vVol」ストレージタイプと「ProfileName」ルールを使用します。ONTAP tools VASA Providerを使用した場合の例については、link：vmware-vvols-ontap.html #ベストプラクティス[ NFS v3経由のVVOLを使用したネットワーク設定例]を参照してください。「NetApp.clustered.Data.ONTAP.VP.VASA10」ストレージのルールは、VVOLベース以外のデータストアで使用します。

以前のリリースも似ていますが、で説明しているように、 ストレージ機能プロファイルONTAP toolsリリース別の機能オプションは異なります。

作成したストレージポリシーは、に示すように、新しいVMのプロビジョニング時に使用できます。 "ストレージポリシーを使用してVMを導入します"。VASA Provider 7.2でパフォーマンス管理機能を使用する場合のガイドラインについては、を参照してください。 ONTAP tools 9.10以降によるパフォーマンス管理。

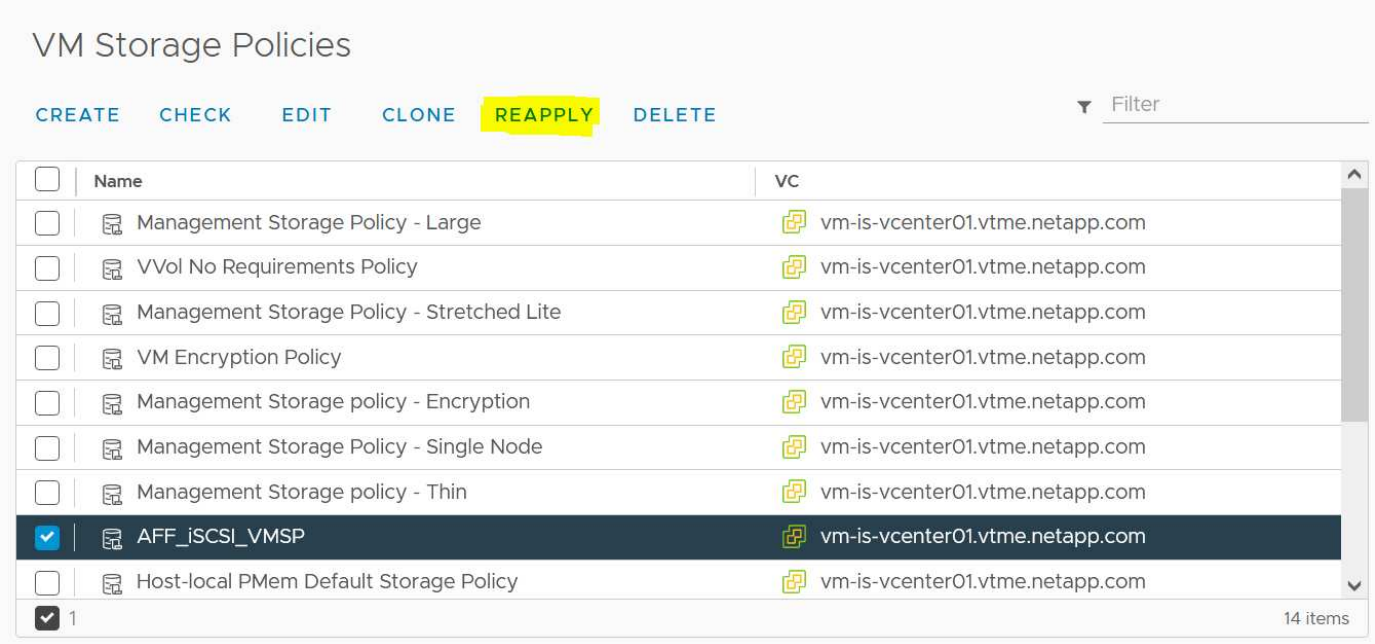
**ONTAP tools VASA Provider 9.10**を使用した**VM**ストレージポリシーの作成




**ONTAP tools 9.10**以降によるパフォーマンス管理

- ONTAP tools 9.10では、独自の分散配置アルゴリズムを使用して、vVolデータストア内の最適なFlexVolに新しいvVolが配置されます。指定したSCPと一致するFlexVol ボリュームに基づいて配置されます。これにより、データストアとバッキングストレージが、指定されたパフォーマンス要件を確実に満たすことができます。
- 最小IOPSや最大IOPSなどのパフォーマンス機能を変更するには、特定の構成に注意する必要があります。
  - *最小IOPSと最大IOPS *はSCPで指定し、VMポリシーで使用できます。
    - SCPでIOPSを変更しても、VMポリシーを編集してそれを使用するVMに再適用するまで、VVOLのQoSは変更されません（ ONTAP tools 9.10以降のストレージ機能）。または、必要なIOPSで新しいSCPを作成し、そのSCPを使用する（VMに再適用する）ようにポリシーを変更します。一般的には、サービス階層ごとに個別のSCPとVMストレージポリシーを定義し、VMのVMストレージポリシーを変更することを推奨します。
    - AFF とFAS のパーソナリティではIOPS設定が異なります。AFF では、MinとMaxの両方を使用できます。ただし、AFF以外のシステムで使用できるのは最大IOPSの設定のみです。
- 場合によっては、ポリシーの変更後（手動またはVASA ProviderとONTAP による自動）にVVOLの移行が必要になることがあります。
  - 一部の変更では移行は必要ありません（最大IOPSの変更など、前述のようにVMにすぐに適用できます）。
  - VVOLが格納されている現在のFlexVol でポリシーの変更をサポートできない場合（要求された暗号化ポリシーまたは階層化ポリシーがプラットフォームでサポートされていない場合など）は、vCenterでVMを手動で移行する必要があります。
- ONTAP toolsは、現在サポートされているバージョンのONTAP に対して、共有されていないQoSポリシーを個別に作成します。そのため、個 々 のVMDKにはそれぞれ独自のIOPSが割り当てられます。

**VM**ストレージポリシーを再適用しています




# VVOLを保護する

以降のセクションでは、VMware VVOLとONTAPストレージを使用する手順とベストプラクティスについて説明します。

## VASA Providerの高可用性

NetApp VASA Providerは、vCenterプラグイン、REST APIサーバ（旧Virtual Storage Console[VSC]）、およびStorage Replication Adapterとともに仮想アプライアンスの一部として実行されます。VASA Providerを使用できない場合、VVOLを使用するVMは引き続き実行されます。ただし、新しいvVolデータストアを作成することはできず、vVolをvSphereで作成またはバインドすることもできません。vCenterはスワップVVolの作成を要求できないため、VVolを使用するVMの電源をオンにできません。また、vVolを新しいホストにバインドできないため、実行中のVMでvMotionを使用して別のホストに移行することはできません。

VASA Provider 7.1以降では、必要なときにサービスを利用できるようにするための新しい機能がサポートされています。VASA Providerと統合データベースサービスを監視する新しいwatchdogプロセスが含まれています。障害が検出されると、ログファイルが更新され、サービスが自動的に再起動されます。

vSphere管理者は、他のミッションクリティカルなVMをソフトウェア、ホストハードウェア、およびネットワークの障害から保護するのと同じ可用性機能を使用して、さらに保護を設定する必要があります。これらの機能を使用するために仮想アプライアンスで追加の設定を行う必要はありません。標準のvSphereアプローチを使用して設定するだけです。これらはネットアップによってテストされ、サポートされています。

vSphere High Availabilityは、障害発生時にホストクラスタ内の別のホストでVMを再起動するように簡単に構成できます。vSphere Fault Toleranceは、継続的にレプリケートされ、任意の時点でテイクオーバーできるセカンダリVMを作成することで、可用性を高めます。これらの機能の追加情報 はで使用できます "ONTAP tools for VMware vSphereのドキュメント（ONTAP toolsの高可用性の設定）"、およびVMware vSphereのドキュメント（「ESXiおよびvCenter ServerのvSphereの可用性」を参照）。

ONTAP tools VASA Providerは、VVOLの設定を管理対象のONTAP システムにリアルタイムで自動的にバックアップします。このシステムでは、VVOL情報がFlexVol ボリュームのメタデータに格納されます。何らかの理由でONTAP toolsアプライアンスが使用できなくなった場合でも、簡単かつ迅速に新しいアプライアンスを導入して設定をインポートできます。VASA Providerのリカバリ手順の詳細については、次の技術情報アーテ

ィクルを参照してください。

"『How to perform a VASA Provider Disaster Recovery - Resolution Guide』"

### vVolレプリケーション

ONTAP をご利用のお客様の多くは、NetApp SnapMirrorを使用して従来のデータストアをセカンダリストレージシステムにレプリケートし、災害発生時にセカンダリシステムを使用して個 々 のVMやサイト全体をリカバリしています。ほとんどの場合、お客様はこの管理にソフトウェアツールを使用します。たとえば、VMware vSphere用NetApp SnapCenterプラグインなどのバックアップソフトウェア製品や、VMwareのSite Recovery Managerなどのディザスタリカバリ解決策（ONTAPツールのStorage Replication Adapterとともに使用）などです。

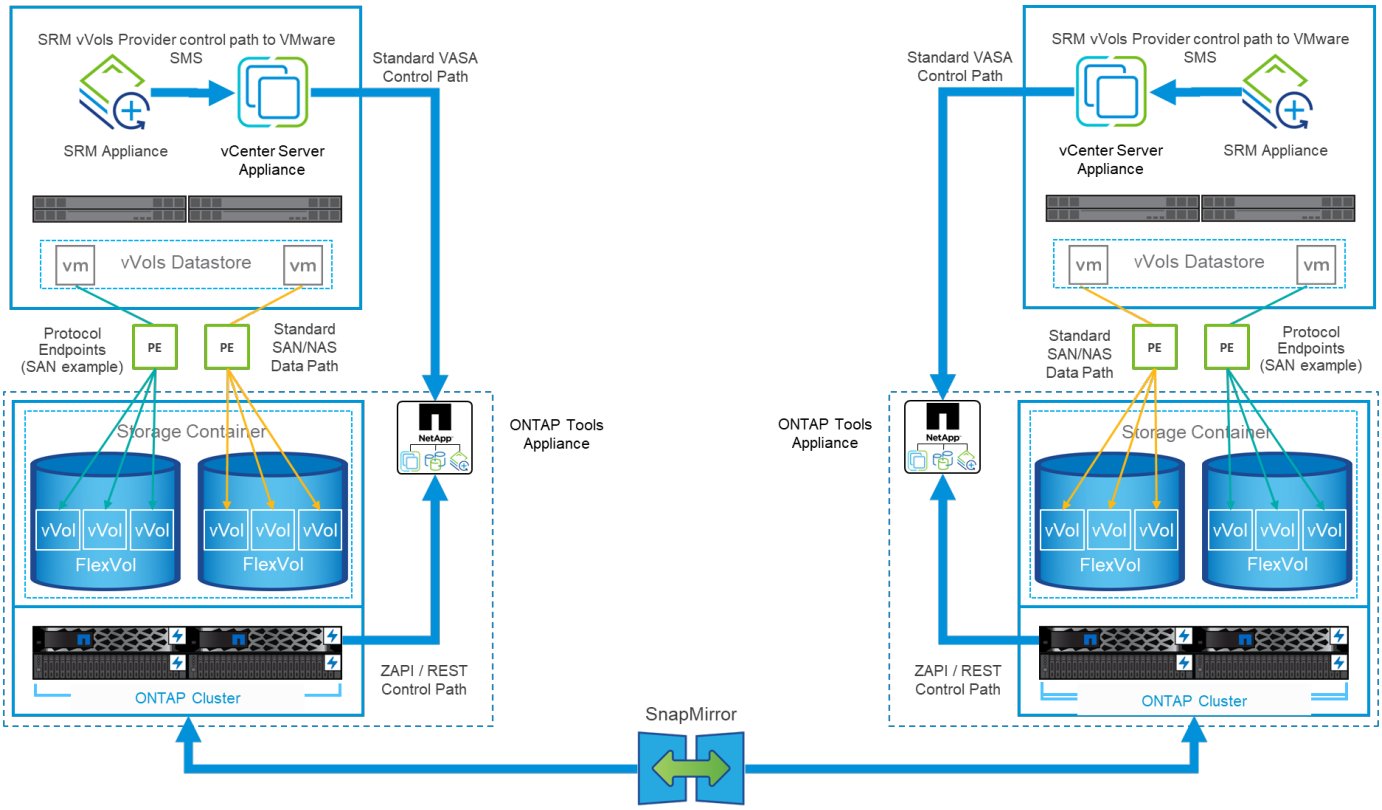
このソフトウェアツールの要件は、vVolレプリケーションの管理においてさらに重要になります。一部の機能はネイティブの機能で管理できます（たとえば、VMwareが管理するvVolのSnapshotは、高速で効率的なファイルクローンまたはLUNクローンを使用するONTAP にオフロードされます）が、一般的には、レプリケーションとリカバリを管理するためにオーケストレーションが必要です。VVOLに関するメタデータは、ONTAPとVASA Providerによって保護されますが、セカンダリサイトでメタデータを使用するには追加の処理が必要です。

ONTAP tools 9.7.1とVMware Site Recovery Manager（SRM）8.3リリースを併用すると、ディザスタリカバリと移行のワークフローオーケストレーションのサポートが追加され、NetApp SnapMirrorテクノロジのメリットを活用できるようになりました。

ONTAP tools 9.7.1を使用したSRMの初期リリースでは、FlexVolを事前に作成し、それらをVVOLデータストアのバッキングボリュームとして使用する前にSnapMirror保護を有効にする必要がありました。ONTAP tools 9.10以降では、このプロセスは不要になりました。既存のバッキングボリュームにSnapMirror保護を追加し、VMのストレージポリシーを更新して、SRMに統合されたディザスタリカバリと移行のオーケストレーション、自動化機能を備えたポリシーベースの管理を活用できるようになりました。

現在、ネットアップがサポートするvVol用のディザスタリカバリおよび移行自動化の解決策 はVMware SRMのみです。ONTAP ツールでは、vVolレプリケーションを有効にする前に、vCenterに登録されているSRM 8.3以降のサーバの有無が確認されます。 ONTAP ツールREST APIを活用して独自のサービスを作成することも可能です。

#### SRMを使用したvVolレプリケーション




**MetroCluster** のサポート

ONTAP toolsではMetroCluster のスイッチオーバーはトリガーされませんが、同じvSphere Metro Storage Cluster（vMSC）構成のVVol用NetApp MetroCluster システムではサポートされます。MetroCluster システムのスイッチオーバーは通常の方法で処理されます。

NetApp SnapMirrorビジネス継続性（SM-BC）はvMSC構成のベースとしても使用できますが、現時点ではVVOLではサポートされていません。

NetApp MetroCluster の詳細については、次のガイドを参照してください。

"*TR-4689 MetroCluster IP解決策 のアーキテクチャと設計*"

"*TR-4705 NetApp MetroCluster 解決策 のアーキテクチャと設計*"

"*VMware KB 2031038 NetApp MetroCluster によるVMware vSphereのサポート*"

**vVol**バックアップの概要

ゲスト内バックアップエージェントの使用、VMデータファイルのバックアッププロキシへの接続、VMware VADPなどの定義済みAPIの使用など、VMを保護する方法はいくつかあります。VVOLは同じメカニズムを使用して保護でき、多くのネットアップパートナーがVVOLを含むVMのバックアップをサポートしています。

前述したように、VMware vCenterで管理されるスナップショットは、スペース効率に優れた高速なONTAP ファイル/ LUNクローンにオフロードされます。これらは迅速な手動バックアップに使用できますが、vCenterでは最大32個のスナップショットに制限されています。vCenterを使用してスナップショットを作成し、必要に応じて元に戻すことができます。

SnapCenter Plugin for VMware vSphere（SCV）4.6以降では、ONTAP tools 9.10以降と組み合わせて使用す

ることで、vVolベースのVMのcrash-consistentバックアップおよびリカバリがサポートされるようになりました。SnapMirrorおよびSnapVault レプリケーションがサポートされたONTAP FlexVol ボリュームSnapshotを活用します。ボリュームあたり最大1023個のSnapshotがサポートされます。また、ミラーバックアップポリシーを使用したSnapMirrorを使用すると、保持期間の長いSnapshotをセカンダリボリュームに格納することもできます。

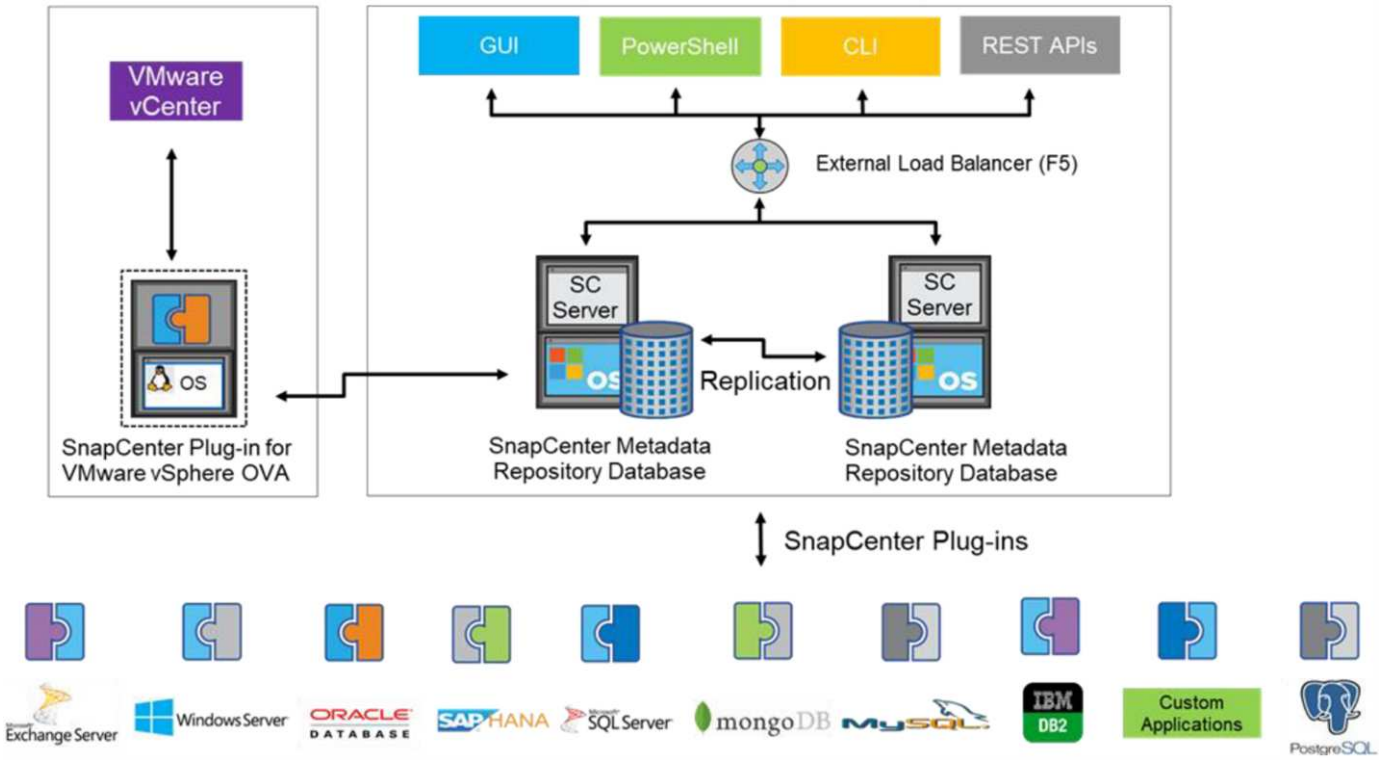
vSphere 8.0のサポートは、分離されたローカルプラグインアーキテクチャを使用するSCV 4.7で導入されました。vSphere 8.0U1のサポートがSCV 4.8に追加され、新しいリモートプラグインアーキテクチャに完全に移行しました。

### VMware vSphere用のSnapCenter プラグインを使用したVVolバックアップ

NetApp SnapCenterでは、タグやフォルダに基づいてvVolのリソースグループを作成し、vVolベースのVMに対してONTAPのFlexVolベースのSnapshotを自動的に利用できるようになりました。これにより、環境内で動的にプロビジョニングされたVMを自動的に保護するバックアップ/リカバリサービスを定義できます。

SnapCenter Plugin for VMware vSphereは、vCenter拡張機能として登録されたスタンドアロンアプライアンスとして導入され、vCenter UIまたはREST APIを使用して管理され、バックアップ/リカバリサービスの自動化が可能です。

#### SnapCenter アーキテクチャ




本ドキュメントの執筆時点では、他のSnapCenterプラグインはまだVVOLをサポートしていないため、本ドキュメントではスタンドアロンの導入モデルについて説明します。

SnapCenter はONTAP FlexVol スナップショットを使用するため、vSphereへのオーバーヘッドは発生しません。また、vCenterで管理されているスナップショットを使用する従来のVMで発生する可能性のあるパフォーマンスの低下もありません。さらに、SCVの機能はREST APIを介して公開されるため、VMware ARIA Automation、Ansible、Terraformなどのツールや、標準のREST APIを使用できるその他のほぼすべての自動化ツールを使用して、自動化されたワークフローを簡単に作成できます。

SnapCenter REST API については、を参照してください "REST API の概要"

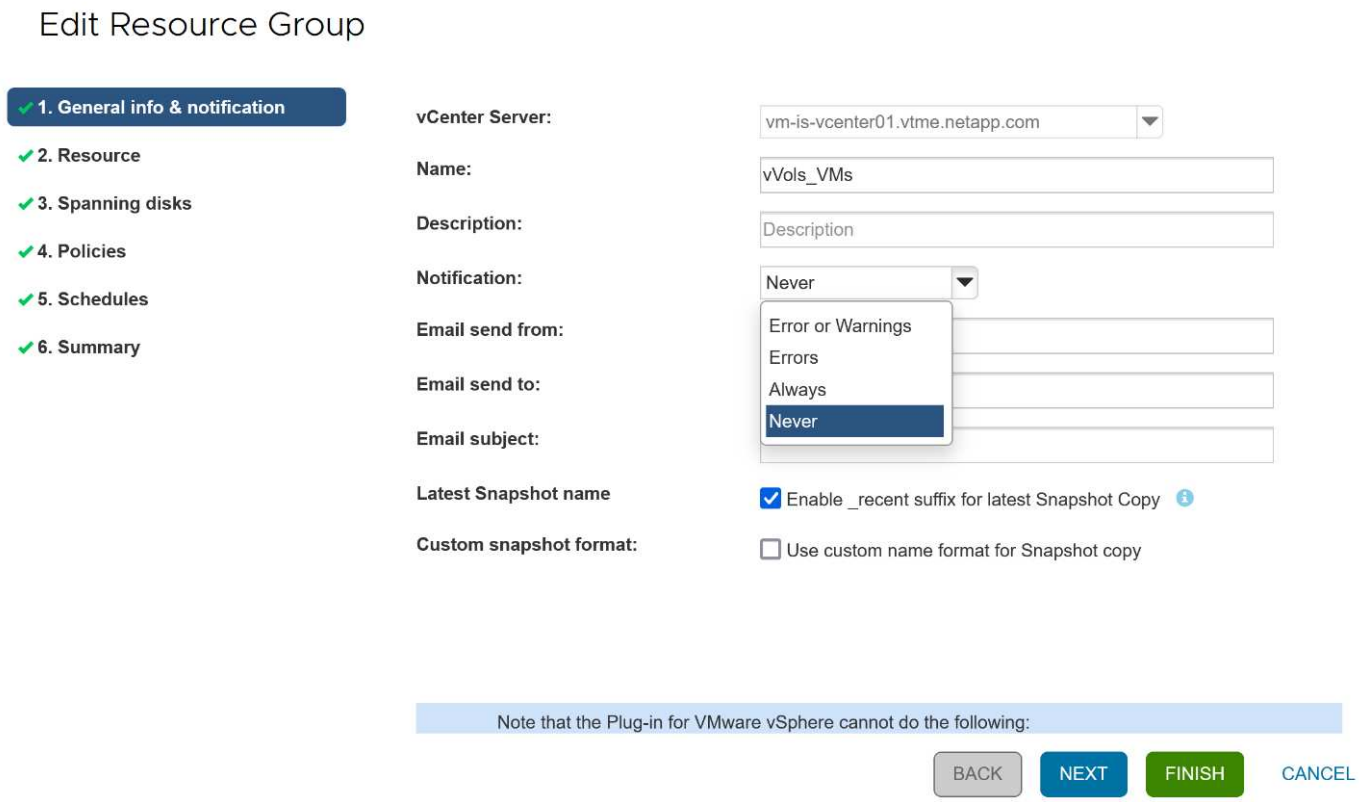
SnapCenter Plug-in for VMware vSphere REST API については、を参照してください "SnapCenter Plug-in for VMware vSphere REST API"

ベストプラクティス

SnapCenter 環境を最大限に活用するには、次のベストプラクティスを参考にしてください。

- SCVはvCenter Server RBACとONTAP RBACの両方をサポートしており、プラグインの登録時に自動的に作成される事前定義されたvCenterロールが用意されています。サポートされるRBACのタイプの詳細については、こちらを参照してください "こちらをご覧ください。"
  - vCenter UIを使用して、説明されている事前定義されたロールを使用して最小権限のアカウントアクセスを割り当てます "こちらをご覧ください"。
  - SnapCenter サーバでSCVを使用する場合は、_SnapCenterADMIN_ROLEを割り当てる必要があります。
  - ONTAP RBACは、SCVで使用するストレージシステムを追加および管理するために使用するユーザアカウントを指します。ONTAP RBACは、VVOLベースのバックアップには適用されません。ONTAP RBACとSCVの詳細については、こちらをご覧ください "こちらをご覧ください"。
- SnapMirrorを使用してバックアップデータセットを別のシステムにレプリケートし、ソースボリュームの完全なレプリカを作成します。前述したように、ソースボリュームのSnapshotの保持設定に関係なく、バックアップデータの長期保持にmirror-vaultポリシーを使用することもできます。どちらのメカニズムもVVOLでサポートされています。
- SCVではVVOL機能にONTAP Tools for VMware vSphereを使用する必要があるため、特定のバージョンの互換性については、必ずNetApp Interoperability Matrix Tool（IMT ）を参照してください
- VMware SRMでvVolレプリケーションを使用する場合は、ポリシーのRPOとバックアップスケジュールに注意してください
- 組織で定義された目標復旧時点（RPO）を満たす保持設定を使用してバックアップポリシーを設計
- バックアップの実行時にステータスが通知されるようにリソースグループに通知を設定します（下記の図10を参照）。

リソースグループの通知オプション




これらのドキュメントを使用して、**SCV**の使用を開始します

"SnapCenter Plug-in for VMware vSphere について説明します"

"SnapCenter Plug-in for VMware vSphere を導入"

## トラブルシューティング

追加情報 には、いくつかのトラブルシューティングリソースが用意されています。

### NetApp Support Site

NetApp Support Site には、ネットアップの仮想化製品に関するさまざまな技術情報アーティクルのほかに、の便利なランディングページも用意されています "VMware vSphere 用の ONTAP ツール" 製品：このポータルには、ネットアップコミュニティの記事、ダウンロード、テクニカルレポート、VMwareソリューションに関するディスカッションへのリンクが掲載されています。次のURLから入手できます。

"_ NetApp Support Site _"

その他の解決策 ドキュメントは、次のURLから入手できます。

"仮想化向けネットアップソリューション"

製品のトラブルシューティング

vCenterプラグイン、VASA Provider、Storage Replication Adapterなど、ONTAP ツールのさまざまなコンポーネントは、いずれもネットアップのドキュメントリポジトリにまとめられています。ただし、それぞれにKnowledge Baseのサブセクションがあり、特定のトラブルシューティング手順が記載されている場合があ

ります。これらは、VASA Providerで発生する可能性のある最も一般的な問題に対処します。

#### VASA ProviderのUIの問題

vCenter vSphere Web ClientでSerenityのコンポーネントに関する問題が発生し、VASA Provider for ONTAPのメニュー項目が表示されないことがあります。導入ガイドまたはこのナレッジベースのVASA Provider登録の問題の解決を参照してください "記事"。

#### vVolデータストアのプロビジョニングが失敗する

vVolデータストアの作成時にvCenterサービスがタイムアウトすることがあります。修正するには、vmware-spsサービスを再起動し、vCenterのメニュー（[Storage]>[New Datastore]）を使用してvVolデータストアを再マウントします。この問題については、『Administration Guide』のvCenter Server 6.5でvVolデータストアのプロビジョニングが失敗するという項を参照してください。

#### Unified Applianceをアップグレードすると、ISOのマウントに失敗します

vCenterのバグが原因で、Unified Applianceをあるリリースから次のリリースへアップグレードするために使用されるISOがマウントに失敗する可能性があります。ISOをvCenterのアプライアンスに接続できる場合は、このナレッジベースの手順に従ってください "記事" 解決するために。

# VMware Site Recovery ManagerとONTAP

## VMware Site Recovery ManagerとONTAP

ONTAPは、2002年に最新のデータセンターに導入されて以来、VMware vSphere環境向けストレージ解決策として業界をリードしてきました。また、コストを削減しながら管理を簡易化する革新的な機能を継続的に追加しています。

このドキュメントでは、業界をリードするVMwareのディザスタリカバリ（DR）ソフトウェアであるONTAP解決策for VMware Site Recovery Manager（SRM）について説明します。最新の製品情報とベストプラクティスを紹介し、導入の合理化、リスクの軽減、継続的な管理の簡素化を実現します。

> このドキュメントは、以前に公開されていたテクニカルレポート「TR-4900：VMware Site Recovery Manager」をONTAPに置き換えます。

ベストプラクティスは、ガイドや互換性ツールなどの他のドキュメントを補うものです。ラボテストに基づいて開発されており、ネットアップのエンジニアやお客様は広範な現場経験を積んでいます。推奨されるベストプラクティスがお客様の環境に適していない場合もありますが、一般に最もシンプルなソリューションであり、ほとんどのお客様のニーズに対応できます。

本ドキュメントでは、ONTAP Tools for VMware vSphere 9.12（NetApp Storage Replication Adapter[SRA]およびVASA Provider[VP]を含む）およびVMware Site Recovery Manager 8.7と組み合わせて使用した場合の、ONTAP 9の最近のリリースの機能を中心に説明します。

#### SRM で ONTAP を使用する理由

ONTAP ソフトウェアを基盤とするネットアップのデータ管理プラットフォームは、 SRM に最も広く採用されているストレージソリューションの一部です。理由はそれだけではありません。セキュアでハイパフォーマンスなユニファイドプロトコル（NASとSANを併用）データ管理プラットフォームで、業界を定義するストレージ効率、マルチテナンシー、サービス品質管理、スペース効率に優れたSnapshotによるデータ保

護、SnapMirrorによるレプリケーションを実現します。VMware ワークロードを保護するためにネイティブのハイブリッドマルチクラウド統合を活用し、多数の自動化ツールやオーケストレーションツールを簡単に利用できます。

SnapMirrorをアレイベースのレプリケーションに使用すると、実績のある成熟したONTAPのテクノロジを活用できます。SnapMirror を使用すると、 VM やデータストア全体ではなく、変更されたファイルシステムブロックのみをコピーして、データを安全かつ効率的に転送できます。重複排除、圧縮、コンパクションなどのスペース削減効果を活用できます。最新の ONTAP システムで、バージョンに依存しない SnapMirror が使用されるようになり、ソースとデスティネーションのクラスタを柔軟に選択できるようになりました。SnapMirror は、災害復旧のための最も強力なツールの 1 つとなりました。

従来の NFS 、 iSCSI 、ファイバチャネル接続データストア（現在は VVOL データストアをサポート）のいずれを使用している場合でも、 SRM は、ディザスタリカバリやデータセンター移行の計画とオーケストレーションに ONTAP の機能のメリットを活用する堅牢なファーストパーティ製品を提供します。

**SRM** での **ONTAP 9** の活用方法

SRM は、 ONTAP システムの高度なデータ管理テクノロジを活用して、 3 つの主要コンポーネントで構成される仮想アプライアンスである VMware vSphere 用 ONTAP ツールと統合します。

- vCenter プラグイン（旧 Virtual Storage Console （ VSC ））は、 SAN と NAS のどちらを使用している場合でも、ストレージ管理と効率化機能の簡易化、可用性の向上、ストレージコストと運用オーバーヘッドの削減を実現します。データストアのプロビジョニングのベストプラクティスを使用して、 NFS 環境およびブロックストレージ環境用の ESXi ホスト設定を最適化します。以上のメリットのために、 ONTAP ソフトウェアを実行するシステムで vSphere を使用する場合はこのプラグインを推奨します。
- VASA Provider for ONTAP は、 VMware vStorage APIs for Storage Awareness （ VASA ）フレームワークをサポートしています。VASA Provider では、 VM ストレージのプロビジョニングと監視に役立つように vCenter Server と ONTAP を接続します。VMware Virtual Volumes （ VVol ）のサポートと、ストレージ機能プロファイル（ VVol レプリケーション機能を含む）の管理、および個々の VM VVol のパフォーマンスの管理が可能になります。また、容量の監視やプロファイルへの準拠に関するアラームも生成されます。SRM と一緒に使用すると、 VASA Provider for ONTAP で VVOL ベースの仮想マシンをサポートできます。 SRM サーバに SRA アダプタをインストールする必要はありません。
- SRA は SRM と一緒に使用され、従来の VMFS データストアと NFS データストアの本番サイトとディザスタリカバリサイト間での VM データのレプリケーションを管理します。また、 DR レプリカの無停止テストにも使用できます。検出、リカバリ、再保護のタスクを自動化します。Windows SRM サーバおよび SRM アプライアンス用の SRA サーバアプライアンスと SRA アダプタの両方が含まれています。

SRM サーバに SRA アダプタをインストールして設定し、 VASA Provider で VVol 以外のデータストアを保護したり VVOL のレプリケーションを有効にしたりしたあとで、ディザスタリカバリ用に vSphere 環境を設定する作業を開始できます。

SRA と VASA Provider には、 SRM サーバ用のコマンド / 制御インターフェイスが用意されており、 VMware 仮想マシン（ VM ）を含む ONTAP FlexVol や、 SRA を保護する SnapMirror レプリケーションを管理できます。

SRM 8.3 以降では、 SRM サーバへの新しい SRM VVol Provider 制御パスが導入され、 SRA を使用せずに vCenter サーバおよびその経由で VASA Provider に通信できるようになりました。これにより、 SRM サーバは緊密に統合するための完全な API を提供するため、以前よりもはるかに ONTAP クラスタの制御を活用できました。

SRMでは、ネットアップ独自のFlexCloneテクノロジを使用して、システムを停止することなくDR計画をテストし、保護されたデータストアのクローンをDRサイトにほぼ瞬時に作成できます。SRM はサンドボックスを作成して安全にテストし、真の災害が発生した場合に組織とお客様を保護します。そのため、組織は災害時

にフェイルオーバーを実行できます。

実際に災害が発生した場合や、計画的な移行の場合でも、 SRM では、最終的な SnapMirror 更新（必要な場合）を使用して、データセットに最新の変更を送信できます。その後、ミラーを解除し、 DR ホストにデータストアをマウントします。この時点で、計画済みの戦略に基づいて、 VM の電源を任意の順序で自動的にオンにすることができます。

#### **SRM** と **ONTAP** などのユースケース：ハイブリッドクラウドと移行

SRM 環境に ONTAP の高度なデータ管理機能を統合することで、ローカルストレージオプションに比べて、拡張性とパフォーマンスが大幅に向上します。それだけではありませんが、ハイブリッドクラウドの柔軟性を備えています。ハイブリッドクラウドを使用すると、 FabricPool を使用して、未使用のデータブロックをハイパフォーマンスアレイから希望するハイパースケーラに階層化してコストを削減できます。これは、 NetApp StorageGRID などのオンプレミスの S3 ストアである可能性があります。また、 ONTAP Select （ CVO ）やを使用して、ソフトウェアで定義される Cloud Volumes ONTAP やクラウドベースの DR でエッジベースのシステムに SnapMirror を使用することもできます "Equinix 内の NetApp Private Storage" Amazon Web Services （ AWS ）、 Microsoft Azure 、 Google Cloud Platform （ GCP ）で、クラウド内に完全に統合されたストレージ、ネットワーク、コンピューティングサービスのスタックを構築できます。

その後、FlexCloneを使用すれば、ストレージの設置面積をほぼゼロに抑えながら、クラウドサービスプロバイダのデータセンター内でテストフェイルオーバーを実行できます。組織を保護することで、かつてないほどコストを削減できます。

SRM は、 SnapMirror を使用して、計画的な移行を実行することもできます。これにより、 VM を 1 つのデータセンターから別のデータセンターに効率的に転送したり、独自のデータセンターや、任意の数のネットアップパートナーサービスプロバイダを介して VM を転送したりできます。

## 導入のベストプラクティス

次のセクションでは、ONTAPとVMware SRMを使用した導入のベストプラクティスについて説明します。

#### **SMT** の **SVM** のレイアウトとセグメント化

ONTAP では、 Storage Virtual Machine （ SVM ）の概念を採用して、セキュアなマルチテナント環境で厳密にセグメント化します。ある SVM の SVM ユーザは、別の SVM のリソースにアクセスしたりリソースを管理したりすることはできませんこれにより、 ONTAP テクノロジを活用できます。ビジネスユニットごとに別々の SVM を作成して、同じクラスタ上で独自の SRM ワークフローを管理することで、全体的なストレージ効率を高めることができます。

SVM を対象としたアカウントと SVM 管理 LIF を使用して ONTAP を管理することを検討し、セキュリティ制御を強化するだけでなく、パフォーマンスも向上させます。SRA は、物理リソースを含むクラスタ全体のすべてのリソースを処理する必要がないため、 SVM を対象とした接続を使用する場合は本質的にパフォーマンスが向上します。その代わり、特定の SVM に抽象化された論理資産だけを認識する必要があります。

NAS プロトコルのみを使用する（ SAN アクセスなし）場合は、次のパラメータを設定することで、 NAS 向けに最適化された新しいモードを利用することもできます（ SRA と VASA は、アプライアンスで同じバックエンドサービスを使用するため）。

1. コントロールパネルにログインします。 `https://<IP address>:9083` [Web based CLI interface]をクリックします。
2. コマンドを実行します `vp updateconfig -key=enable.qtree.discovery -value=true`。

3. コマンドを実行します `vp updateconfig -key=enable.optimised.sra -value=true`。
4. コマンドを実行します `vp reloadconfig`。

**VVOL** に **ONTAP** ツールを導入する際の考慮事項について説明します

SRM で VVol を使用する場合は、クラスタを対象としたクレデンシャルとクラスタ管理 LIF を使用してストレージを管理する必要があります。これは、 VM ストレージポリシーに必要なポリシーを満たすためには、VASA Provider で基盤となる物理アーキテクチャを理解しておく必要があるためです。たとえば、オールフラッシュストレージを必要とするポリシーが設定されている場合、 VASA Provider では、どのシステムがオールフラッシュであるかを認識できる必要があります。

ONTAP Tools アプライアンスを管理している VVOL データストアに格納しないことを推奨します。その結果、アプライアンスがオフラインのためにアプライアンスのスワップ VVOL を作成できず、 VASA Provider の電源をオンにできなくなることがあります。

**ONTAP 9** システムの管理に関するベストプラクティス

前述したように、クラスタまたは SVM を対象としたクレデンシャルと管理 LIF を使用して ONTAP クラスタを管理できます。パフォーマンスを最適化するには、VVOLを使用しないときは常にSVMを対象としたクレデンシャルの使用を検討してください。ただし、その場合は、いくつかの要件について確認しておく必要があります。また、機能の一部は失われます。

- デフォルトの vsadmin SVM アカウントには、 ONTAP ツールのタスクを実行するために必要なアクセスレベルがありません。そのため、新しい SVM アカウントを作成する必要があります。
- ONTAP 9.8以降を使用している場合はNetApp、ONTAP System Managerの[Users]メニューとONTAP toolsアプライアンスにあるjsonファイルを使用して、RBACの最小権限を持つユーザアカウントを作成することを推奨します。 `https://<IP address>:9083/vsc/config/`。管理者パスワードを使用して JSON ファイルをダウンロードしてください。これは SVM またはクラスタを対象としたアカウントに使用できます。

  ONTAP 9.6 以前を使用している場合は、で使用可能な RBAC User Creator （ RUC ）ツールを使用する必要があります "NetApp Support Siteの Toolchest"。

- vCenter UI プラグイン、 VASA Provider 、 SRA サーバはすべて完全に統合されたサービスであるため、vCenter UI で ONTAP ツール用のストレージを追加する場合と同じ方法で、 SRM で SRA アダプタにストレージを追加する必要があります。そうしないと、 SRA サーバが SRA アダプタ経由で SRM から送信された要求を認識しない可能性があります。
- SVM を対象としたクレデンシャルを使用している場合、 NFS パスのチェックは実行されませんこれは、物理的な場所が SVM から論理的に抽象化されているためです。ただしこれは原因の問題ではありません。最新の ONTAP システムで間接パスを使用してもパフォーマンスが著しく低下することはなくなりました。
- Storage Efficiency によるアグリゲートのスペース削減量が報告されないことがあります。
- サポートされている場合、負荷共有ミラーを更新することはできません。
- SVM を対象としたクレデンシャルで管理されている ONTAP システムでは、 EMS ロギングが実行されない場合があり

## 運用上のベストプラクティス

以降のセクションでは、VMware SRMとONTAPストレージの運用に関するベストプラク

ティスについて説明します。

データストアおよびプロトコル

- 可能であれば、必ず ONTAP ツールを使用してデータストアとボリュームをプロビジョニングしてください。ボリューム、ジャンクションパス、 LUN 、 igroup 、エクスポートポリシーが その他の設定は互換性のある方法で構成されます。
- SRM では、 ONTAP 9 で iSCSI 、ファイバチャネル、および NFS バージョン 3 をサポートしているのは、 SRA 経由のアレイベースのレプリケーションを使用している場合です。SRM は、従来のデータストアまたは VVOL データストアでの NFS バージョン 4.1 のアレイベースのレプリケーションをサポートしていません。
- 接続を確認するために、 DR サイトの新しいテスト用データストアをデスティネーション ONTAP クラスタからマウントしてアンマウントできることを必ず確認してください。データストアの接続に使用する各プロトコルをテストします。テスト用データストアは SRM の指示に従ってすべてのデータストアの自動化を実行するため、 ONTAP ツールを使用して作成することを推奨します。
- SAN プロトコルは各サイトで同機種にする必要があります。NFS と SAN を混在させることはできますが、 SAN プロトコルを 1 つのサイト内に混在させないでください。たとえば、サイト A では FCP を、サイト B では iSCSI を使用できますサイト A では、 FCP と iSCSI の両方を使用しないでくださいその理由は、 SRA がリカバリサイトに混在する igroup を作成しないため、 SRM が SRA に指定されたイニシエータリストをフィルタリングしないためです。
- 以前のガイドでは、データの局所性にLIFを作成することを推奨つまり、必ず、ボリュームを物理的に所有するノード上の LIF を使用してデータストアをマウントします。これは、 ONTAP 9 の最新バージョンでは必須ではなくなりました。可能なかぎり、クラスタを対象としたクレデンシャルを指定した場合でも、ONTAPツールではデータに対してローカルなLIF間で負荷を分散するように選択されますが、高可用性やパフォーマンスを確保するための必須要件ではありません。
- ONTAP 9では、オートサイズが緊急時に十分な容量を提供できない場合に、スペース不足が発生したときにSnapshotを自動的に削除してアップタイムを維持するように設定できます。この機能のデフォルト設定では、SnapMirrorで作成されたSnapshotは自動的に削除されません。SnapMirror Snapshotが削除されると、NetApp SRAは影響を受けたボリュームのレプリケーションを反転および再同期できません。ONTAPがSnapMirror Snapshotを削除しないようにするには、Snapshotの自動削除機能をtryに設定します。

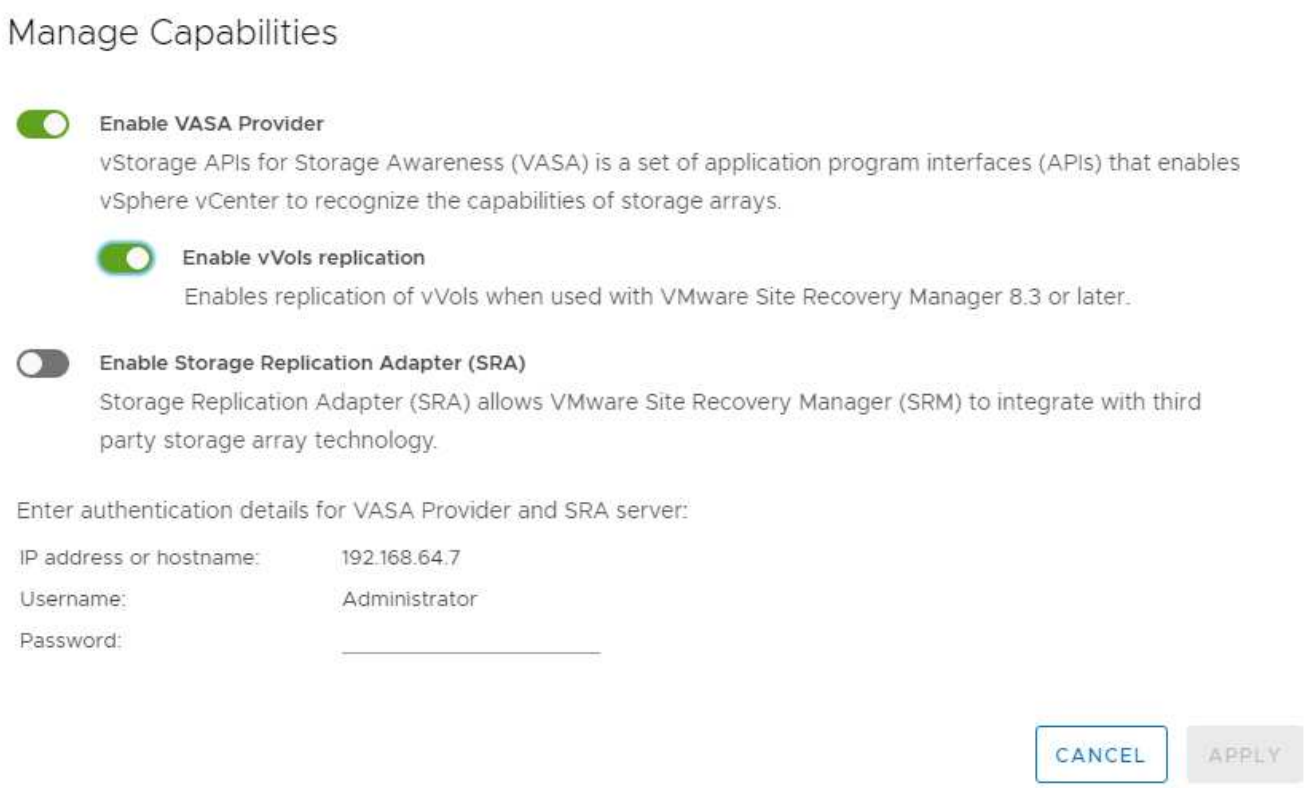
```
snap autodelete modify -volume -commitment try
```

- ボリュームのオートサイズの設定： `grow` SANデータストアヲフクムボリューム `grow_shrink` （NFSデータストアの場合）。の詳細を確認してください "ボリュームを自動的に拡張または縮小するための設定"。
- SRMは、データストアの数が少なく、保護グループがリカバリプランで最小化されている場合に最適なパフォーマンスを発揮します。したがって、RTOが重要なSRMで保護された環境では、VM密度の最適化を検討する必要があります。
- Distributed Resource Scheduler（DRS）を使用して、保護対象のESXiクラスタとリカバリESXiクラスタの負荷を分散します。フェイルバックを計画している場合、再保護を実行すると、以前に保護されていたクラスタが新しいリカバリクラスタになります。DRSは、両方向への配置のバランスをとるのに役立ちます。
- SRMでIPカスタマイズを使用するとRTOが増加する可能性があるため、可能な場合は使用しないでください。

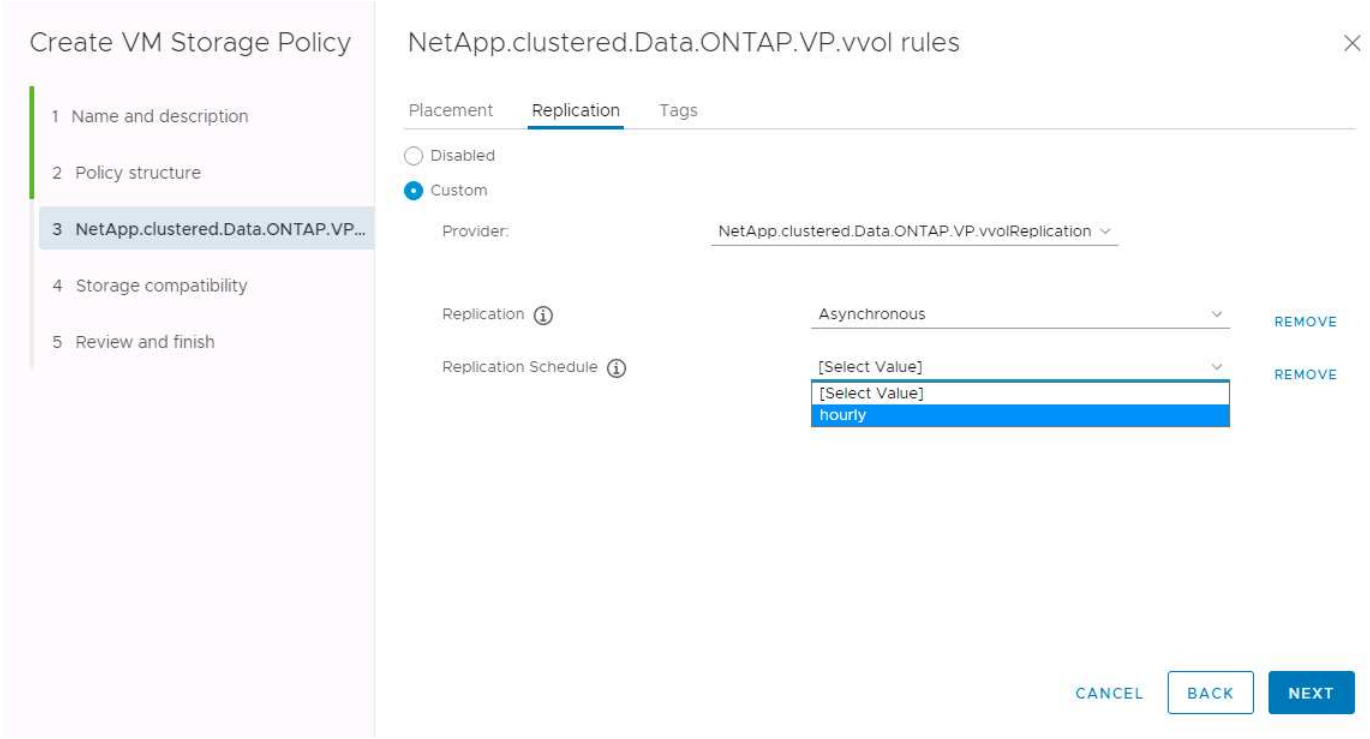
**Storage Policy Based Management（SPBM；ストレージポリシーベースの管理）とVVOL**

SRM 8.3以降では、vVolデータストアを使用したVMの保護がサポートされます。SnapMirror スケジュールは、次のスクリーンショットに示すように、 ONTAP のツール設定メニューで VVOL のレプリケーションが有効になっている場合、 VASA Provider によって VM ストレージポリシーに公開されます。

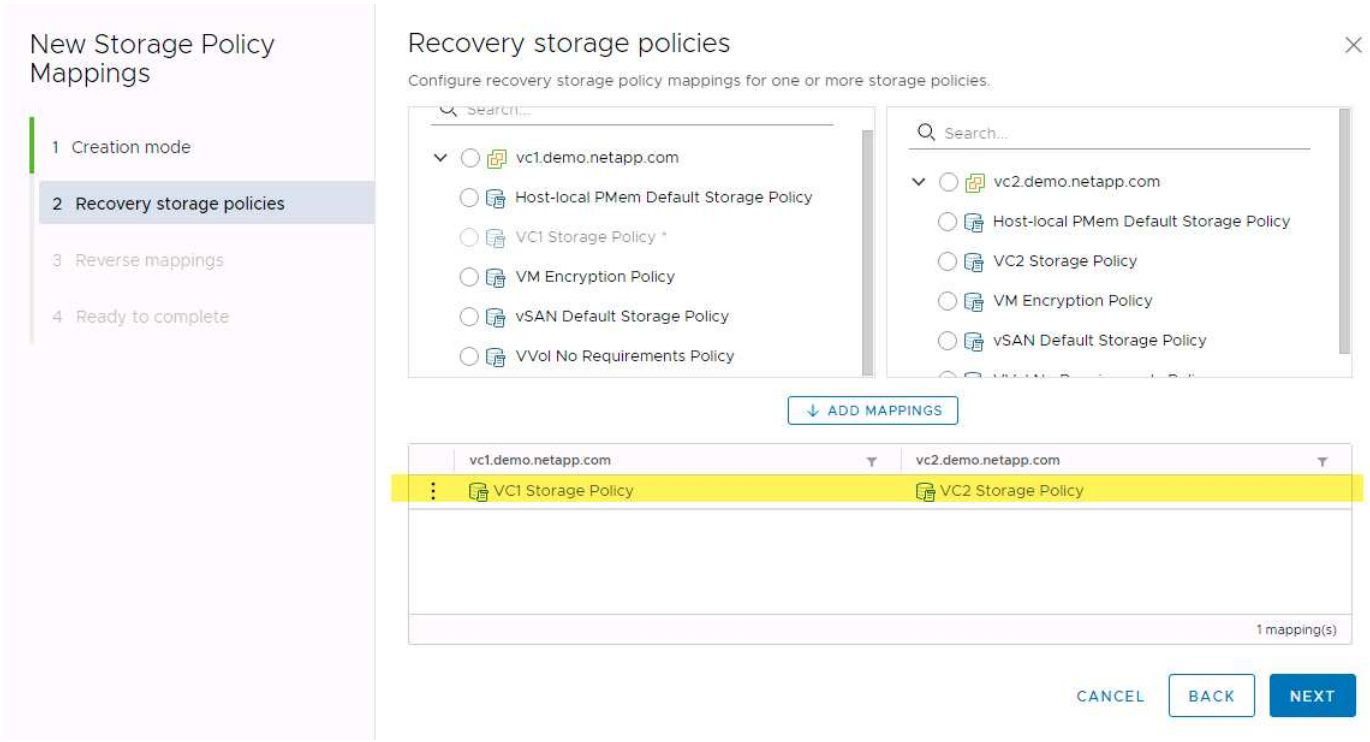
次の例は、vVolレプリケーションを有効にする方法を示しています。




次のスクリーンショットは、 VM ストレージポリシーの作成ウィザードに表示される SnapMirror スケジュールの例を示しています。




ONTAP VASA プロバイダでは、異なるストレージへのフェイルオーバーがサポートされます。たとえば、システムは、エッジの場所にある ONTAP Select からコアデータセンターの AFF システムにフェイルオーバーできます。ストレージの類似性に関係なく、レプリケーションが有効な VM ストレージポリシーのストレージポリシーマッピングとリバースマッピングを常に設定して、リカバリサイトで提供されるサービスが期待される要件を満たしていることを確認する必要があります。次のスクリーンショットは、ポリシーマッピングの例を示しています。



**VVOL** データストア用にレプリケートされたボリュームを作成します

以前の VVOL データストアとは異なり、レプリケートされた VVOL データストアはレプリケーションを有効にして最初から作成する必要があります。また、 SnapMirror 関係を持つ ONTAP システムで事前に作成されたボリュームを使用する必要があります。そのためには、クラスタピアリングや SVM ピアリングなどの設定を事前に行う必要があります。これらのアクティビティはONTAP管理者が実行する必要があります。これにより、複数のサイトでONTAPシステムを管理する担当者とvSphereの運用を主に担当する担当者が厳密に分離されます。

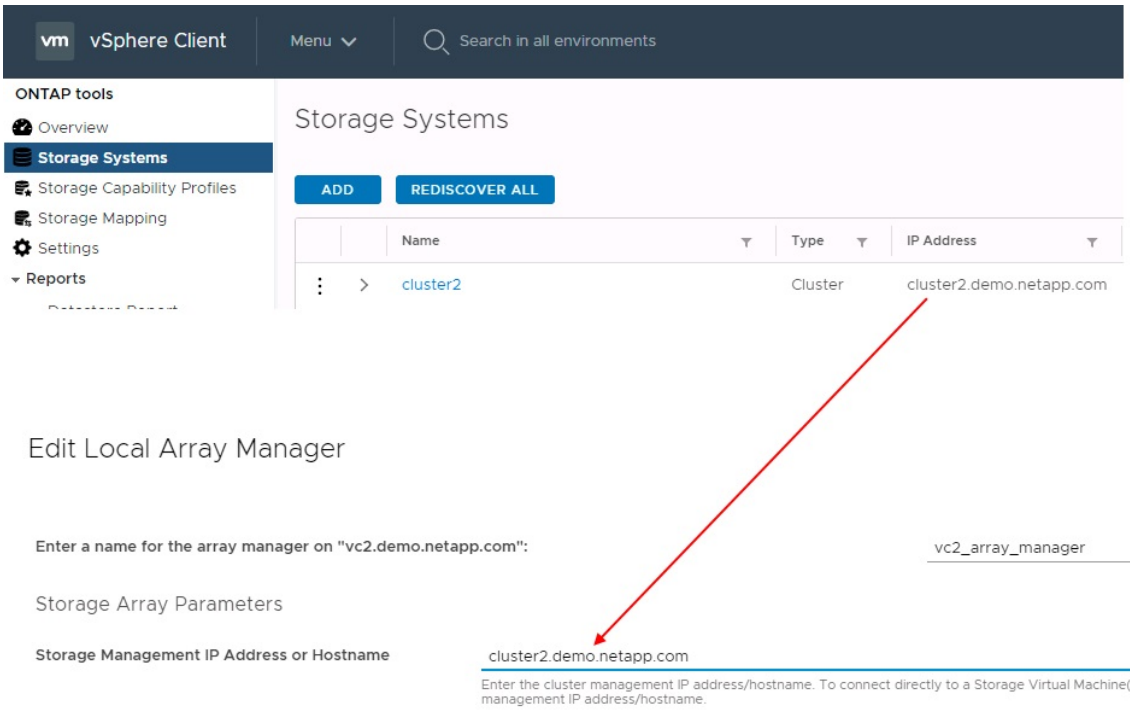
これは、 vSphere 管理者の代わりに新たな要件となります。ボリュームは ONTAP ツールの範囲外に作成されるため、定期的な再検出スケジュール期間が設定されるまで ONTAP 管理者が行った変更を認識することはありません。そのため、 VVOL で使用するボリュームまたは SnapMirror 関係を作成したときは常に再検出を実行することを推奨します。次のスクリーンショットに示すように、ホストまたはクラスタを右クリックし、ONTAP tools]>[Update Host and Storage Data]を選択します。


VVOL と SRM については、 1 つ注意が必要です。保護された VM と保護されていない VM を同じ VVOL データストアに混在させないでください。これは、 SRM を使用して DR サイトにフェイルオーバーする場合、保護グループに属する VM のみが DR でオンラインになるためです。そのため、再保護（ SnapMirror を DR から本番環境に戻して再保護）する際に、フェイルオーバーされなかった VM が上書きされて、貴重なデータが含まれる可能性があります。

アレイペアについて

アレイペアごとにアレイマネージャが作成されます。SRM ツールと ONTAP ツールでは、クラスタクレデンシャルを使用している場合でも、各アレイペアリングを SVM の範囲で実行します。これにより、管理対象に割り当てられている SVM を基に、各テナント間で DR ワークフローを分割できます。特定のクラスタに対して複数のアレイマネージャを作成し、非対称にすることができます。異なる ONTAP 9 クラスタ間でファンアウトまたはファンインを実行できます。たとえば、クラスタ 1 の SVM A と SVM B をクラスタ 2 の SVM C に、クラスタ 3 の SVM D に、またはその逆にレプリケートできます。

SRM でアレイペアを設定する場合は、 ONTAP ツールに追加するのと同じ方法でアレイペアを SRM に追加する必要があります。つまり、アレイペアは同じユーザ名、パスワード、および管理 LIF を使用する必要があります。これは、 SRA がアレイと正しく通信するための要件です。次のスクリーンショットは、 ONTAP ツールでのクラスタの表示方法と、アレイマネージャへのクラスタの追加方法を示しています。







### 複製グループについて

レプリケーショングループには、同時にリカバリされる仮想マシンの論理集合が含まれます。レプリケーショングループは、 ONTAP ツール VASA Provider で自動的に作成されます。ONTAP の SnapMirror レプリケーションはボリュームレベルで実行されるため、ボリューム内のすべての VM が同じレプリケーショングループに属します。

レプリケーショングループについて考慮する必要がある要素と、 FlexVol ボリュームに VM を分散する方法にはいくつかの要素があります。類似するVMを同じボリュームにグループ化すると、アグリゲートレベルの重複排除機能がない古いONTAPシステムでストレージ効率を高めることができますが、グループ化するとボリュームのサイズが大きくなり、ボリュームのI/Oの同時実行数が少なくなります。最新のONTAPシステムでは、同じアグリゲート内のFlexVolボリュームにVMを分散することで、パフォーマンスとストレージ効率の最適なバランスを実現できます。その結果、アグリゲートレベルの重複排除が活用され、複数のボリューム間でI/Oの並列化が促進されます。保護グループ（以下で説明）には複数のレプリケーショングループを含めることができるため、ボリューム内の VM を 1 つにまとめてリカバリできます。このレイアウトの欠点は、Volume SnapMirrorではアグリゲートの重複排除が考慮されないため、ブロックがネットワーク経由で複数回送信される可能性があることです。

レプリケーショングループの最後の考慮事項の 1 つは、各グループがその性質によって論理整合グループになることです（ SRM 整合グループと混同しないようにしてください）。これは、ボリューム内のすべての VM が同じ Snapshot を使用して同時に転送されるためです。したがって、相互に整合性が必要な VM がある場合は、同じ FlexVol に格納することを検討してください。

### 保護グループについて

保護グループでは、 VM とデータストアをグループ単位で定義し、グループをまとめて保護サイトからリカバリします。保護対象サイトとは、通常の安定状態での運用中、保護グループで構成された VM が存在する場所です。SRM には保護グループの複数のアレイマネージャが表示される場合がありますが、保護グループは複数のアレイマネージャにまたがることはできません。このため、異なる SVM 上の複数のデータストアに VM ファイルをまたがって配置することはできません。

### リカバリ・プランについて

リカバリプランでは、同じプロセスでリカバリする保護グループを定義します。同じリカバリプランに複数の保護グループを設定できます。また、リカバリプランの実行オプションを増やすには、 1 つの保護グループを複数のリカバリプランに含めることもできます。

リカバリプランを使用すると、 SRM 管理者は、 VM を優先グループ 1 （最大）から 5 （最小）に割り当てて、リカバリワークフローを定義できます。デフォルトは 3 （中）です。優先度グループ内で、 VM に依存関係を設定できます。

たとえば、データベースにMicrosoft SQL Serverを使用するティア1のビジネスクリティカルなアプリケーションがあるとします。したがって、優先度グループ 1 に VM を配置することにします。優先度グループ 1 では、サービスの提供順序の計画を開始します。Microsoft Windows ドメイン・コントローラを起動してから Microsoft SQL Server を起動してください。アプリケーション・サーバの前にオンラインになっている必要があります。依存関係は特定の優先度グループ内でのみ適用されるため、これらすべてのVMを優先度グループに追加してから依存関係を設定します。

アプリケーションチームと連携してフェイルオーバーシナリオに必要な処理の順序を把握し、それに応じてリカバリ計画を作成することを強く推奨します。

### テストフェイルオーバー

ベストプラクティスとして、保護対象の VM ストレージの構成を変更する場合は、必ずテストフェイルオーバーを実行してください。これにより、災害が発生した場合に、Site Recovery Managerが予想されるRTOターゲット内でサービスをリストアできると信頼できます。

特に VM ストレージの再設定後にゲストアプリケーションの機能を確認することを推奨します。

テストリカバリ処理を実行すると、 VM 用の ESXi ホストにプライベートテスト用のバブルネットワークが作成されます。ただし、このネットワークは物理ネットワークアダプタに自動的には接続されないため、 ESXi ホスト間の接続は提供されません。DR テスト時に異なる ESXi ホストで実行されている VM 間の通信を可能にするために、 DR サイトの ESXi ホスト間に物理プライベートネットワークを作成します。テスト用ネットワークがプライベートであることを確認するために、テスト用のバブルネットワークを物理的に分離するか、 VLAN や VLAN タギングを使用して分離します。このネットワークは本番用ネットワークから分離する必要があります。 VM がリカバリされると、実際の本番用システムと競合する可能性のある IP アドレスを持つ本番用ネットワークに配置することはできなくなります。SRM でリカバリプランを作成する際、テスト中に VM を接続するためのプライベートネットワークとして、作成したテストネットワークを選択できます。

テストが検証されて不要になったら、クリーンアップ処理を実行します。クリーンアップを実行すると、保護されている VM が初期状態に戻り、リカバリプランが Ready 状態にリセットされます。

### フェイルオーバーに関する考慮事項

サイトのフェイルオーバーに関しては、このガイドに記載されている処理の順序に加えて、その他にもいくつかの考慮事項があります。

競合する問題の 1 つに、サイト間のネットワークの違いがあります。環境によっては、プライマリサイトと DR サイトで同じネットワーク IP アドレスを使用できる場合があります。この機能は、拡張仮想 LAN （ VLAN ）または拡張ネットワークセットアップと呼ばれます。それ以外の環境では、プライマリサイトと DR サイトで別々のネットワーク IP アドレス（異なる VLAN など）を使用する必要があります。

VMware では、この問題を解決する方法をいくつか提供しています。1 つは、 VMware NSX -T Data Center のようなネットワーク仮想化テクノロジーです。ネットワークスタック全体を運用環境からレイヤ 2 ～ 7 に

抽象化し、より移植性の高いソリューションを実現します。の詳細を確認してください "SRMでのNSX-Tオプション"。

SRM では、リカバリ時に VM のネットワーク設定を変更することもできます。この再設定には、IPアドレス、ゲートウェイアドレス、DNSサーバ設定などの設定が含まれます。リカバリ時に個 々 のVMに適用されるさまざまなネットワーク設定は、リカバリプランのVMのプロパティ設定で指定できます。

VMware の dr-ip-customizer というツールを使用すると、リカバリプランで複数の VM のプロパティを個別に編集しなくても、 SRM で VM ごとに異なるネットワーク設定を適用できます。このユーティリティの使用方法については、を参照してください。 "VMwareのドキュメント"。

再保護

リカバリ後、リカバリサイトが新しい本番用サイトになります。リカバリ処理によって SnapMirror レプリケーションが解除されたため、新しい本番用サイトは今後の災害から保護されません。新しい本番用サイトは、リカバリ後すぐに別のサイトで保護することを推奨します。元の本番サイトが運用されている場合、 VMware 管理者は、元の本番サイトを新しいリカバリサイトとして使用して新しい本番サイトを保護できるため、保護の方向を実質的に変えることができます。再保護は、致命的でない障害でのみ使用できます。そのため、元の vCenter Server 、 ESXi サーバ、 SRM サーバ、および対応するデータベースを最終的にリカバリ可能な状態にする必要があります。使用できない場合は、新しい保護グループと新しいリカバリプランを作成する必要があります。

フェイルバック

フェイルバック処理は、基本的に以前とは異なる方向のフェイルオーバーです。ベストプラクティスとして、フェイルバックを実行する前に、元のサイトが許容可能なレベルの機能に戻っていること、つまり元のサイトにフェイルオーバーしていることを確認することを推奨します。元のサイトが侵害されたままの場合は、障害が十分に修正されるまでフェイルバックを遅らせる必要があります。

フェイルバックのもう 1 つのベストプラクティスとして、再保護の完了後、および最終フェイルバックの実行前に、常にテストフェイルオーバーを実行することがあります。これにより、元のサイトに配置されたシステムで処理が完了できるかどうかを確認できます。

元のサイトを再保護する

フェイルバック後、再保護を再度実行する前に、すべての関係者にサービスが正常に戻ったことを確認する必要があります。

フェイルバック後の再保護を実行すると、基本的に環境は最初の状態に戻り、 SnapMirror レプリケーションが本番用サイトからリカバリサイトに再度実行されます。

## レプリケーショントポロジ

ONTAP 9 では、クラスタの物理コンポーネントはクラスタ管理者には見えますが、クラスタを使用しているアプリケーションやホストからは直接見えません。物理コンポーネントは共有リソースのプールを提供し、このリソースプールから論理クラスタリソースが構築されます。アプリケーションとホストは、ボリュームと LIF を含む SVM 経由でのみデータにアクセスします。

VMware vCenter Site Recovery Manager では、各 NetApp SVM がアレイとして扱われます。SRM は、特定のアレイ間（または SVM から SVM ）のレプリケーションレイアウトをサポートしています。

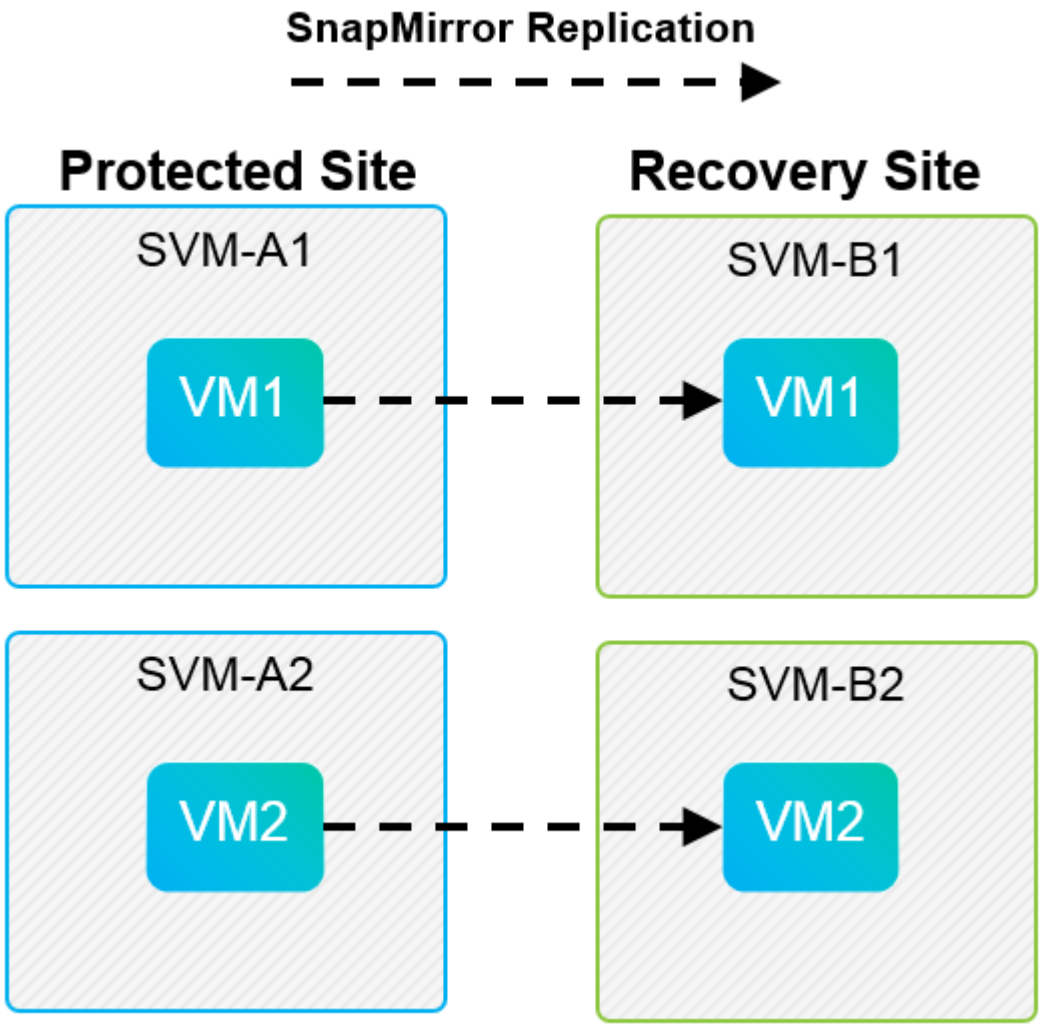
1 つの VM が、次の理由から、複数の SRM アレイ上で仮想マシンディスク（ VMDK ）または RDM を所有することはできません。

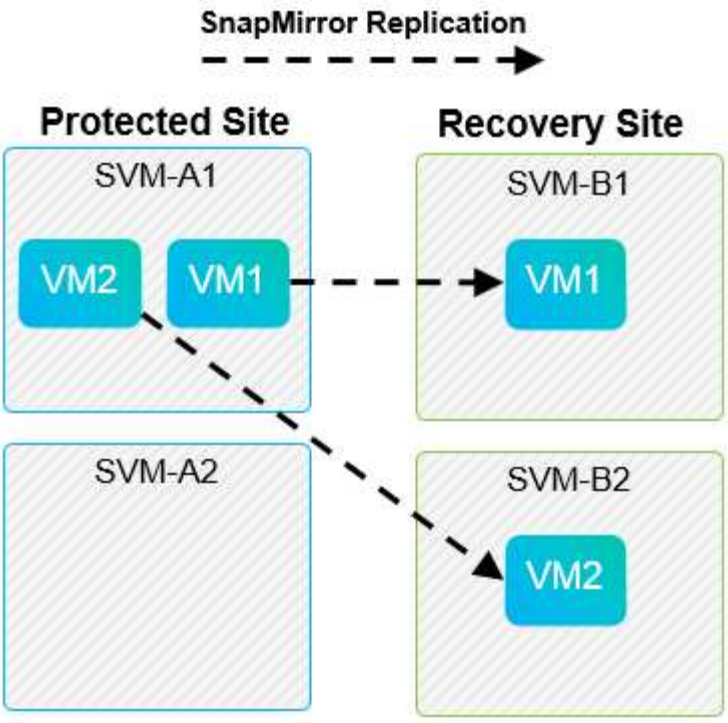
- SRM は SVM のみを認識し、個々の物理コントローラは認識しません。
- SVM は、クラスタ内の複数のノードにまたがる LUN とボリュームを制御できます。

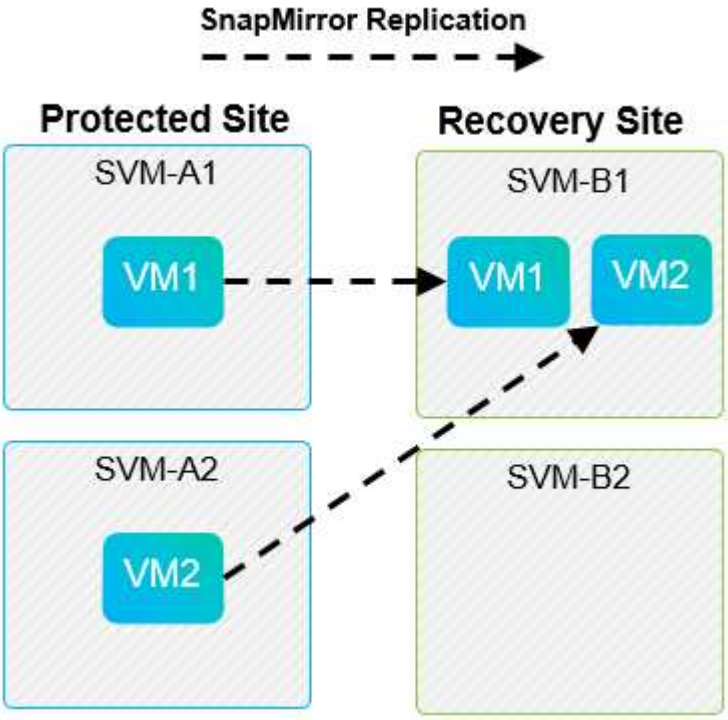
| ベストプラクティス |
| --- |
| サポートされるかどうかを判断するには、このルールに注意してください。 SRM と NetApp SRA を使用して VM を保護するには、 VM のすべての部分が 1 つの SVM 上にのみ存在する必要があります。このルールは、保護対象サイトとリカバリサイトの両方に適用されます。 |

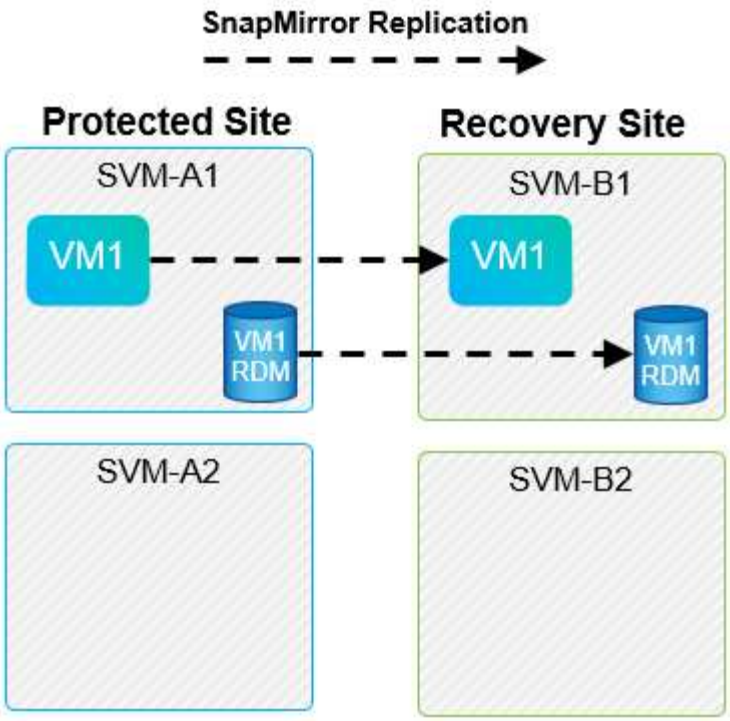
サポートされる **SnapMirror** レイアウト

次の図は、 SRM と SRA でサポートされる SnapMirror 関係のレイアウトシナリオを示しています。レプリケートされたボリューム内の各 VM は、各サイトの 1 つの SRM アレイ（ SVM ）上のデータのみを所有します。



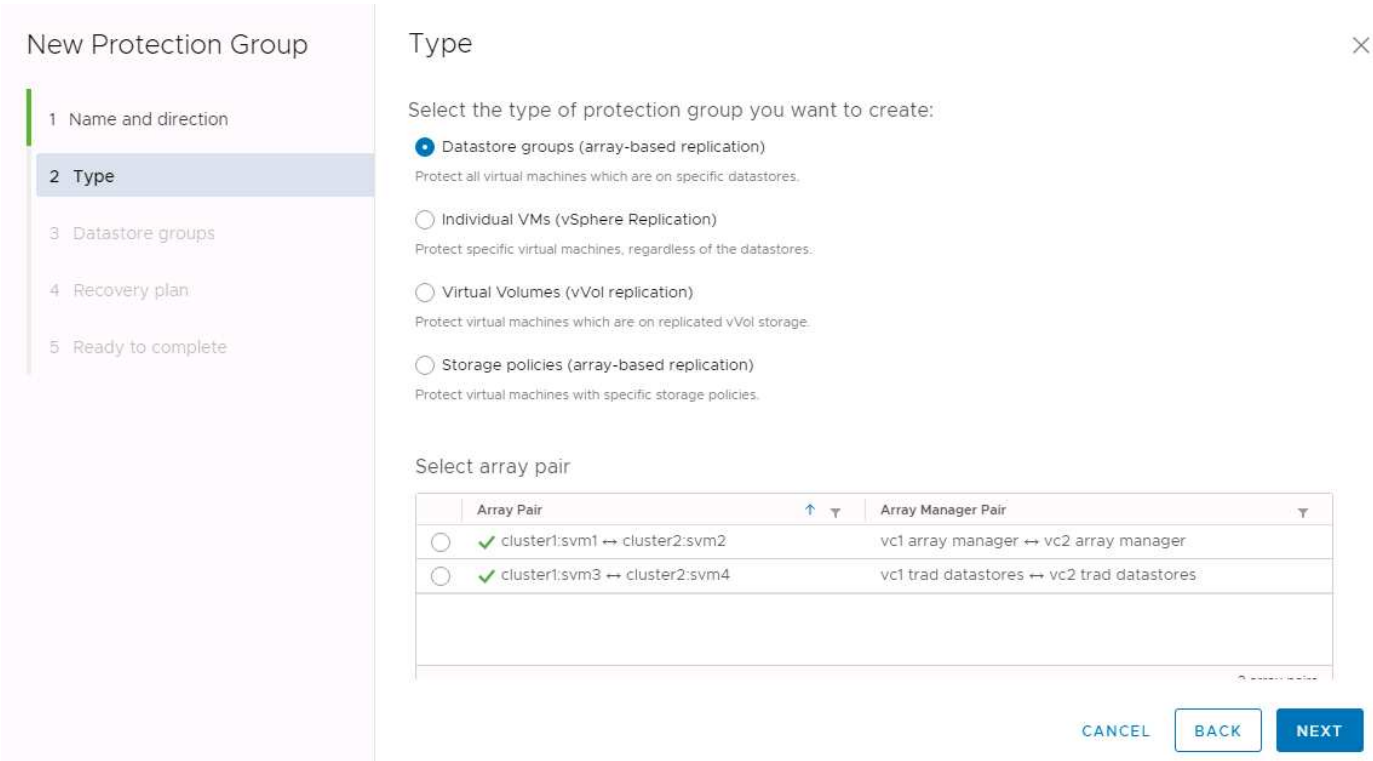

SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
SVM-B1
VM2
VM1
VM1
SVM-A2
SVM-B2
VM2


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
SVM-B1
VM1
VM1
VM2
SVM-A2
SVM-B2
VM2



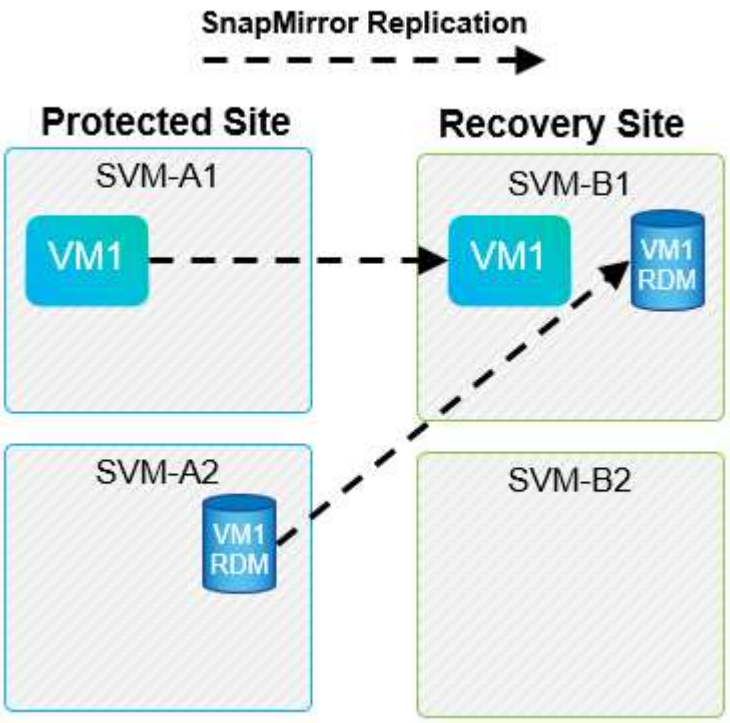

サポートされている **Array Manager** レイアウト

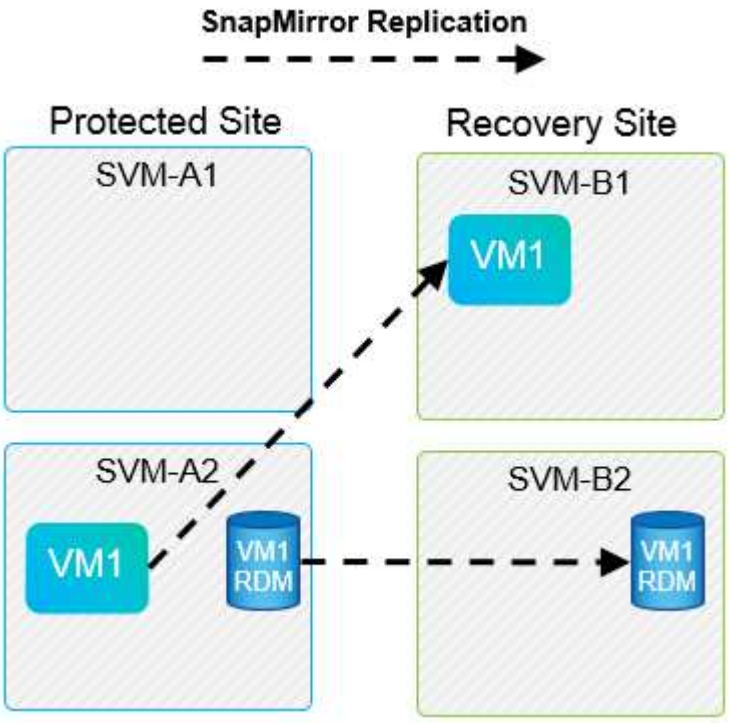
次のスクリーンショットに示すように、 SRM でアレイベースレプリケーション（ ABR ）を使用すると、保護グループは単一のアレイペアに分離されます。このシナリオでは、 `SVM1` および `SVM2` ピア関係を設定する `SVM3` および `SVM4` リカバリサイトで。ただし、保護グループを作成するときに選択できるアレイペアは 2 つのうちの 1 つだけです。



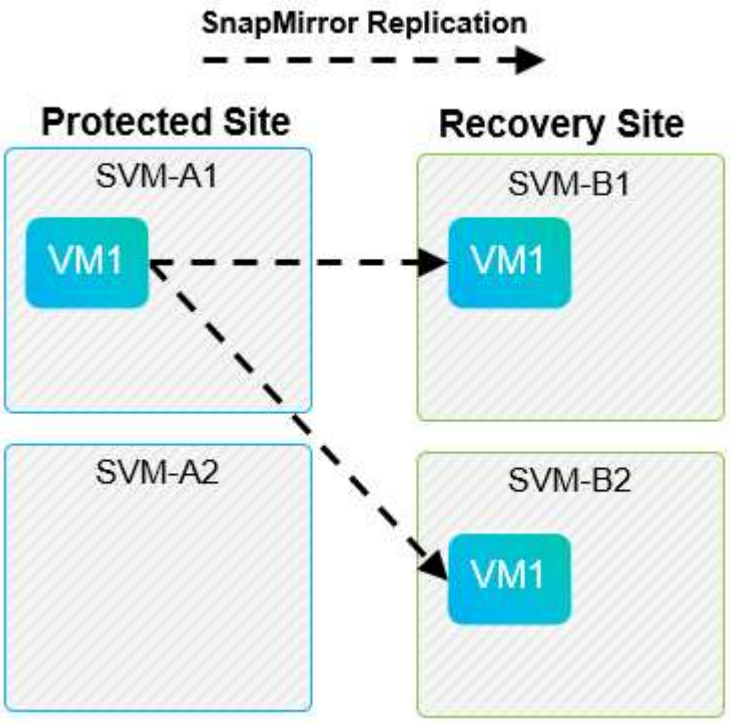
サポートされないレイアウトです

サポート対象外の構成では、個々の VM が所有する複数の SVM にデータ（ VMDK または RDM ）があります。次の図に示す例では、 `VM1` SRMで保護を設定できません。理由： `VM1` 2つのSVM上のデータがあります。



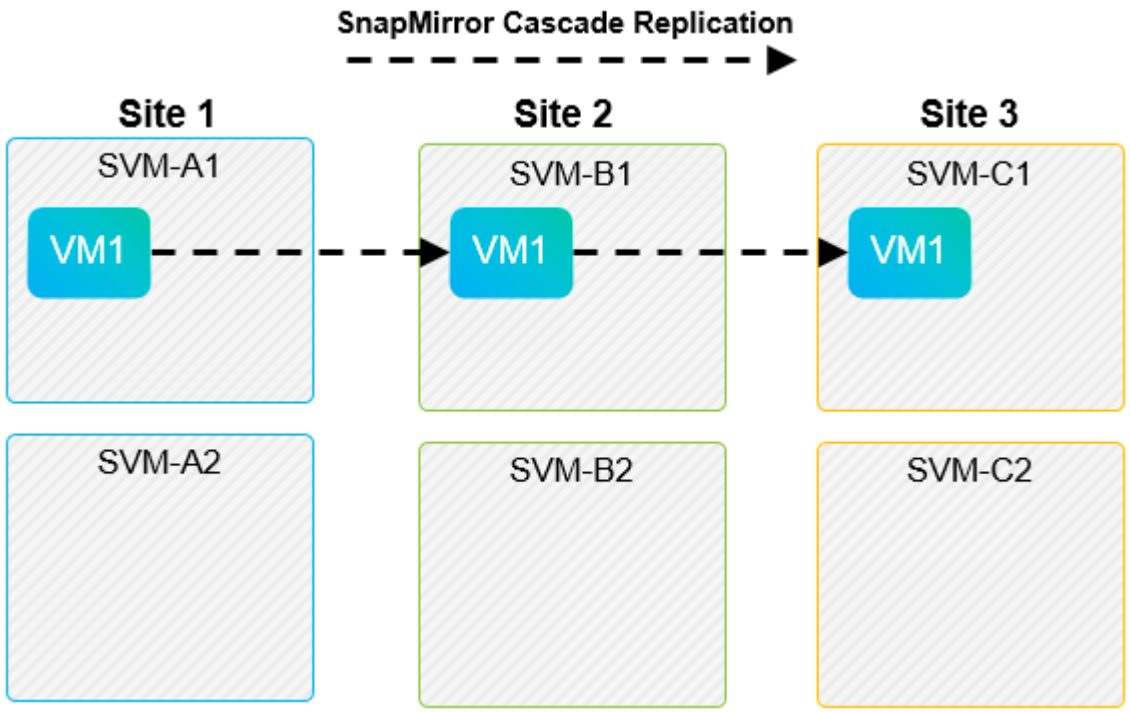




1 つのネットアップボリュームを 1 つのソース SVM から同じ SVM または異なる SVM の複数のデスティネーションにレプリケートするレプリケーション関係は、 SnapMirror ファンアウトと呼ばれます。SRM ではファンアウトはサポートされていません。次の図の例では、 `VM1` SnapMirrorを使用して2つの異なる場所にレプリケートされるため、SRMで保護を設定できません。




**SnapMirror** カスケード

SnapMirror でソースボリュームをデスティネーションボリュームにレプリケートし、そのデスティネーションボリュームを SnapMirror で別のデスティネーションボリュームにレプリケートする SnapMirror 関係のカスケードを、 SRM ではサポートしていません。次の図に示すシナリオでは、 SRM を使用してサイト間のフェイルオーバーを実行することはできません。



### SnapMirror と SnapVault

NetApp SnapVault ソフトウェアを使用すると、ネットアップストレージシステム間でエンタープライズデータをディスクベースでバックアップできます。SnapVault と SnapMirror は同じ環境内に共存できますが、SRM でサポートされているのは、 SnapMirror 関係のフェイルオーバーだけです。

NetApp SRAは、 `mirror-vault` ポリシータイプ。

SnapVault は ONTAP 8.2 で一から再構築されました。以前の Data ONTAP 7-Mode で使用されていたユーザは共通点に注意する必要がありましたが、このバージョンの SnapVault では主に拡張機能が追加されています。大きな進歩の 1 つは、 SnapVault 転送時にプライマリデータの Storage Efficiency を維持できることです。

アーキテクチャの重要な変更点は、 7-Mode SnapVault の場合と同様に、 ONTAP 9 の SnapVault でも qtree レベルではなくボリュームレベルでレプリケートされる点です。つまり、 SnapVault 関係のソースはボリュームでなければならず、そのボリュームは SnapVault セカンダリシステム上の独自のボリュームにレプリケートされる必要があります。

SnapVaultを使用する環境では、プライマリストレージシステム上に特別な名前のスナップショットが作成されます。実装されている構成に応じて、SnapVaultスケジュールまたはNetApp Active IQ Unified Managerなどのアプリケーションを使用して、名前付きSnapshotをプライマリシステムに作成できます。プライマリシステムで作成された名前付きSnapshotがSnapMirrorデスティネーションにレプリケートされ、そこからSnapVaultデスティネーションに保存されます。

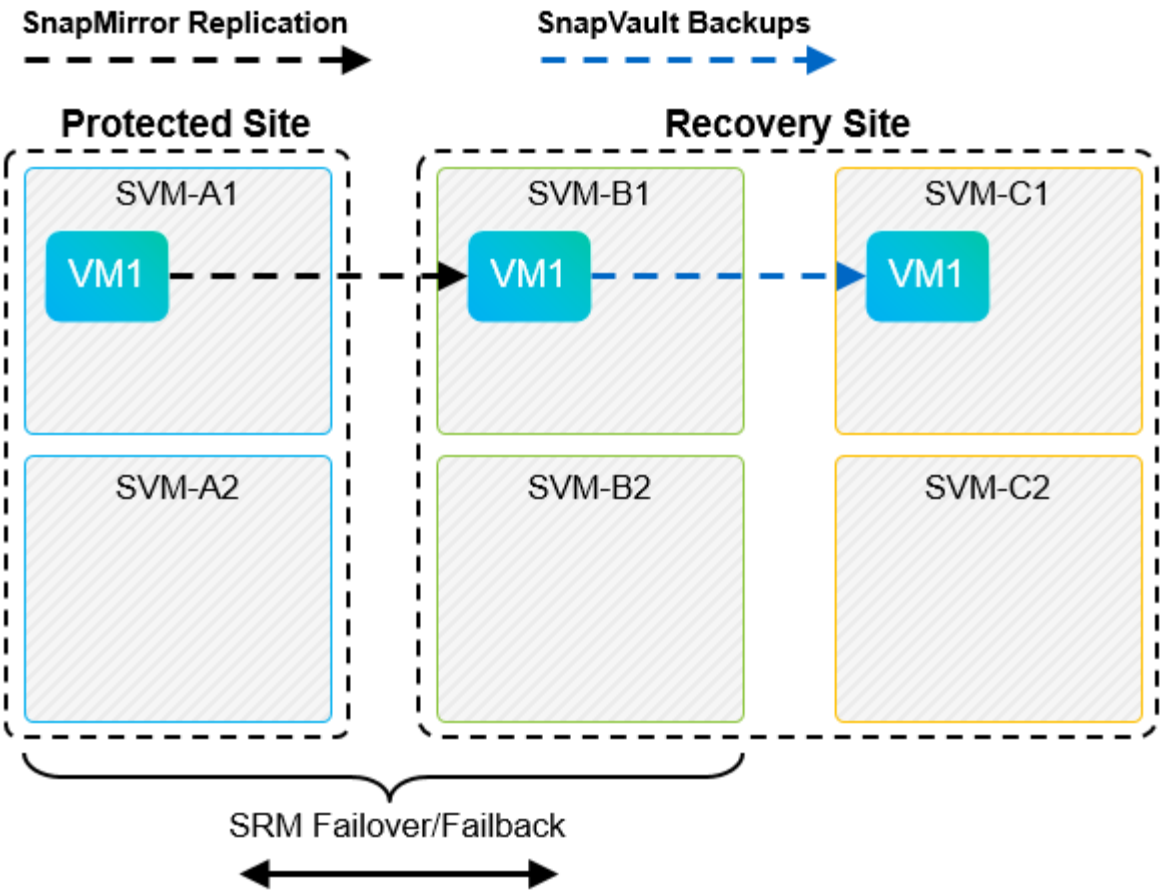
ソースボリュームは、ボリュームが DR サイトの SnapMirror デスティネーションにレプリケートされるカスケード構成で作成でき、そこから SnapVault デスティネーションに保存されます。ファンアウト関係では、一方のデスティネーションが SnapMirror デスティネーション、もう一方が SnapVault デスティネーションであるソースボリュームも作成できます。ただし、 SRM フェイルオーバーまたはレプリケーションの反転時に、SRA は、 SnapMirror デスティネーションボリュームを SnapVault のソースとして使用するように SnapVault 関係を自動では再設定しません。

SnapMirror および SnapVault for ONTAP 9 の最新情報については、を参照してください "TR-4015 ：『 SnapMirror Configuration Best Practice Guide for ONTAP 9 』"

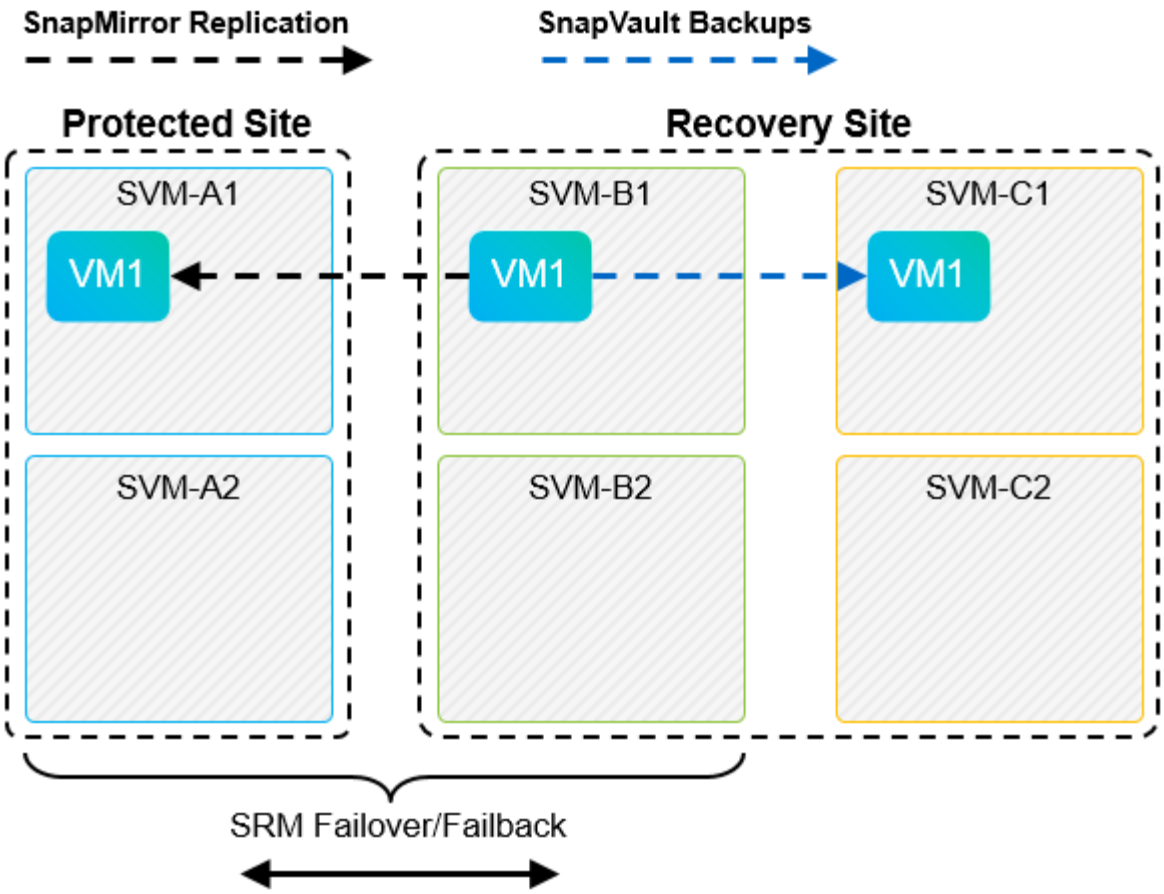
| ベストプラクティス |
| --- |
| SnapVault と SRM を同じ環境で使用する場合、通常は DR サイトの SnapMirror デスティネーションから SnapVault バックアップを実行する、 SnapMirror から SnapVault へのカスケード構成を使用することを推奨します。災害が発生すると、この構成によってプライマリサイトにアクセスできなくなります。リカバリサイトに SnapVault デスティネーションを配置すると、フェイルオーバー後に SnapVault バックアップを再設定して、リカバリサイトで SnapVault バックアップを継続できるようになります。 |

VMware 環境では、各データストアに Universal Unique Identifier （ UUID ）が割り当てられ、各 VM には一意の Managed Object ID （ MOID ）が割り当てられます。SRM は、フェイルオーバーやフェイルバックの実行時にこれらの ID を維持しません。SRM はフェイルオーバーでデータストア UUID と VM MOID を維持しないため、これらの ID に依存するアプリケーションは SRM フェイルオーバーのあとに再設定する必要があります。たとえば、 SnapVault レプリケーションを vSphere 環境と調整する NetApp Active IQ Unified Manager などがあります。

次の図に、 SnapMirror から SnapVault へのカスケード構成を示します。SnapVault デスティネーションがプライマリサイトの停止の影響を受けない DR サイトまたは第 3 のサイトにある場合、フェイルオーバー後にバックアップを続行できるように環境を再設定できます。




次の図は、 SRM を使用して SnapMirror レプリケーションをプライマリサイトに反転したあとの構成を示しています。SnapMirror ソースから SnapVault バックアップが実行されるように環境が再設定されている。このセットアップは、 SnapMirror SnapVault のファンアウト構成です。




SRM でフェイルバックを実行し、 SnapMirror 関係が再度反転されると、本番環境のデータはプライマリサイトに戻ります。SnapMirror と SnapVault のバックアップにより、 DR サイトへのフェイルオーバー前と同じ方法でこのデータを保護できるようになりました。

#### Site Recovery Manager 環境での qtree の使用

qtree は、 NAS のファイルシステムクォータを適用可能な特殊なディレクトリです。ONTAP 9 では qtree を作成でき、 SnapMirror でレプリケートされたボリュームに配置できます。ただし、 SnapMirror では、個々の qtree のレプリケーションまたは qtree レベルのレプリケーションは実行できません。すべての SnapMirror レプリケーションは、ボリュームレベルで実行されます。このため、 SRM で qtree を使用することは推奨されません。

#### FC と iSCSI の混在環境

サポート対象の SAN プロトコル（ FC 、 FCoE 、 iSCSI ）の場合、 ONTAP 9 は LUN サービスを提供します。 LUN サービスの提供とは、 LUN を作成して、接続されているホストにマッピングする機能です。クラスタは複数のコントローラで構成されるため、個々の LUN へのマルチパス I/O で管理される論理パスが複数あります。ホスト上で Asymmetric Logical Unit Access （ ALUA ；非対称論理ユニットアクセス）が使用されるため、 LUN への最適なパスが選択され、データ転送用にアクティブになります。LUN への最適パスが変わった場合（格納先ボリュームが移動された場合など）、 ONTAP 9 は自動的にこの変更を認識し、システムを停止することなく調整します。最適パスが利用できなくなった場合、 ONTAP は無停止で他の利用可能なパスに切り替えることができます。

VMware SRM と NetApp SRA の環境では、一方のサイトで FC プロトコルを使用し、もう一方のサイトで iSCSI プロトコルを使用できます。ただし、 FC 接続のデータストアと iSCSI 接続のデータストアを同じ ESXi ホストで混在させたり、同じクラスタ内の別のホストで使用したりすることはできません。この構成は SRM ではサポートされていません。 SRM フェイルオーバーまたはテストフェイルオーバーの実行中、 SRM

は要求に応じて ESXi ホストのすべての FC イニシエータと iSCSI イニシエータを含めます。

| ベストプラクティス |
| --- |
| SRM と SRA では、保護サイトとリカバリサイト間での FC プロトコルと iSCSI プロトコルの混在をサポートしています。ただし、各サイトで FC または iSCSI のどちらかのプロトコルを 1 つだけ使用し、同じサイトで両方のプロトコルを使用することはできません。1 つのサイトに FC プロトコルと iSCSI プロトコル両方を設定する必要がある場合、一部のホストで iSCSI を使用し、他のホストで FC を使用することを推奨します。また、 VM がどちらか一方のホストグループまたは他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されるように、 SRM リソースマッピングを設定することも推奨します。 |

## VVol レプリケーションを使用する場合の SRM のトラブルシューティング

SRM で VVOL レプリケーションを使用する場合、 SRA と従来のデータストアで使用するワークフローは大きく異なります。たとえば、アレイマネージャの概念はありません。そのため、 `discoverarrays` および `discoverdevices` コマンドは表示されません。

トラブルシューティングを行う場合は、以下に示す新しいワークフローについて理解しておくと役立ちます。

1. queryReplicationPeer ： 2 つのフォールトドメイン間のレプリケーション契約を検出します。
2. queryFaultDomain ：障害ドメインの階層を検出します。
3. queryReplicationGroup ：ソースドメインまたはターゲットドメインに存在するレプリケーショングループを検出します。
4. syncReplicationGroup ：ソースとターゲット間でデータを同期します。
5. queryPointInTimeReplica ：ターゲット上のポイントインタイムレプリカを検出します。
6. testFailoverReplicationGroupStart ：テストフェイルオーバーを開始します。
7. testFailoverReplicationGroupStop ：テストフェイルオーバーを終了します。
8. promoteReplicationGroup ：テスト中のグループを本番環境に昇格します。
9. prepareFailoverReplicationGroup ：災害復旧の準備をします。
10. FailoverReplicationGroup ：ディザスタリカバリを実行します。
11. revertReplicateGroup ：逆方向のレプリケーションを開始します。
12. queryMatchingContainer: 指定されたポリシーを使用したプロビジョニング要求を満たす可能性のあるコンテナを（ホストまたはレプリケーショングループとともに）検索します。
13. queryResourceMetadata ： VASA Provider からすべてのリソースのメタデータを検出し、リソース利用率を回答として queryMatchingContainer 関数に返すことができます。

VVOL レプリケーションの設定時に表示される最も一般的なエラーは、 SnapMirror 関係を検出できないエラーです。これは、ボリュームおよび SnapMirror 関係が ONTAP ツールを対象としたものではないためです。そのため、 SnapMirror 関係が常に完全に初期化されていることを確認し、レプリケートされた VVOL データストアを作成する前に両方のサイトの ONTAP ツールで再検出を実行することを推奨します。

## 追加情報

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web

サイトを参照してください。

- TR-4597 ：『 VMware vSphere for ONTAP 』
"https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- TR-4400 ：『 VMware vSphere Virtual Volumes with ONTAP 』
"https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- TR-4015 ：『 SnapMirror Configuration Best Practice Guide for ONTAP 9 』
https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P
- RBAC User Creator for ONTAP の略
"https://mysupport.netapp.com/site/tools/tool-eula/rbac"
- VMware vSphere リソース用の ONTAP ツール
"https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- VMware Site Recovery Manager のドキュメント
"https://docs.vmware.com/en/Site-Recovery-Manager/index.html"

を参照してください "Interoperability Matrix Tool （ IMT ）" NetApp Support Siteで、本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかを確認してください。NetApp IMT には、ネットアップがサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

# ONTAPを使用したvSphere Metroストレージクラスタ

## ONTAPを使用したvSphere Metroストレージクラスタ

VMwareの業界をリードするvSphereハイパーバイザーは、vSphere Metro Storage Cluster（vMSC）と呼ばれるストレッチクラスタとして導入できます。

vMSCソリューションは、NetApp®MetroCluster™とSnapMirrorアクティブ同期（旧称SnapMirrorビジネス継続性（SMBC））の両方でサポートされており、1つ以上の障害ドメインで全体的な停止が発生した場合に高度なビジネス継続性を提供します。さまざまな障害モードへの耐障害性は、どの設定オプションを選択するかによって異なります。

**vSphere**環境向けの継続的可用性ソリューション

ONTAPのアーキテクチャは、柔軟性と拡張性に優れたストレージプラットフォームであり、データストアにSAN（FCP、iSCSI、NVMe-oF）サービスとNAS（NFS v3およびv4.1）サービスを提供します。NetApp AFF、ASA、FASの各ストレージシステムは、ONTAPオペレーティングシステムを使用して、ゲストストレージアクセス用にS3、SMB / CIFSなどの追加プロトコルを提供します。

NetApp MetroClusterは、ネットアップのHA（コントローラフェイルオーバーまたはCFO）機能を使用してコントローラ障害から保護します。また、ローカルSyncMirrorテクノロジ、災害時のクラスタフェイルオーバー（オンデマンドのコントローラフェイルオーバーまたはCFOD）、ハードウェアの冗長性、地理的な分離によって高レベルの可用性を実現します。SyncMirrorは、アクティブにデータを提供しているローカルプレックス（ローカルシェルフ上）と、通常はデータを提供していないリモートプレックス（リモートシェルフ上）の2つのプレックスにデータを書き込むことで、MetroCluster構成の2つの部分にわたってデータを同期的にミラーリングします。ハードウェアの冗長性は、コントローラ、ストレージ、ケーブル、スイッチ（ファブリックMetroClusterで使用）、アダプタなど、MetroClusterのすべてのコンポーネントで確保されています。

NetApp SnapMirrorアクティブ同期は、FCPおよびiSCSI SANプロトコルを使用してデータストアをきめ細かく保護するため、優先度の高いワークロードのみを選択的に保護できます。アクティブ/スタンバイ解決策であるNetApp MetroClusterとは異なり、ローカルサイトとリモートサイトの両方にアクティブ/アクティブアクセスを提供します。現時点では、アクティブ同期は非対称解決策であり、一方が他方よりも優先されるため、パフォーマンスが向上します。これにはAsymmetric Logical Unit Access（ALUA；非対称論理ユニットアクセス）機能が使用され、どのコントローラを優先するかがESXiホストに自動的に通知されます。ただし、NetAppでは、アクティブな同期によって完全対称アクセスがまもなく有効になることが発表されています。

2つのサイトにVMware HA / DRSクラスタを作成するために、ESXiホストをvCenter Server Appliance（vCSA）で使用および管理します。vSphere管理ネットワーク、vMotion®ネットワーク、および仮想マシンネットワークは、2つのサイト間の冗長ネットワークを介して接続されます。HA / DRSクラスタを管理するvCenter Serverは両方のサイトのESXiホストに接続でき、vCenter HAを使用して設定する必要があります。

を参照してください "vSphere Clientでクラスタを作成および構成する方法" をクリックしてvCenter HAを設定します。

また、 "VMware vSphere Metro Storage Cluster Recommended Practices"。

**vSphere Metro Storage Cluster**とは

vSphere Metro Storage Cluster（vMSC）は、仮想マシン（VM）とコンテナを障害から保護する認定済みの構成です。これは、ストレッチストレージの概念とESXiホストのクラスタを使用して実現されます。ESXiホストは、ラック、建物、キャンパス、さらには都市など、さまざまな障害ドメインに分散されます。NetApp MetroClusterとSnapMirrorのアクティブな同期ストレージテクノロジは、それぞれホストクラスタに対してRPO=0またはNearRPO=0の保護を提供するために使用されます。vMSCの構成は、物理的または論理的な「サイト」全体に障害が発生した場合でも、データを常に利用できるように設計されています。vMSC構成に含まれるストレージデバイスは、vMSC認定プロセスを完了したあとに認定されている必要があります。サポートされているすべてのストレージデバイスは、 "VMwareストレージ互換性ガイド"。

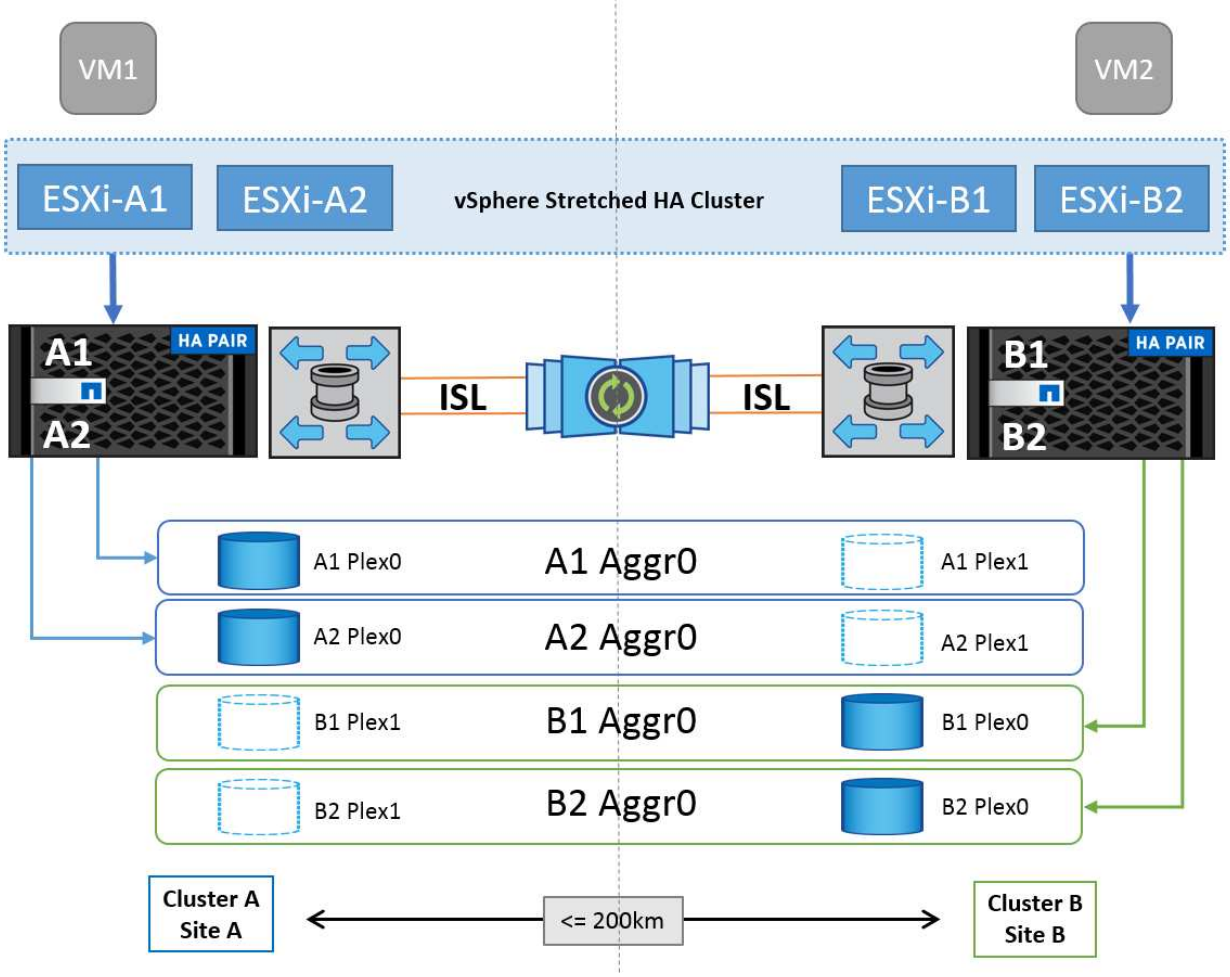
vSphere Metro Storage Clusterの設計ガイドラインの詳細については、次のドキュメントを参照してください。

- "NetApp MetroClusterによるVMware vSphereのサポート"
- "NetApp SnapMirrorビジネス継続性によるVMware vSphereのサポート" （SnapMirrorアクティブ同期）

レイテンシの考慮事項に応じて、NetApp MetroClusterを導入してvSphereで使用できます。

- ストレッチMetroCluster
- ファブリックMetroCluster

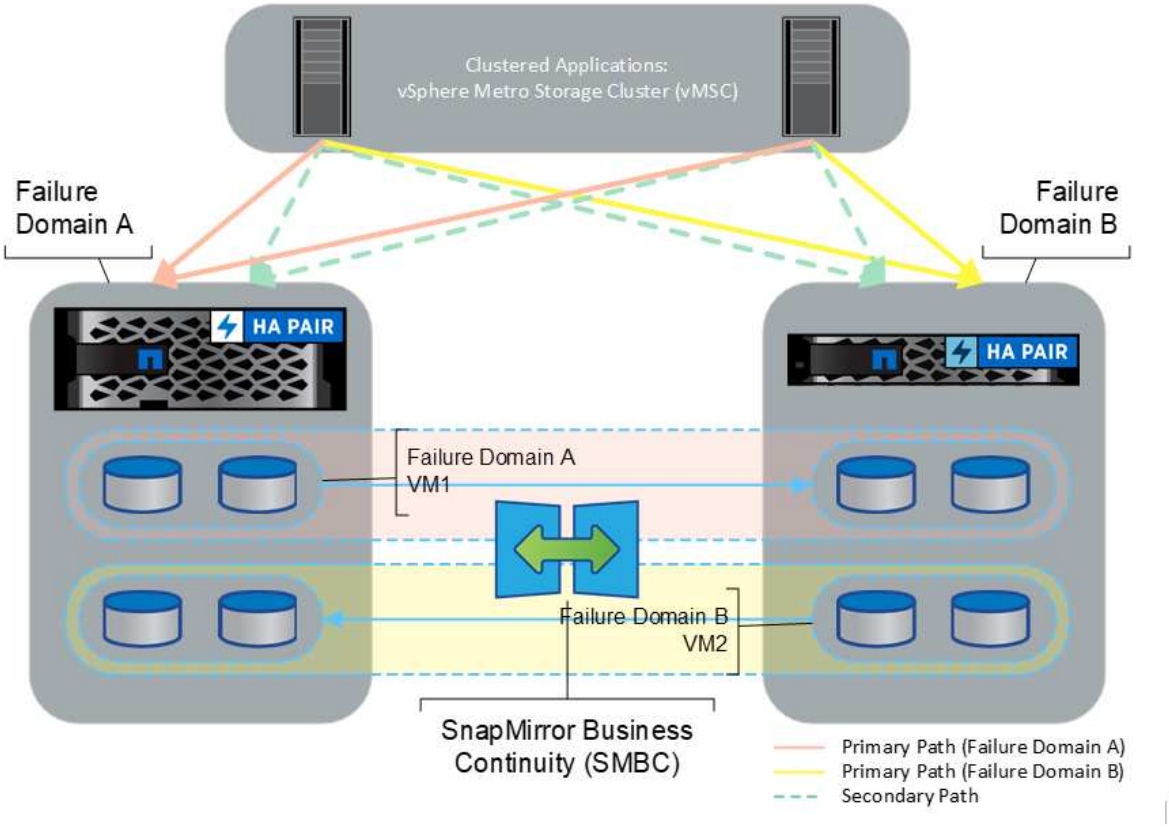
次の図は、ストレッチMetroClusterのトポロジ図の概要を示しています。




を参照してください "MetroCluster のドキュメント" を参照してくださいMetroCluster。

SnapMirror Active Syncは、2つの方法で導入することもできます。

- 非対称
- 対称（ONTAP 9.14.1でのプライベートプレビュー）




を参照してください "ネットアップのドキュメント" を参照し、SnapMirror Active Syncの設計と導入に関する情報を確認してください。

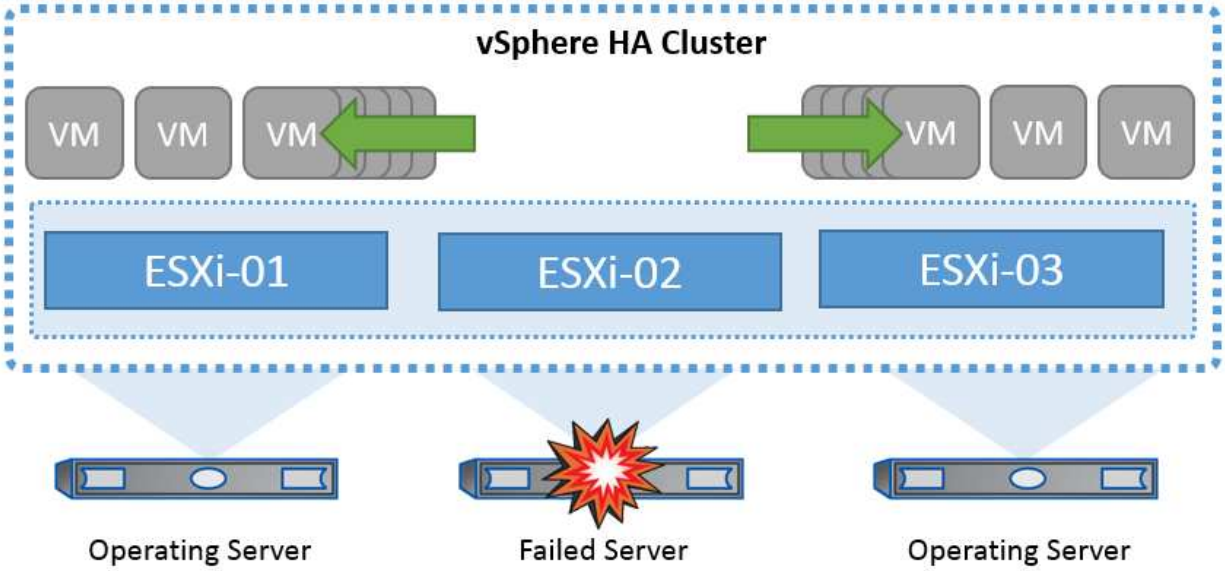
## VMware vSphere解決策の概要

vCenter Server Appliance（vCSA）は、管理者がESXiクラスタを効果的に運用できるようにする、強力な一元管理システムであり、vSphere用の単一コンソールです。VMプロビジョニング、vMotion処理、High Availability（HA；高可用性）、Distributed Resource Scheduler（DRS；分散リソーススケジューラ）、Tanzu Kubernetes Gridなどの主要な機能を簡易化します。VMwareクラウド環境に欠かせないコンポーネントであり、サービスの可用性を考慮して設計する必要があります。

### vSphereの高可用性

VMwareのクラスタテクノロジは、ESXiサーバを仮想マシンの共有リソースプールにグループ化し、vSphere High Availability（HA；高可用性）を提供します。vSphere HAは、仮想マシンで実行されるアプリケーションに対して、使いやすく高可用性を提供します。クラスタでHA機能を有効にすると、いずれかのESXiホストが応答しなくなったり分離されたりした場合に、各ESXiサーバが他のホストとの通信を維持します。 HAクラスタは、そのESXiホストで実行されていた仮想マシンのリカバリを、クラスタ内の残りのホスト間でネゴシエートできます。ゲストオペレーティングシステムに障害が発生すると、vSphere HAは影響を受ける仮想マシンを同じ物理サーバ上で再起動します。vSphere HAを使用すると、計画的停止の削減、計画外停止の防止、システム停止からの迅速なリカバリが可能になります。

vSphere HAクラスタ：障害が発生したサーバからVMをリカバリします。




VMware vSphereはNetApp MetroClusterまたはSnapMirrorのアクティブ同期を認識しないため、vSphereクラスタ内のすべてのESXiホストが、ホストおよびVMグループのアフィニティ構成に応じてHAクラスタ処理の対象となるホストとして認識されることを理解しておくことが重要です。

ホスト障害の検出

HAクラスタが作成されるとすぐに、クラスタ内のすべてのホストが選択対象になり、いずれかのホストがマスターになります。各スレーブはマスターに対してネットワークハートビートを実行し、マスターはすべてのスレーブホストに対してネットワークハートビートを実行します。vSphere HAクラスタのマスターホストは、スレーブホストの障害を検出する役割を果たします。

検出された障害のタイプによっては、ホストで実行されている仮想マシンのフェイルオーバーが必要になる場合があります。

vSphere HAクラスタでは、次の3種類のホスト障害が検出されます。

- 障害-ホストが機能を停止しました。
- 分離-ホストがネットワークから分離されます。
- パーティション-ホストとマスターホストとのネットワーク接続が失われます。

マスターホストは、クラスタ内のスレーブホストを監視します。この通信は、1秒ごとにネットワークハートビートを交換して行われます。マスターホストは、スレーブホストからのハートビートの受信を停止すると、ホストの稼働状況を確認してから、ホストに障害が発生したことを宣言します。マスターホストが実行する活性チェックでは、スレーブホストがいずれかのデータストアとハートビートを交換しているかどうかを確認します。また、マスターホストは、管理IPアドレスに送信されたICMP pingにホストが応答するかどうかをチェックして、単にマスターノードから隔離されているか、ネットワークから完全に隔離されているかを検出します。これは、デフォルトゲートウェイに対してpingを実行することによって行われます。隔離アドレスを手動で指定することで、隔離検証の信頼性を高めることができます。

ベストプラクティス

NetAppでは、隔離アドレスを少なくとも2つ追加し、各アドレスをサイトローカルにすることを推奨しています。これにより、隔離検証の信頼性が向上します。

ホスト隔離時の対応

[Isolation Response]はvSphere HAの設定で、vSphere HAクラスタ内のホストが管理ネットワーク接続を失い、実行は継続した場合に仮想マシンでトリガーされる処理を決定します。この設定には、[Disabled]、[Shut Down and Restart VMs]、[Power Off and Restart VMs]の3つのオプションがあります。

[Shut Down]は、[Power Off]よりも優れています。[Power Off]では、最新の変更がディスクにフラッシュされたり、トランザクションがコミットされたりしません。仮想マシンが300秒以内にシャットダウンされない場合は、電源がオフになります。待機時間を変更するには、詳細オプションdas.isolationshutdowntimeoutを使用します。

HAは隔離時の対応を開始する前に、vSphere HAマスターエージェントがVM構成ファイルが格納されたデータストアを所有しているかどうかを確認します。そうでない場合、VMを再起動するマスターがないため、ホストは隔離時の対応をトリガーしません。ホストはデータストアの状態を定期的にチェックして、マスターロールを持つvSphere HAエージェントがデータストアを要求しているかどうかを判断します。

ベストプラクティス

NetAppでは、[Host Isolation Response]を[Disabled]に設定することを推奨しています。

ホストがvSphere HAマスターホストから分離またはパーティショニングされ、ハートビートデータストアまたはpingを介してマスターと通信できなくなると、スプリットブレイン状態が発生することがあります。マスターは、隔離されたホストの停止を宣言し、クラスタ内の他のホスト上のVMを再起動します。仮想マシンのインスタンスが2つ実行され、そのうちの1つだけが仮想ディスクの読み取りまたは書き込みを実行できるため、スプリットブレイン状態が発生します。VM Component Protection（VMCP）を設定することで、スプリットブレイン状態を回避できるようになりました。

**VM**コンポーネント保護（**VMCP**）

vSphere 6で強化されたHA関連機能の1つにVMCPがあります。VMCPは、ブロック（FC、iSCSI、FCoE）とファイルストレージ（NFS）のAll Paths Down（APD）状態とPermanent Device Loss（PDL）状態からの保護を強化します。

**Permanent Device Loss（PDL）**

PDLとは、ストレージデバイスに永続的に障害が発生した場合、または管理上削除されて元に戻ることがない場合に発生する状態です。NetAppストレージアレイは、デバイスが永続的に失われたことを宣言するSCSIセンスコードをESXiに発行します。vSphere HAの[Failure Conditions and VM Response]セクションで、PDL状態が検出されたあとの応答を設定できます。

ベストプラクティス

NetAppでは、[Response for Datastore with PDL]を[* Power off and restart VMs]に設定することを推奨しています。この状態が検出されると、vSphere HAクラスタ内の正常なホストでVMが即座に再起動されます。

すべてのパスがダウン（**APD**）

APDは、ストレージデバイスがホストからアクセスできなくなり、アレイへのパスが使用できなくなった場合に発生する状態です。ESXiは、これをデバイスの一時的な問題とみなし、再び使用可能になることを想定しています。

APD状態が検出されると、タイマーが開始されます。140秒後、APD状態が正式に宣言され、デバイスはAPDタイムアウトとしてマークされます。140秒が経過すると、[Delay for VM Failover APD]で指定された分数が

カウントされます。指定した時間が経過すると、影響を受ける仮想マシンが再起動されます。必要に応じて異なる方法（[Disabled]、問題Events]、[Power Off and Restart VMs]）で応答するようにVMCPを設定できます。

ベストプラクティス

NetAppでは、[Response for Datastore with APD]を「* Power off and restart VMs（conservative）*」に設定することを推奨しています。

保守的とは、HAがVMを再起動できる可能性を示します。[Conservative]に設定すると、APDの影響を受けるVMは、別のホストで再起動できることがわかっている場合にのみ再起動されます。アグレッシブの場合、HAは他のホストの状態を認識していなくてもVMの再起動を試行します。その結果、VMが配置されているデータストアにアクセスできるホストがないと、VMが再起動されない可能性があります。

タイムアウトになる前にAPDステータスが解決され、ストレージへのアクセスが回復した場合は、明示的に設定していないかぎり、仮想マシンが不要に再起動されることはありません。環境がAPD状態から回復した場合でも応答が必要な場合は、[Response for APD Recovery After APD Timeout]を[Reset VMs]に設定する必要があります。

ベストプラクティス

NetAppでは、[Response for APD Recovery After APD Timeout]を[Disabled]に設定することを推奨します。

**NetApp MetroCluster**向け**VMware DRS**の実装

VMware DRSは、クラスタ内のホストリソースを集約する機能で、主に仮想インフラストラクチャ内のクラスタ内での負荷分散に使用されます。VMware DRSは、クラスタ内でロードバランシングを実行するために、主にCPUリソースとメモリリソースを計算します。vSphereはストレッチクラスタリングを認識しないため、両方のサイトのすべてのホストをロードバランシングの対象とします。サイト間トラフィックを回避するために、NetAppでは、VMの論理的な分離を管理するDRSアフィニティルールを設定することを推奨しています。これにより、サイト全体に障害が発生しないかぎり、HAとDRSでローカルホストのみが使用されるようになります。

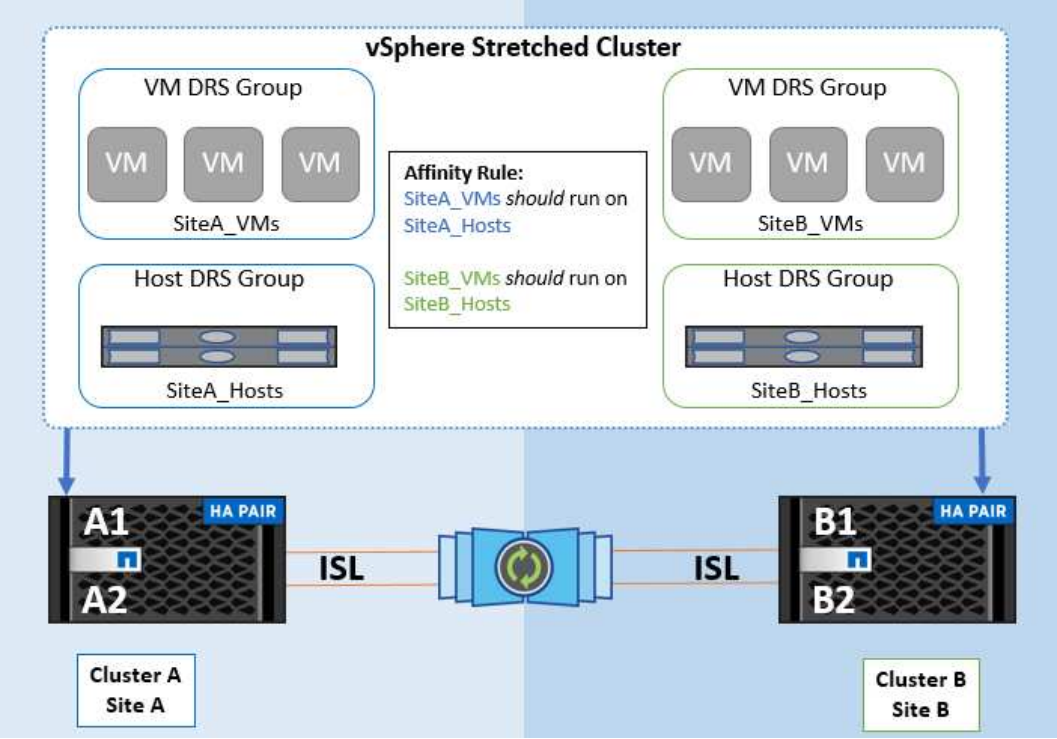
クラスタ用のDRSアフィニティルールを作成する場合は、仮想マシンのフェイルオーバー時にvSphereがそのルールを適用する方法を指定できます。

vSphere HAのフェイルオーバー動作を指定できるルールには、次の2種類があります。

- VMの非アフィニティルールでは、フェイルオーバー処理中に指定した仮想マシンが分離されたままになります。
- VMホストアフィニティルールは、フェイルオーバー処理中に、指定した仮想マシンを特定のホストまたは定義されたホストグループのメンバーに配置します。

VMware DRSのVMホストアフィニティルールを使用すると、サイトAとサイトBを論理的に分離して、特定のデータストアのプライマリ読み取り/書き込みコントローラとして設定されたアレイと同じサイトのホストでVMを実行できます。また、VMホストアフィニティルールを使用すると、仮想マシンはストレージに対してローカルなままになり、サイト間でネットワーク障害が発生した場合に仮想マシンの接続が確保されます。

次に、VMホストグループとアフィニティルールの例を示します。




ベストプラクティス

NetAppでは、障害が発生した場合にvSphere HAによって違反されるため、「must」ルールではなく「should」ルールを実装することを推奨しています。「must」ルールを使用すると、サービスが停止する可能性があります。

サービスの可用性は常にパフォーマンスより優先されるべきです。データセンター全体で障害が発生した場合、「must」ルールではVMホストアフィニティグループからホストを選択する必要があり、データセンターが使用できなくなっても仮想マシンは再起動されません。

### NetApp MetroClusterでのVMware Storage DRSの実装

VMware Storage DRS機能を使用すると、データストアを1つのユニットに集約し、Storage I/O Controlのしきい値を超えた場合に仮想マシンディスクのバランスを調整できます。

Storage I/O Controlは、Storage DRS対応のDRSクラスタではデフォルトで有効になっています。Storage I/O Controlを使用すると、I/Oの輻輳時に仮想マシンに割り当てるストレージI/Oの量を管理者が制御できるため、重要度の高い仮想マシンを優先してI/Oリソースを割り当てることができます。

Storage DRSは、Storage vMotionを使用して、データストアクラスタ内の別のデータストアに仮想マシンを移行します。NetApp MetroCluster環境では、仮想マシンの移行をそのサイトのデータストア内で制御する必要があります。たとえば、サイトAのホストで実行されている仮想マシンAを移行する場合は、サイトAのSVMのデータストア内で移行するのが理想的です。そうしないと、仮想ディスクの読み取り/書き込みはサイト間リンクを介してサイトBから行われるため、仮想マシンは引き続き動作しますが、パフォーマンスは低下します。

ベストプラクティス

NetAppでは、ストレージサイトのアフィニティに従ってデータストアクラスタを作成することを推奨しています。つまり、サイトAに対するサイトアフィニティが設定されたデータストアクラスタと、サイトBに対するサイトアフィニティが設定されたデータストアを混在させないでください。

Storage vMotionを使用して仮想マシンを新規にプロビジョニングまたは移行するたびに、NetAppそれらの仮想マシンに固有のすべてのVMware DRSルールを手動で更新することを推奨します。これにより、ホストとデータストアの両方について、サイトレベルで仮想マシンのアフィニティが確保され、ネットワークとストレージのオーバーヘッドが削減されます。

# vMSC設計および実装ガイドライン

本ドキュメントでは、ONTAPストレージシステムを使用するvMSCの設計と実装のガイドラインについて説明します。

### NetAppストレージ構成

NetApp MetroCluster（MCC構成）のセットアップ手順については、次のWebサイトを参照してください。"MetroCluster のドキュメント"。SnapMirrorアクティブ同期の手順については、 "SnapMirror のビジネス継続性機能の概要"。

一度MetroClusterを設定すると、従来のONTAP環境を管理するようなものになります。Storage Virtual Machine（SVM）は、コマンドラインインターフェイス（CLI）、System Manager、Ansibleなどのさまざまなツールを使用してセットアップできます。SVMを設定したら、通常の運用に使用する論理インターフェイス（LIF）、ボリューム、論理ユニット番号（LUN）をクラスタに作成します。これらのオブジェクトは、クラスタピアリングネットワークを使用してもう一方のクラスタに自動的にレプリケートされます。

MetroClusterを使用していない場合は、SnapMirrorアクティブ同期を使用して、異なる障害ドメインにある複数のONTAPクラスタ間で、データストア単位でのきめ細かな保護とアクティブ/アクティブアクセスを実現できます。SnapMirrorアクティブ同期では、整合グループを使用して1つ以上のデータストア間で書き込み順序の整合性が確保されます。また、アプリケーションとデータストアの要件に応じて、複数の整合グループを作成することもできます。整合グループは、複数のデータストア間でのデータ同期が必要なアプリケーションに特に役立ちます。SnapMirror Active Syncでは、rawデバイスマッピング（RDM）とゲスト内iSCSIイニシエータを使用するゲスト接続ストレージもサポートされます。整合グループの詳細については、を参照してください。 "整合グループの概要"。

SnapMirrorアクティブ同期を使用するvMSC構成の管理は、MetroClusterとは多少異なります。まず、これはSANのみの構成であり、SnapMirrorのアクティブな同期でNFSデータストアを保護することはできません。次に、両方の障害ドメインのレプリケートされたデータストアにアクセスできるように、両方のLUNのコピーをESXiホストにマッピングする必要があります。

### VMware vSphere HA の場合

#### vSphere HAクラスタの作成

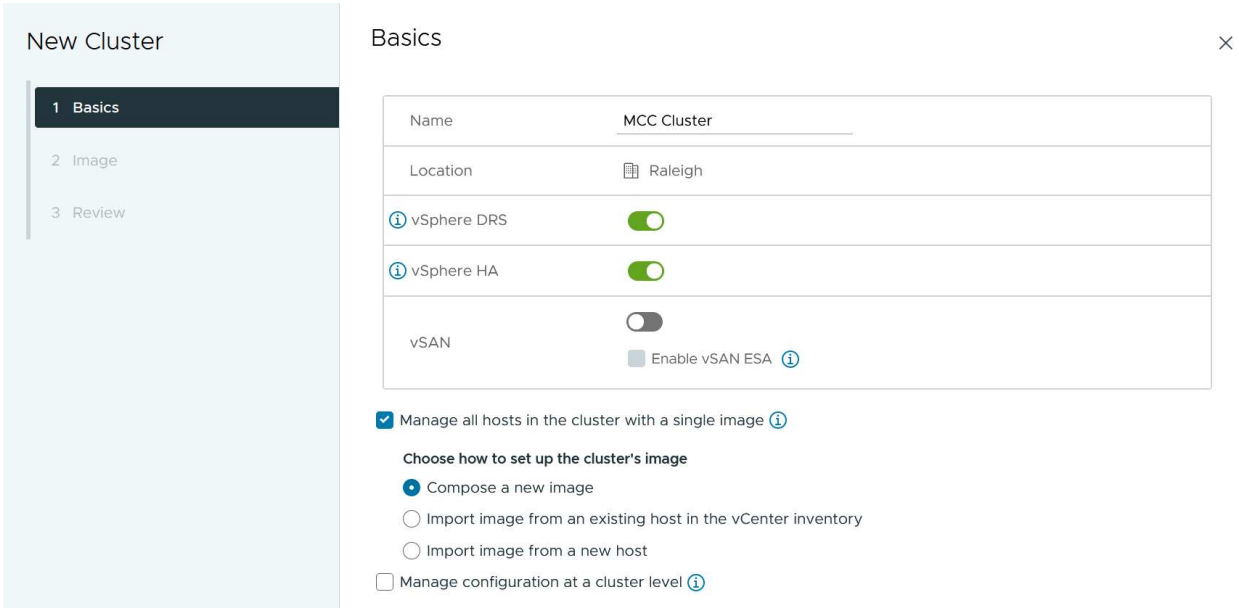
vSphere HAクラスタの作成は複数の手順で構成されます。詳細については、を参照してください。"docs.vmware.comのvSphere Clientでクラスタを作成および構成する方法"。つまり、最初に空のクラスタを作成してから、vCenterを使用してホストを追加し、クラスタのvSphere HAなどの設定を指定する必要があります。

*注：*このドキュメントには、このドキュメントより優先されるものはありません。 "VMware vSphere Metro Storage Cluster Recommended Practices"

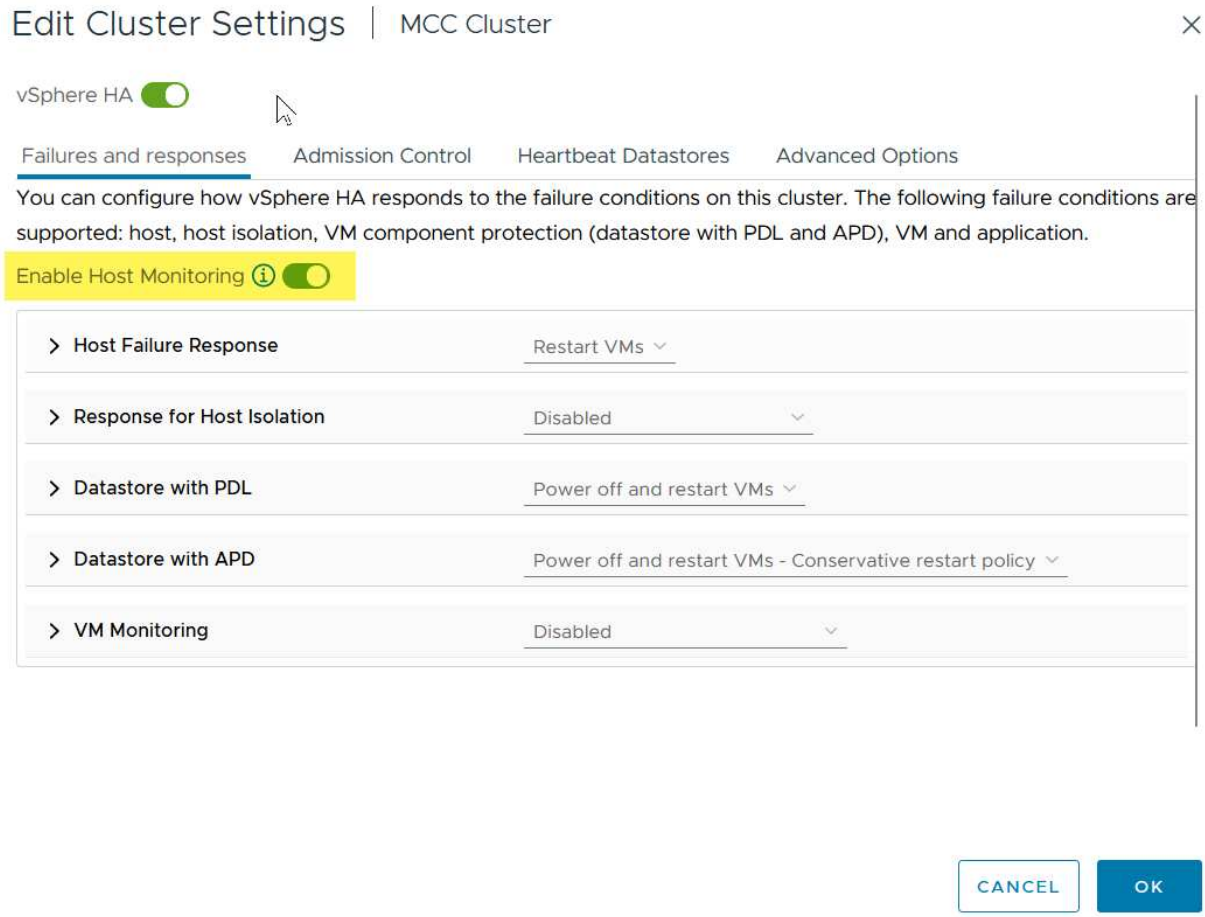
HAクラスタを設定するには、次の手順を実行します。

1. vCenter UIに接続します。
2. [Hosts and Clusters]で、HAクラスタを作成するデータセンターを選択します。

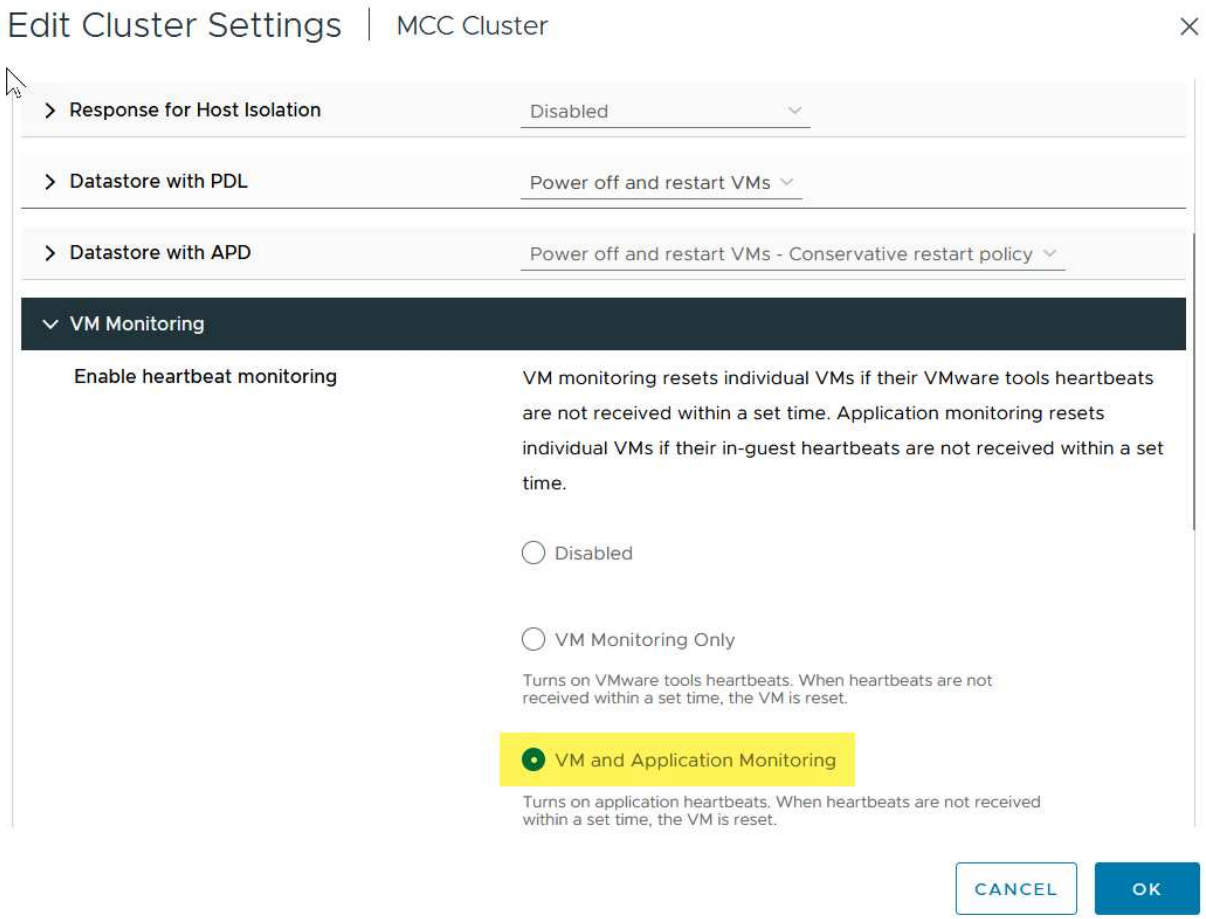
3. データセンターオブジェクトを右クリックし、[New Cluster]を選択します。[Basics]で、vSphere DRSとvSphere HAが有効になっていることを確認します。ウィザードの手順を実行します。



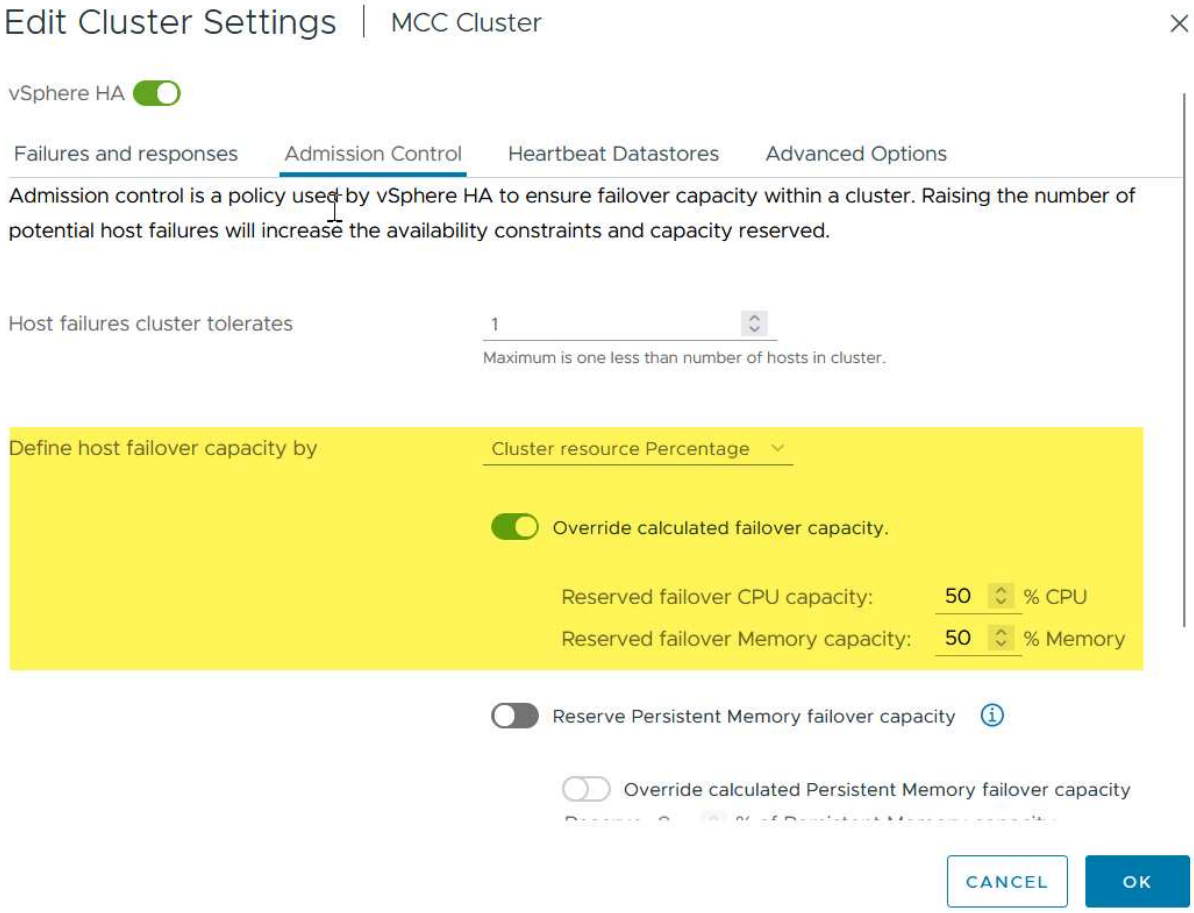

1. クラスタを選択し、[Configure]タブに移動します。[vSphere HA]を選択し、[edit]をクリック
2. [Host Monitoring]で、[Enable Host Monitoring]オプションを選択します。



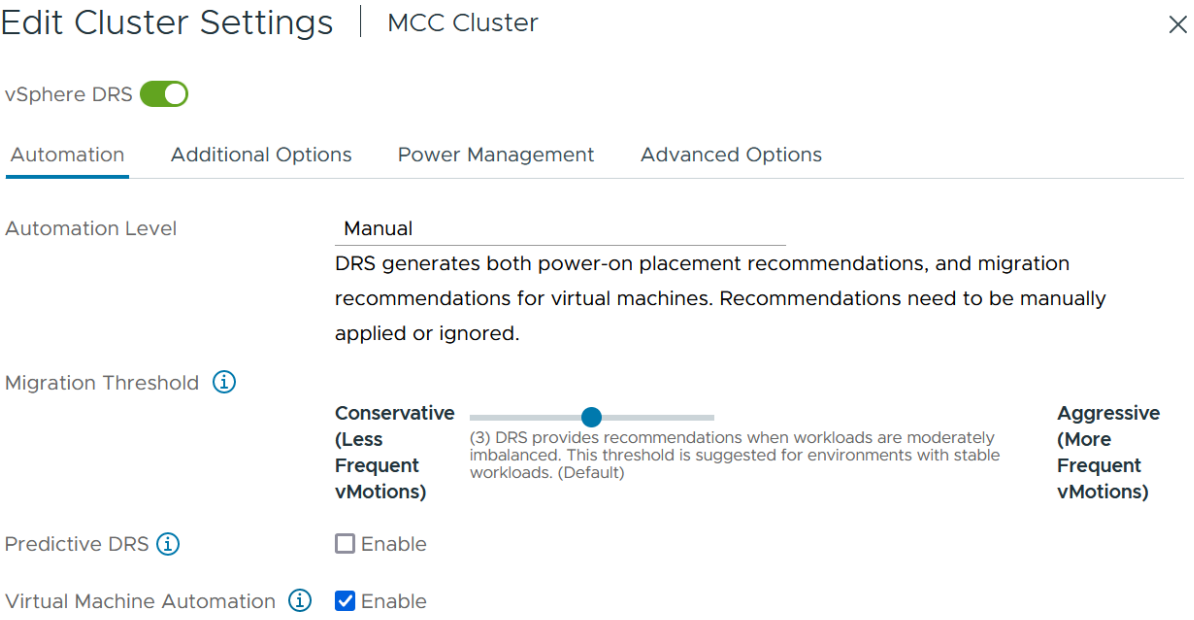
1. [Failures and Responses]タブの[VM Monitoring]で、[VM Monitoring Only]オプションまたは[VM and Application Monitoring]オプションを選択します。




1. [Admission Control]で、[HA Admission Control]オプションを[cluster resource reserve]に設定し、50%のCPU/MEMを使用します。




1. [OK]をクリックします。
2. [DRS]を選択し、[編集]をクリックします。
3. アプリケーションで必要な場合を除き、自動化レベルを手動に設定します。



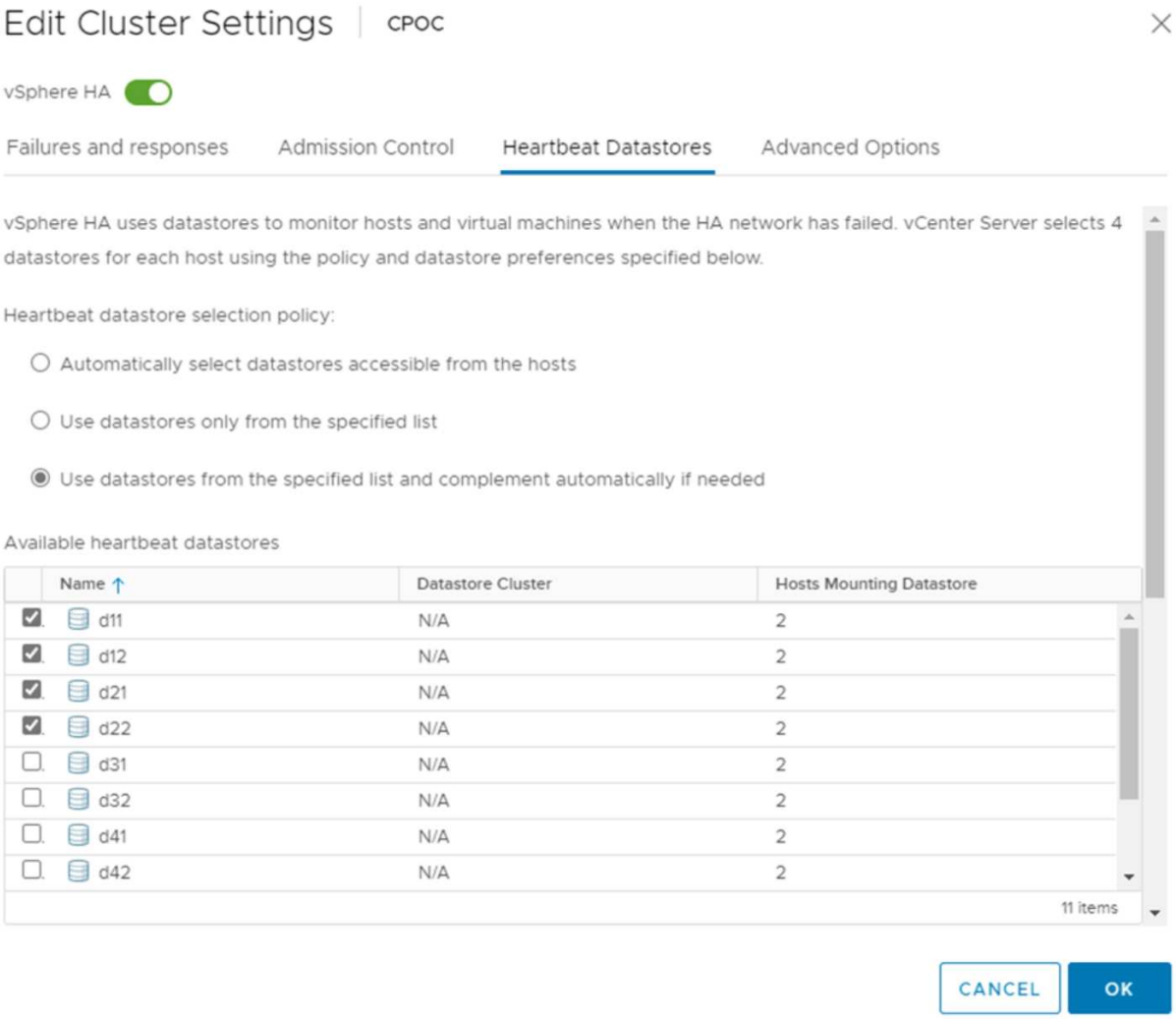
1. VMコンポーネント保護を有効にします。を参照してください。 "docs.vmware.com"。
2. MCCを使用するvMSCでは、次のvSphere HAの追加設定が推奨されます。

| 失敗 | 応答 |
| --- | --- |
| ホスト障害です | VMの再起動 |
| ホストの分離 | 無効 |
| Permanent Device Loss（PDL；永続的デバイス損失）のあるデータストア | VMの電源をオフにして再起動する |
| すべてのパスがダウンしているデータストア（APD） | VMの電源をオフにして再起動する |
| ゲストが鼓動しない | VMのリセット |
| VM再起動ポリシー | VMの重要度に応じて決定 |
| ホスト隔離時の応答 | VMのシャットダウンと再起動 |
| PDLを使用したデータストアの応答 | VMの電源をオフにして再起動する |
| APDを使用するデータストアの応答 | VMの電源をオフにして再起動する（控えめ） |
| APDのVMフェイルオーバーの遅延 | 3分 |
| APDタイムアウトによるAPDリカバリの応答 | 無効 |
| VM監視の感度 | プリセット高 |

ハートビート用のデータストアの設定

vSphere HAでは、管理ネットワークに障害が発生した場合、データストアを使用してホストと仮想マシンを監視します。vCenterでのハートビートデータストアの選択方法を設定できます。ハートビート用のデータストアを設定するには、次の手順を実行します。

1. [Datastore Heartbeating]セクションで、[Use Datastores from the Specified List and Complement Automatically if Needed]を選択します。
2. vCenterで使用するデータストアを両方のサイトから選択し、[OK]を押します。

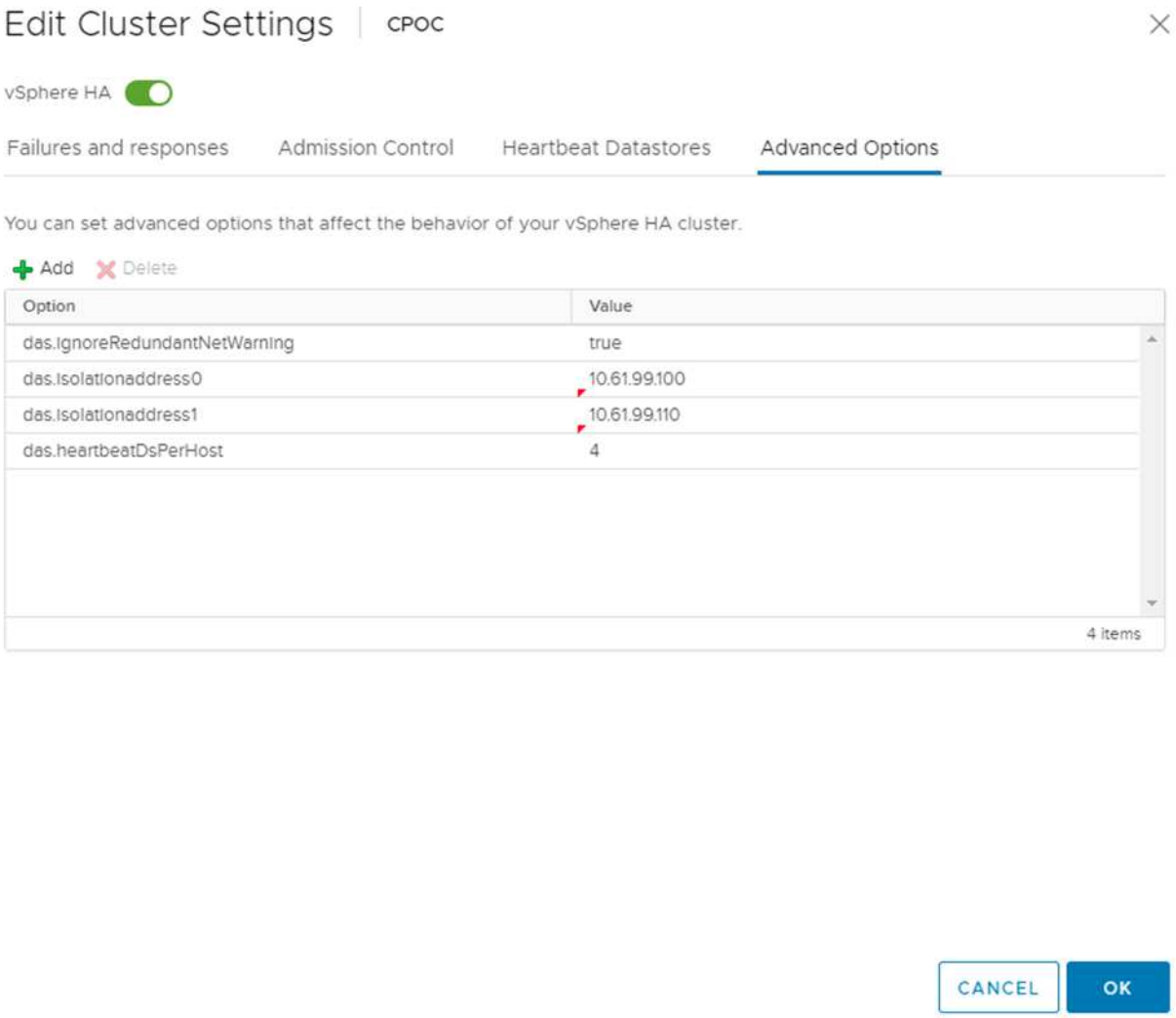



詳細オプションの設定

ホスト障害の検出

HAクラスタ内のホストがネットワークまたはクラスタ内の他のホストに接続できなくなると、分離イベントが発生します。デフォルトでは、vSphere HAは管理ネットワークのデフォルトゲートウェイをデフォルトの分離アドレスとして使用します。ただし、ホストがpingを実行するための追加の隔離アドレスを指定して、隔離応答をトリガーするかどうかを判断することができます。pingを実行できる隔離IPをサイトごとに1つずつ追加します。ゲートウェイIPは使用しないでください。使用するvSphere HAの詳細設定はdas.isolationaddressです。この目的には、ONTAPまたはメディエーターのIPアドレスを使用できます。

を参照してください "core.vmware.com" 詳細については、_を参照してください。




das.heartbeatDsPerHostという詳細設定を追加すると、ハートビートデータストアの数を増やすことができます。4つのハートビートデータストア（HB DSS）（サイトごとに2つ）を使用します。[Select from List but complent]オプションを使用します。これは、1つのサイトで障害が発生してもHB DSSが2つ必要になるためです。ただし、MCCやSnapMirrorのアクティブな同期で保護する必要はありません。

を参照してください "core.vmware.com" 詳細については、_を参照してください。

NetApp MetroCluster向けVMware DRSアフィニティ

このセクションでは、MetroCluster環境内のサイト/クラスタごとに、VMとホストのDRSグループを作成します。次に、VMホストアフィニティをローカルストレージリソースとアライメントするようにVM\Hostルールを設定します。たとえば、サイトAのVMがVMグループsitea_vmsに属し、サイトAのホストがホストグループsitea_hostsに属しているとします。次に、VM\Hostルールで、sitea_vmsをsitea_hostsのホストで実行するように記述します。

ベストプラクティス

- NetAppでは、「Must Run on Hosts in Group」という仕様ではなく、「Should Run on Hosts in Group」という仕様を使用することを強く推奨しています。サイトAのホストで障害が発生した場合、vSphere HAを使用してサイトAのVMをサイトBのホストで再起動する必要がありますが、後者の仕様では、HAがサイトBのVMを再起動することは難しいルールであるため許可されていません。前者の仕様はソフトルールで

あり、HAが発生した場合は違反となるため、パフォーマンスではなく可用性が確保されます。

*注：*仮想マシンがVMとホストのアフィニティルールに違反したときにトリガーされるイベントベースのアラームを作成できます。vSphere Clientで、仮想マシンの新しいアラームを追加し、イベントトリガーとして[VM is violating VM-Host Affinity Rule]を選択します。アラームの作成と編集の詳細については、を参照してください。 "vSphereの監視とパフォーマンス" ドキュメント

#### DRSホストグループの作成

サイトAとサイトBに固有のDRSホストグループを作成するには、次の手順を実行します。

1. vSphere Web Clientで、インベントリ内のクラスタを右クリックし、[Settings]を選択します。
2. [VM\Host Groups]をクリックします。
3. 追加をクリックします。
4. グループの名前を入力します（例：sitea_hosts）。
5. [Type]メニューから[Host Group]を選択します。
6. [Add]をクリックし、サイトAから目的のホストを選択して[OK]をクリックします。
7. 同じ手順を繰り返して、サイトBのホストグループをもう1つ追加します。
8. [OK] をクリックします。

#### DRS VMグループの作成

サイトAとサイトBに固有のDRS VMグループを作成するには、次の手順を実行します。

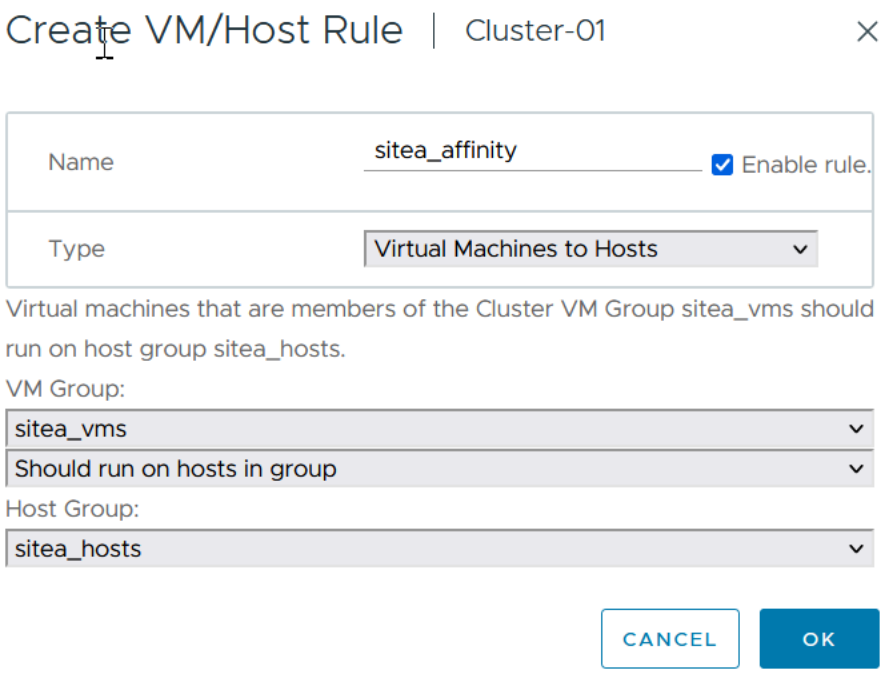
1. vSphere Web Clientで、インベントリ内のクラスタを右クリックし、[Settings]を選択します。
2. [VM\Host Groups]をクリックします。
3. 追加をクリックします。
4. グループの名前を入力します（例：sitea_vms）。
5. [Type]メニューから[VM Group]を選択します。
6. [Add]をクリックし、サイトAから目的のVMを選択して[OK]をクリックします。
7. 同じ手順を繰り返して、サイトBのホストグループをもう1つ追加します。
8. [OK] をクリックします。

#### VMホストルールの作成

サイトAとサイトBに固有のDRSアフィニティルールを作成するには、次の手順を実行します。

1. vSphere Web Clientで、インベントリ内のクラスタを右クリックし、[Settings]を選択します。
2. [VM\Host Rules]をクリックします。
3. 追加をクリックします。
4. ルールの名前を入力します（例：sitea_affinity）。
5. Enable Ruleオプションがオンになっていることを確認します。
6. [Type]メニューから[Virtual Machines to Hosts]を選択します。

7. VMグループを選択します（例：sitea_vms）。
8. ホストグループを選択します（例：sitea_hosts）。
9. 同じ手順を繰り返して、サイトBのVM\Hostルールをもう1つ追加します。
10. [OK] をクリックします。




### NetApp MetroCluster向けVMware vSphere Storage DRS

データストアクラスタの作成

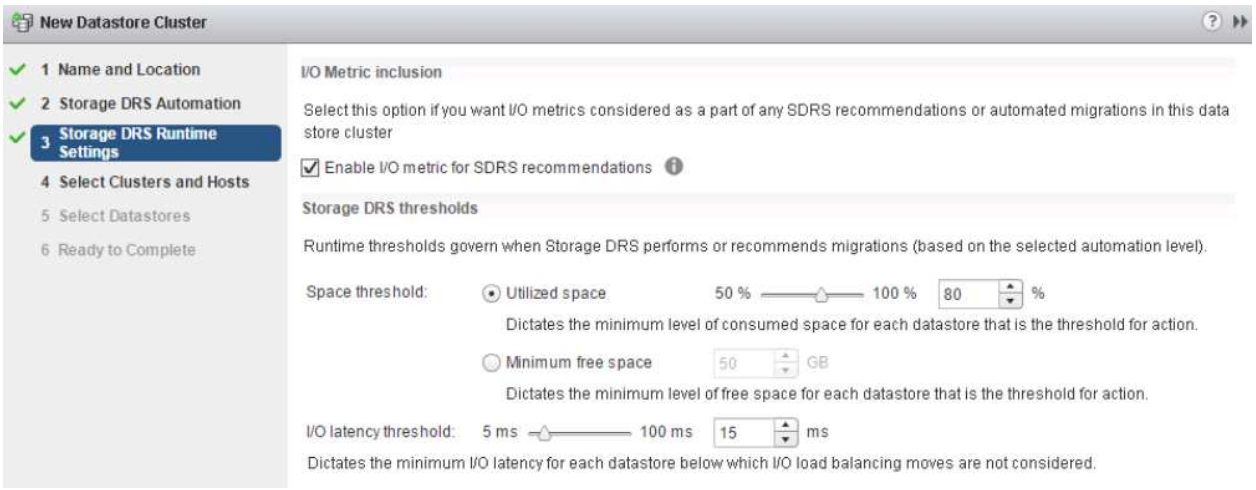
各サイトのデータストアクラスタを設定するには、次の手順を実行します。

1. vSphere Web Clientを使用して、[Storage]の下にあるHAクラスタが配置されているデータセンターに移動します。
2. データセンターオブジェクトを右クリックし、[Storage]>[New Datastore Cluster]を選択します。
3. [Turn on Storage DRS]オプションを選択し、[Next]をクリックします。
4. すべてのオプションを[No Automation（Manual Mode）]に設定し、[Next]をクリックします。

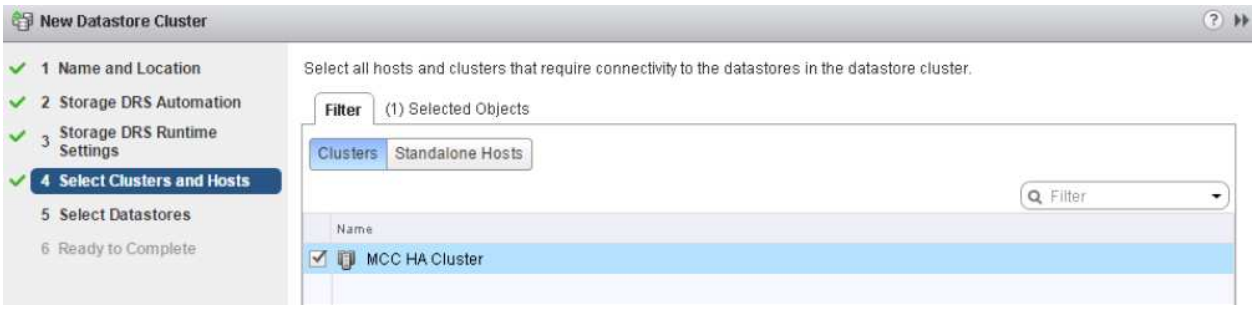
ベストプラクティス

- NetAppでは、移行が必要になるタイミングを管理者が判断して制御できるように、Storage DRSを手動モードで設定することを推奨しています。

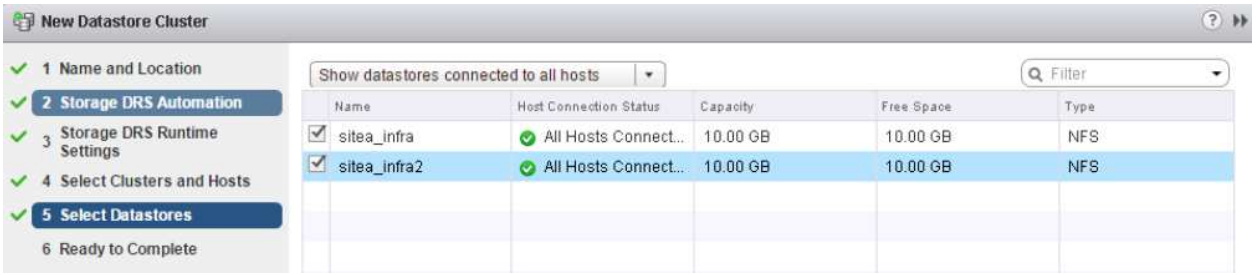
1. [Enable I/O Metric for SDRS Recommendations]チェックボックスがオンになっていることを確認します。メトリック設定はデフォルト値のままにできます。




1. HAクラスタを選択し、[Next]をクリックします。




1. サイトAに属するデータストアを選択し、[Next]をクリックします。




1. オプションを確認し、[完了]をクリックします。
2. 同じ手順を繰り返してサイトBのデータストアクラスタを作成し、サイトBのデータストアのみが選択されていることを確認します。

**vCenter Server**の可用性

vCenter Server Appliance（VCSA）はvCenter HAで保護する必要があります。vCenter HAでは、アクティブ/パッシブHAペアに2つのVCSAを導入できます。障害ドメインごとに1つ。vCenter HAの詳細については、"docs.vmware.com"。

# 計画的イベントと計画外イベントの耐障害性

## NetApp MetroClusterとSnapMirrorのアクティブ同期は、NetAppハードウェアとONTAP®ソフトウェアの高可用性とノンストップオペレーションを強化する強力なツールです。

これらのツールは、ストレージ環境全体をサイト全体で保護し、データの可用性を確保します。スタンドアロンサーバ、高可用性サーバクラスタ、Dockerコンテナ、仮想サーバのいずれを使用している場合でも、NetAppテクノロジは、停電、冷却装置の障害、ネットワーク接続の障害、ストレージアレイのシャットダウン、または運用上のエラーが原因で全体が停止した場合でも、ストレージの可用性をシームレスに維持します。

MetroClusterとSnapMirrorのアクティブな同期では、計画的または計画外のイベントが発生した場合に、次の3つの基本的な方法でデータを継続できます。

- 冗長コンポーネントによる単一コンポーネント障害からの保護
- ローカルのHAテイクオーバー：1台のコントローラに影響するイベントに対応
- 完全なサイト保護–ストレージおよびクライアントのアクセスをソースクラスタからデスティネーションクラスタに移動することで、サービスを迅速に再開します。

つまり、1つのコンポーネントで障害が発生してもシームレスに運用が継続され、障害が発生したコンポーネントを交換すると自動的に冗長運用に戻ります。

シングルノードクラスタ（通常はONTAP Selectなどのソフトウェア定義バージョン）を除くすべてのONTAPクラスタには、テイクオーバーとギブバックと呼ばれるHA機能が組み込まれています。クラスタ内の各コントローラが別のコントローラとペアリングされ、HAペアが形成されます。これらのペアにより、各ノードはストレージにローカルで接続されます。

テイクオーバーは、データサービスを維持するために一方のノードがもう一方のノードのストレージをテイクオーバーする自動プロセスです。ギブバックは、通常動作に戻る逆のプロセスです。テイクオーバーは、ハードウェアのメンテナンス時やONTAPのアップグレード時などに計画的に行うことも、ノードのパニックやハードウェア障害による計画外で行うこともできます。

テイクオーバー時に、MetroCluster構成のネットワーク接続型ストレージ論理インターフェイス（NAS LIF）が自動的にフェイルオーバーされます。ただし、ストレージエリアネットワークLIF（SAN LIF）はフェイルオーバーせず、引き続き論理ユニット番号（LUN）への直接パスを使用します。

HAのテイクオーバーとギブバックの詳細については、 "HAペアの管理の概要"。この機能は、MetroClusterまたはSnapMirrorのアクティブな同期に固有ではないことに注意してください。

MetroClusterによるサイトのスイッチオーバーは、一方のサイトがオフラインになった場合、またはサイト全体のメンテナンスのために計画的に実行された場合に実行されます。オフラインになったクラスタのストレージリソース（ディスクおよびアグリゲート）の所有権がもう一方のサイトに引き継がれ、障害が発生したサイトのSVMがディザスタサイトでオンラインになって再起動されます。その際、クライアントとホストのアクセス用にIDは保持されます。

SnapMirrorのアクティブな同期では、両方のコピーが同時にアクティブに使用されるため、既存のホストは引き続き動作します。サイトのフェイルオーバーを正しく実行するには、NetAppメディエーターが必要です。

## MCCを使用するvMSCの障害シナリオ

以降のセクションでは、vMSCおよびNetApp MetroClusterシステムで発生したさまざまな障害シナリオで想定される結果について説明します。

### 単一のストレージパス障害

このシナリオでは、HBAポート、ネットワークポート、フロントエンドデータスイッチポート、FCケーブル、イーサネットケーブルなどのコンポーネントで障害が発生すると、ストレージデバイスへの特定のパスがESXiホストによって停止とマークされます。HBA /ネットワーク/スイッチポートで耐障害性を提供してストレージデバイスに複数のパスが設定されている場合は、ESXiがパススイッチオーバーを実行するのが理想的です。この間、ストレージデバイスへの複数のパスを提供することでストレージの可用性が確保されるため、仮想マシンは影響を受けずに実行され続けます。

*注：*このシナリオではMetroClusterの動作に変更はなく、すべてのデータストアがそれぞれのサイトで引き続き実行されます。

#### ベストプラクティス

NFS / iSCSIボリュームを使用している環境ではNetApp、NFS vmkernelポート用に少なくとも2つのネットワークアップリンクを標準vSwitchに設定し、NFS vmkernelインターフェイスが分散vSwitchにマッピングされているポートグループに設定することを推奨します。NICチーミングは、アクティブ/アクティブまたはアクティブ/スタンバイのいずれかで設定できます。

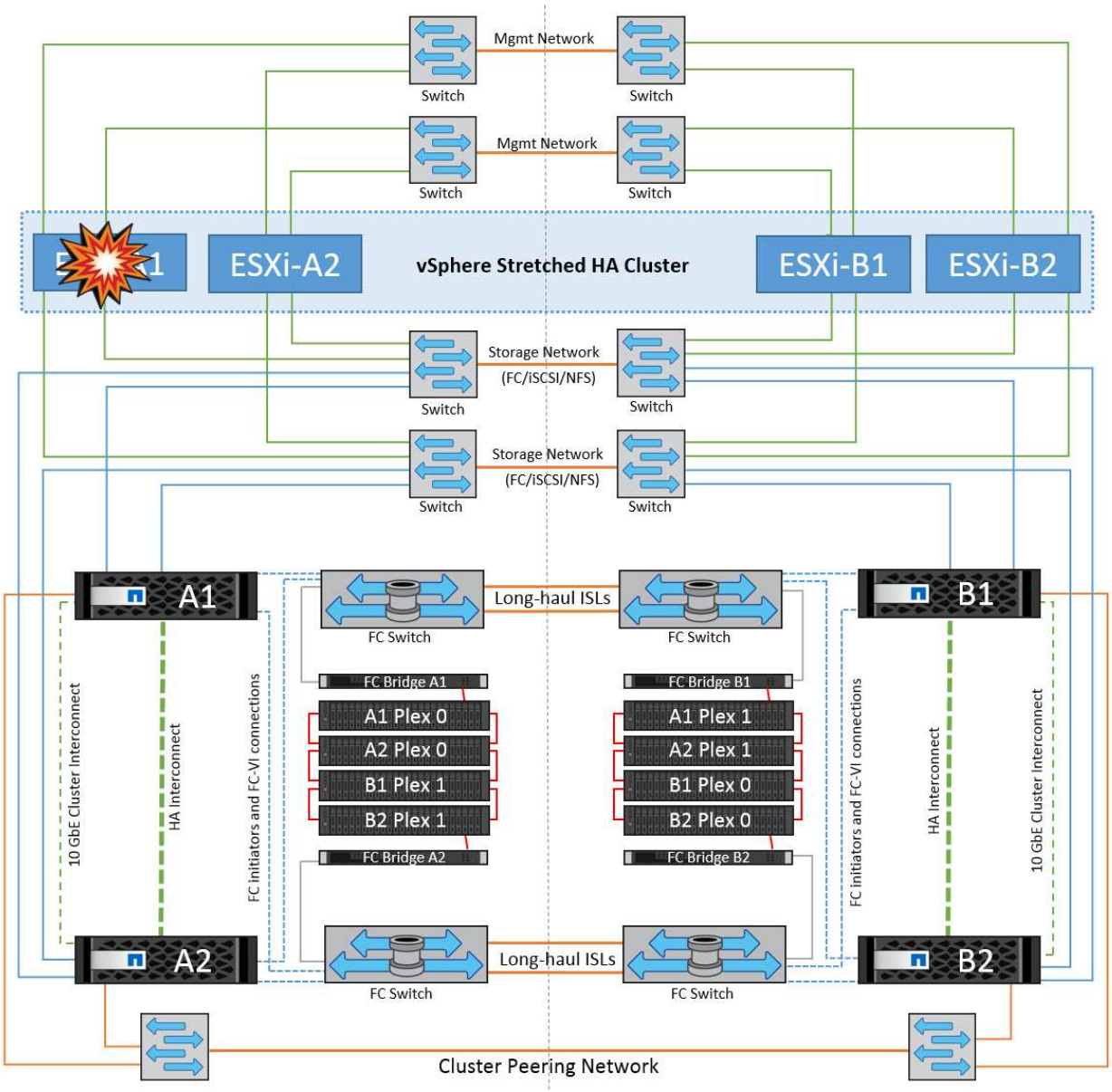
また、iSCSI LUNの場合は、vmkernelインターフェイスをiSCSIネットワークアダプタにバインドしてマルチパスを設定する必要があります。詳細については、vSphereストレージのドキュメントを参照してください。

#### ベストプラクティス

ファイバチャネルLUNを使用する環境でNetAppは、HBAを少なくとも2つ搭載し、HBA /ポートレベルでの耐障害性を保証することを推奨します。NetAppでは、ゾーニングを設定するためのベストプラクティスとして、単一のイニシエータから単一のターゲットへのゾーニングも推奨しています。

新規および既存のすべてのNetAppストレージデバイスにポリシーが設定されるため、Virtual Storage Console（VSC）を使用してマルチパスポリシーを設定する必要があります。

### 単一のESXiホスト障害




このシナリオでは、ESXiホストで障害が発生すると、VMware HAクラスタのマスターノードがネットワークハートビートを受信しなくなるため、ホスト障害を検出します。ホストが本当に停止しているのか、ネットワークパーティションだけなのかを判別するために、マスターノードはデータストアハートビートを監視し、ハートビートがない場合は、障害が発生したホストの管理IPアドレスに対してpingを実行して最終チェックを実行します。これらのチェックがすべて無効の場合、マスターノードはこのホストを障害が発生したホストであると宣言し、この障害が発生したホストで実行されていたすべての仮想マシンが、クラスタ内の残りのホストでリブートされます。

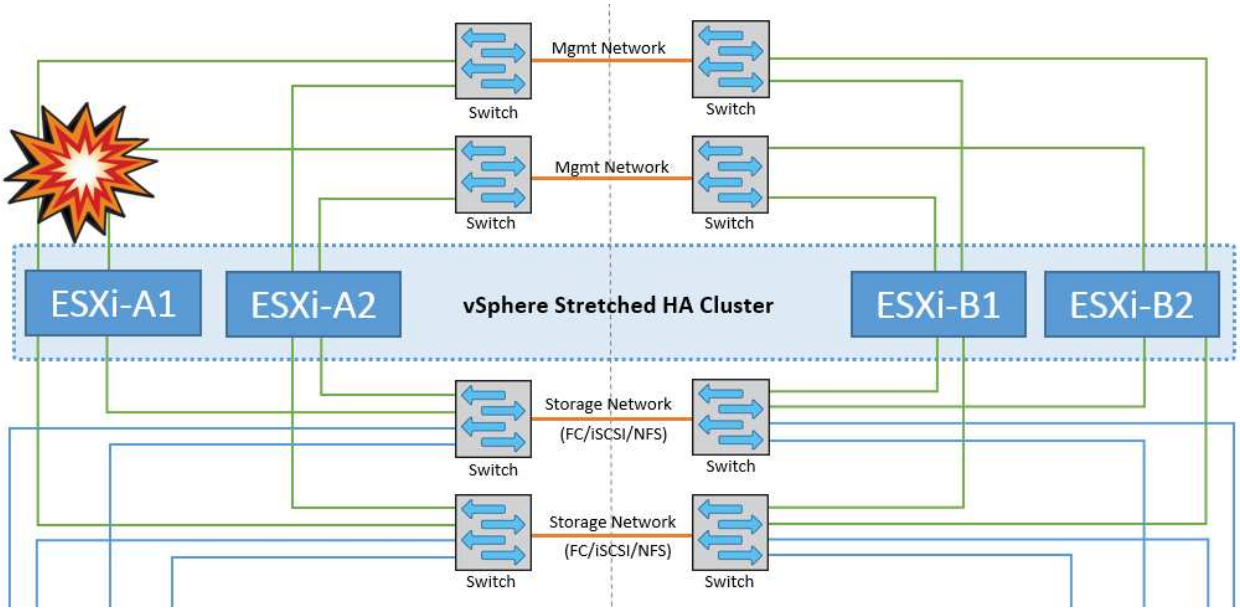
DRSのVMとホストのアフィニティルールが設定されている場合（VMグループsitea_vmsのVMはホストグループsitea_hostsのホストを実行する必要があります）、HAマスターは最初にサイトAで使用可能なリソースを確認します。サイトAに使用可能なホストがない場合、マスターはサイトBのホストでVMの再起動を試みます。

ローカルサイトのリソースに制約がある場合は、もう一方のサイトのESXiホストで仮想マシンが起動される可能性があります。ただし、DRSのVMとホストのアフィニティルールに違反した場合は、仮想マシンをローカルサイトの稼働しているESXiホストに移行することで修正されます。DRSが手動に設定されている場合、NetAppはDRSを起動し、推奨事項を適用して仮想マシンの配置を修正することを推奨します。

このシナリオではMetroClusterの動作に変更はなく、すべてのデータストアがそれぞれのサイトで引き続き実

行されます。

**ESXi**ホストの分離

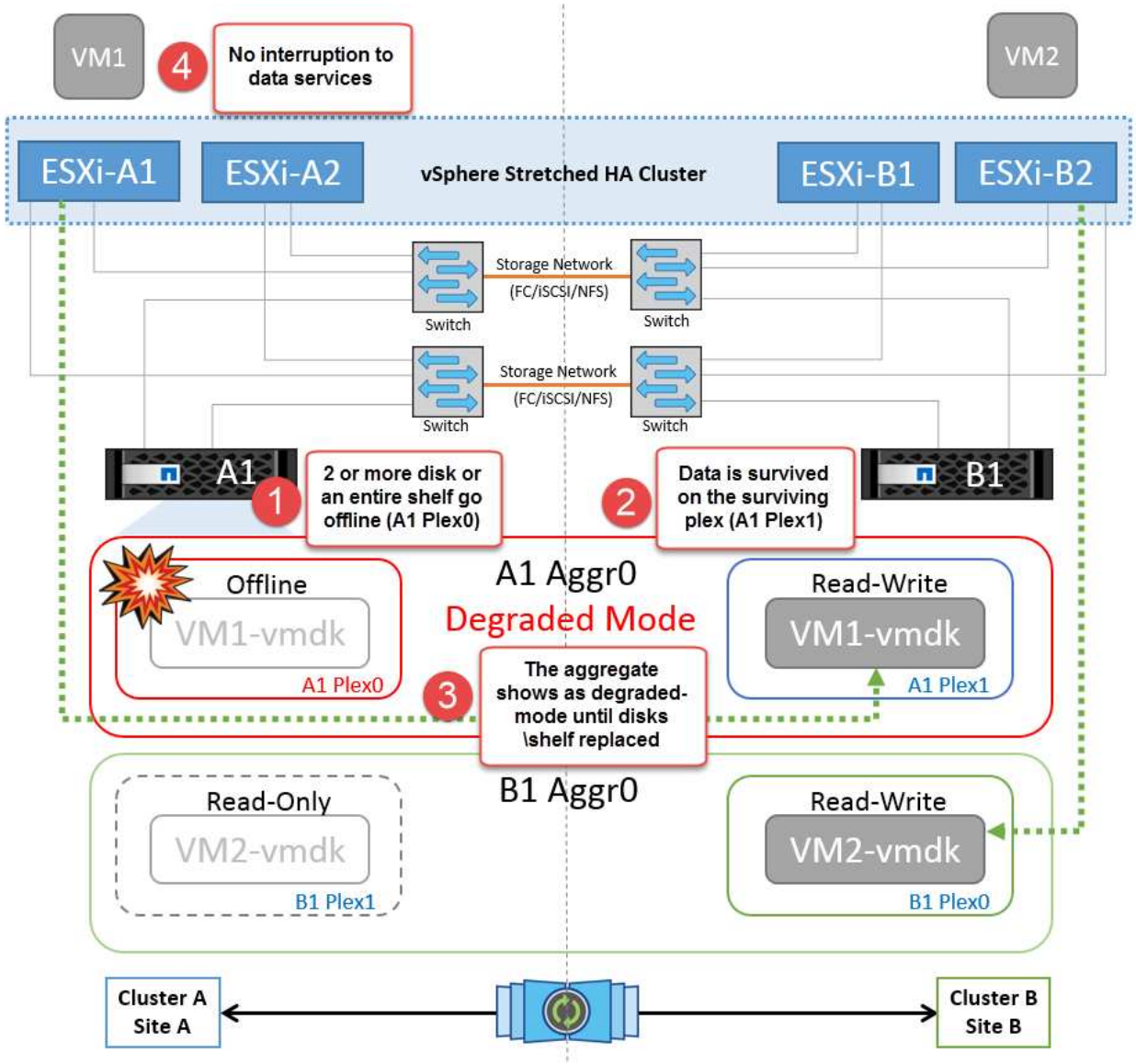



このシナリオでは、ESXiホストの管理ネットワークが停止すると、HAクラスタ内のマスターノードがハートビートを受信しなくなり、このホストがネットワークから分離された状態になります。障害が発生したか、隔離されているだけかを判別するために、マスターノードはデータストアハートビートの監視を開始します。ホストが存在する場合、ホストはマスターノードによって分離されていると宣言されます。構成されている隔離時の対応に応じて、ホストは仮想マシンの電源をオフにするか、シャットダウンするか、仮想マシンの電源をオンにしたままにするかを選択できます。分離応答のデフォルトの間隔は30秒です。

このシナリオではMetroClusterの動作に変更はなく、すべてのデータストアがそれぞれのサイトで引き続き実行されます。

ディスクシェルフの障害

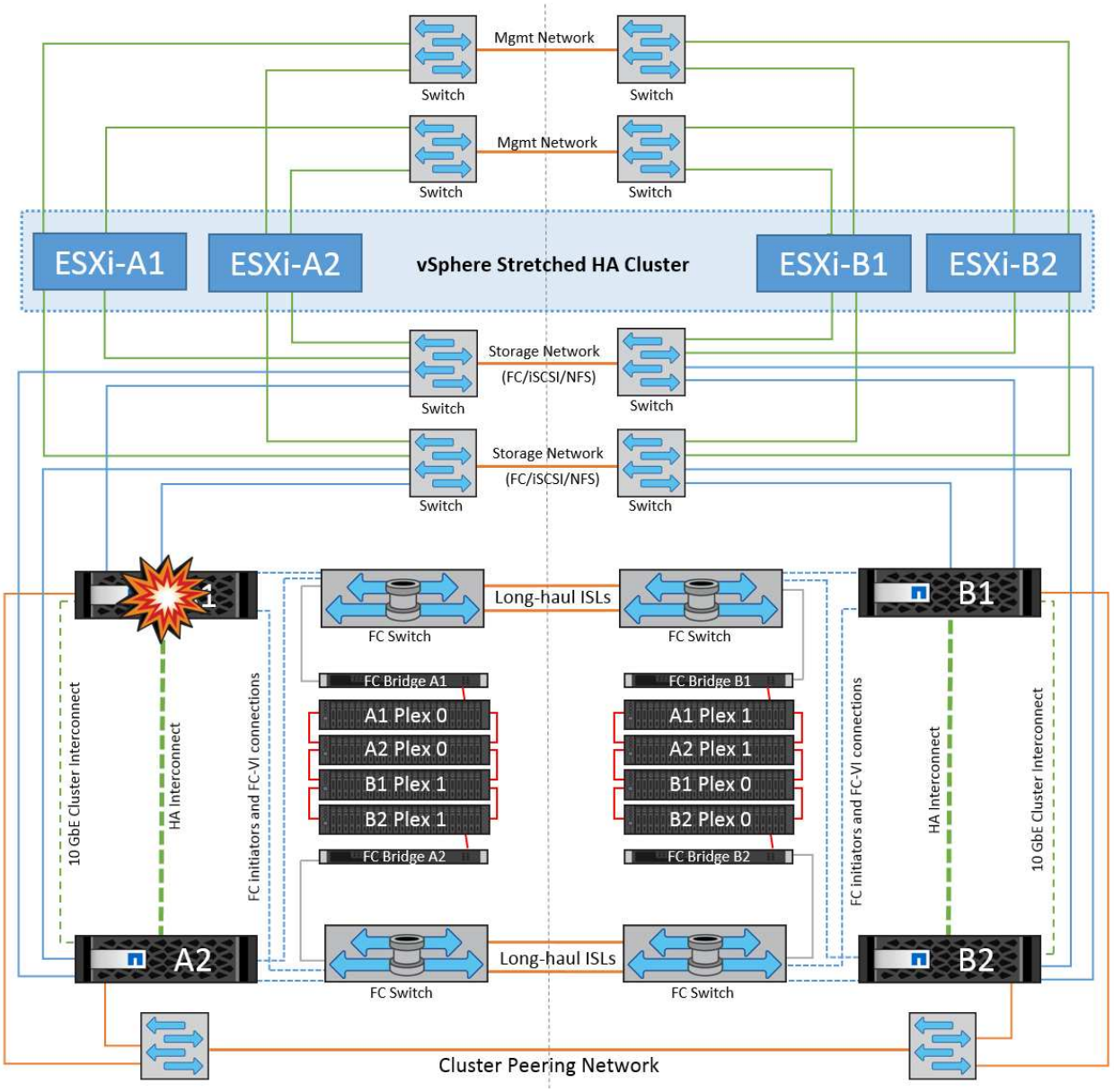
このシナリオでは、3本以上のディスクまたはシェルフ全体で障害が発生しています。データは、データサービスを中断することなく、稼働しているプレックスから提供されます。ディスク障害は、ローカルまたはリモートのプレックスに影響する可能性があります。アクティブなプレックスが1つしかないため、アグリゲートはデグレードモードになります。障害が発生したディスクを交換すると、影響を受けたアグリゲートが自動的に再同期されてデータが再構築されます。再同期後、アグリゲートは自動的に通常のミラーモードに戻ります。単一のRAIDグループ内の3本以上のディスクで障害が発生した場合は、プレックスを最初から再構築する必要があります。




*注：*この間、仮想マシンのI/O処理への影響はありませんが、データはISLリンクを介してリモートのディスクシェルフからアクセスされるため、パフォーマンスが低下します。

単一のストレージコントローラ障害

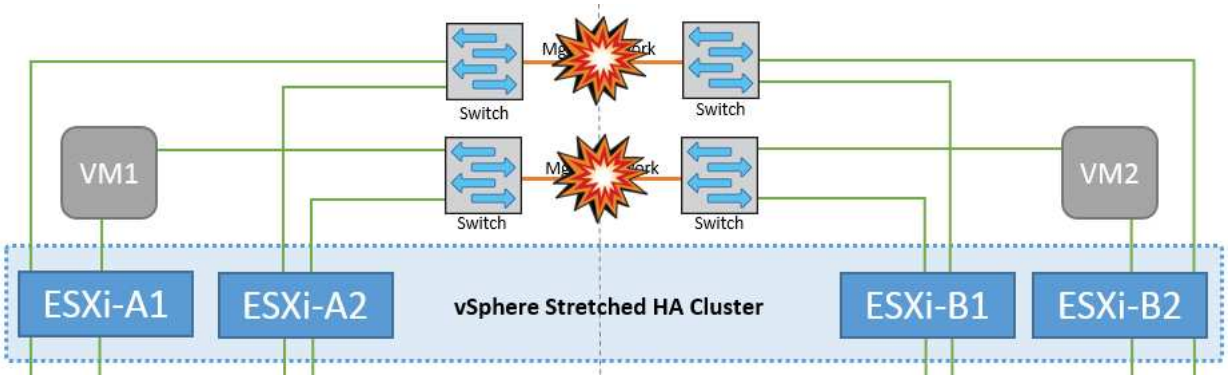
このシナリオでは、一方のサイトの2台のストレージコントローラのどちらかで障害が発生します。各サイトにHAペアがあるため、一方のノードで障害が発生すると、もう一方のノードへのフェイルオーバーが透過的かつ自動的にトリガーされます。たとえば、ノードA1に障害が発生した場合、そのストレージとワークロードは自動的にノードA2に転送されます。すべてのプレックスが引き続き使用可能なため、仮想マシンに影響はありません。2つ目のサイトのノード（B1とB2）は影響を受けません。また、クラスタ内のマスターノードは引き続きネットワークハートビートを受信するため、vSphere HAによる処理は行われません。




フェイルオーバーがローリングディザスタ（ノードA1からA2にフェイルオーバー）の一部である場合に、その後A2またはサイトA全体で障害が発生すると、災害後にサイトBでスイッチオーバーが発生する可能性があります。

## スイッチ間リンクの障害

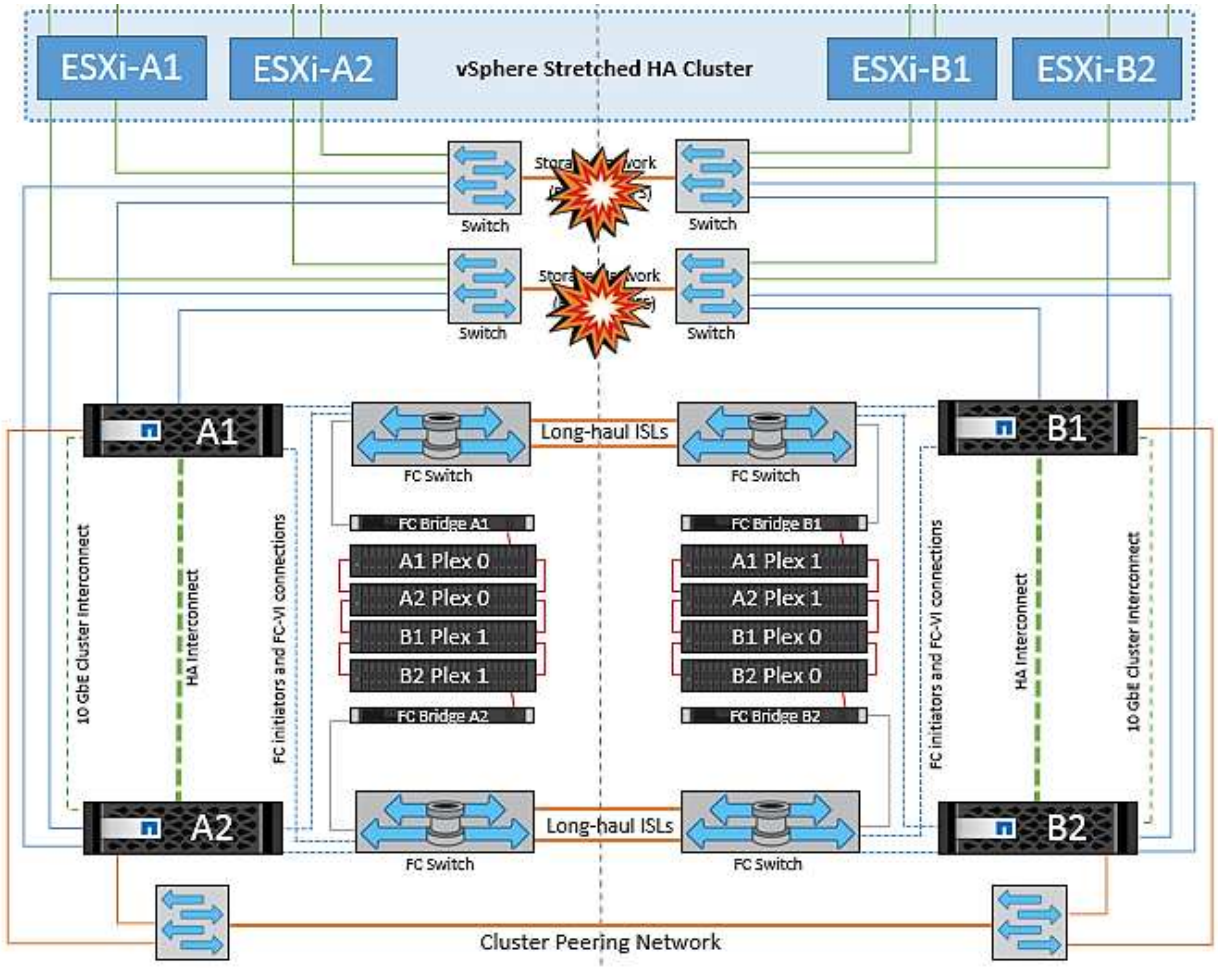
### 管理ネットワークでのスイッチ間リンク障害




このシナリオでは、フロントエンドホスト管理ネットワークのISLリンクで障害が発生し、サイトAのESXiホストがサイトBのESXiホストと通信できなくなります。これにより、特定のサイトのESXiホストからHAクラスタ内のマスターノードにネットワークハートビートを送信できなくなるため、ネットワークが分割されます。そのため、パーティションのために2つのネットワークセグメントがあり、各セグメントにマスターノードがあり、特定のサイト内でVMがホスト障害から保護されます。

*注：*この間、仮想マシンは実行されたままであり、このシナリオではMetroClusterの動作に変更はありません。すべてのデータストアがそれぞれのサイトで引き続き実行されます。

ストレージネットワークのスイッチ間リンク障害

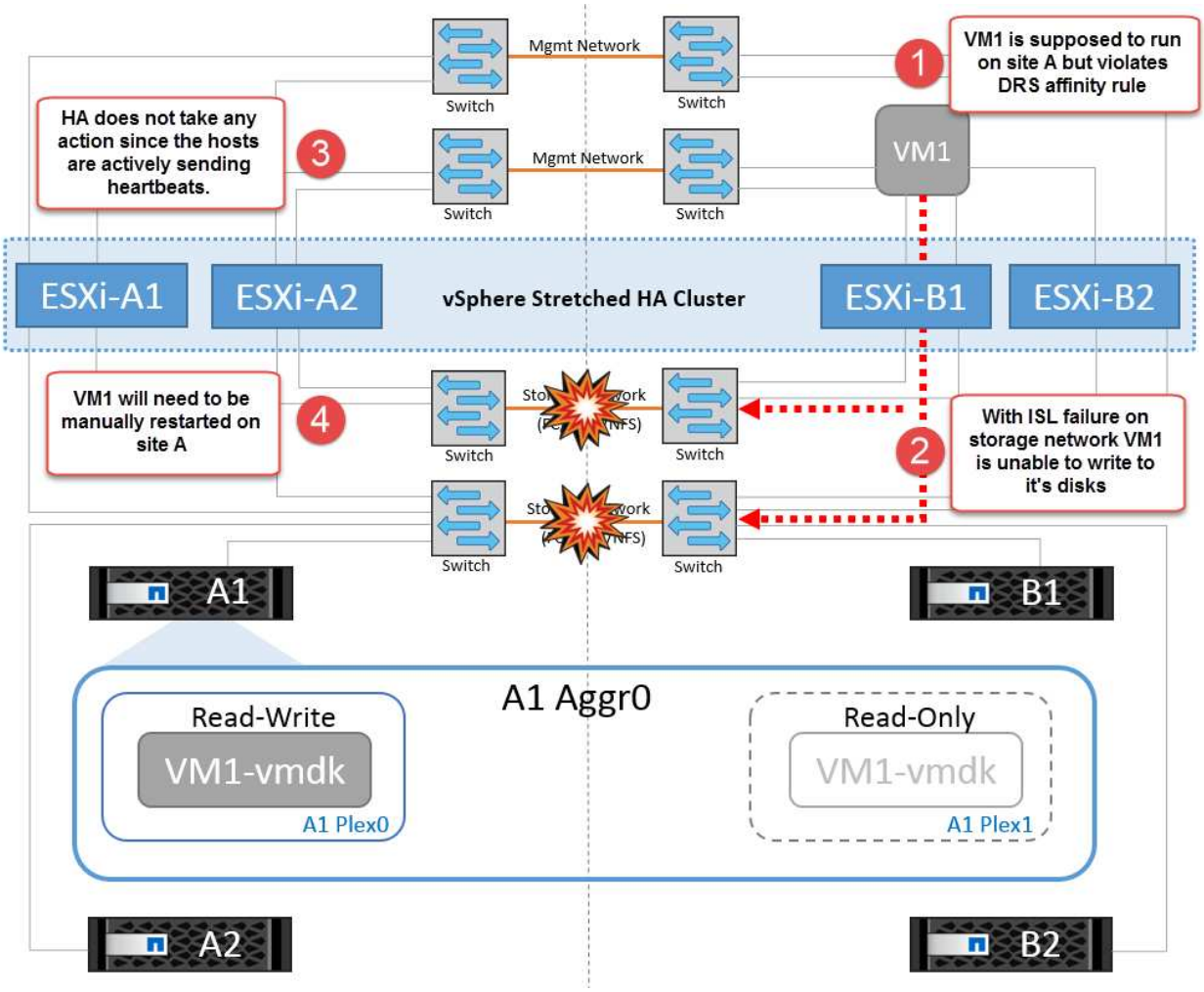



このシナリオでは、バックエンドストレージネットワークのISLリンクで障害が発生すると、サイトAのホストはサイトBのクラスタBのストレージボリュームまたはLUNにアクセスできなくなります。その逆も同様です。VMware DRSルールは、ホストとストレージサイトのアフィニティによって、サイト内で影響を与えるこ

となく仮想マシンを実行できるように定義されています。

この間、仮想マシンはそれぞれのサイトで実行されたままになり、このシナリオではMetroClusterの動作に変更はありません。すべてのデータストアがそれぞれのサイトで引き続き実行されます。

何らかの理由でアフィニティルールに違反した場合（ローカルクラスタAのノードにディスクが配置されているサイトAから実行されていたVM1がサイトBのホストで実行されている場合など）、仮想マシンのディスクにISLリンクを介してリモートからアクセスされます。ISLリンクで障害が発生すると、ストレージボリュームへのパスが停止し、その仮想マシンが停止するため、サイトBで実行されているVM1はディスクに書き込むことができなくなります。この場合、ホストからハートビートがアクティブに送信されるため、VMware HAによる処理は行われません。これらの仮想マシンは、それぞれのサイトで手動で電源をオフにしてオンにする必要があります。次の図は、VMがDRSアフィニティルールに違反していることを示しています。

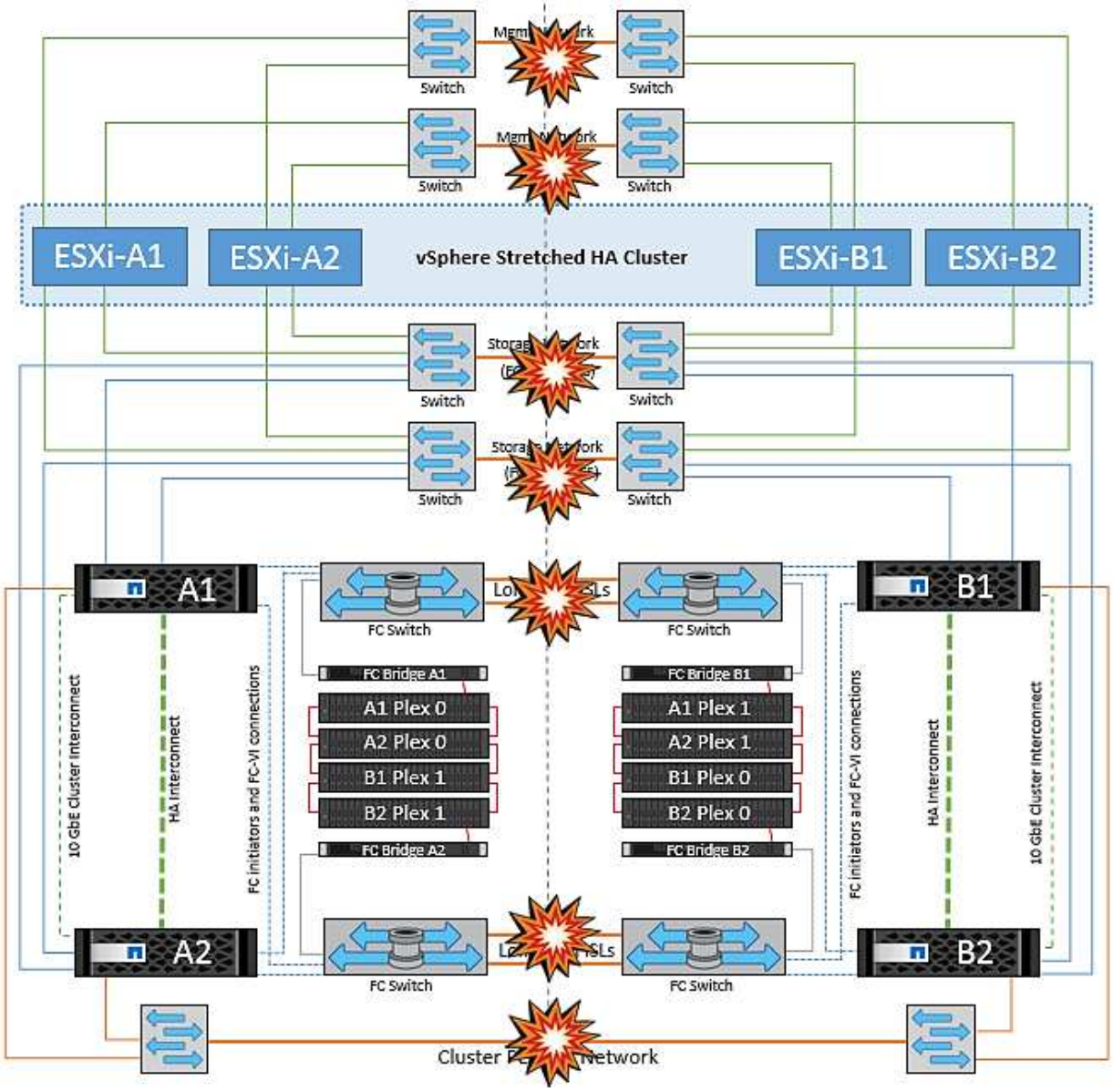



すべてのスイッチ間障害またはデータセンターの完全なパーティション

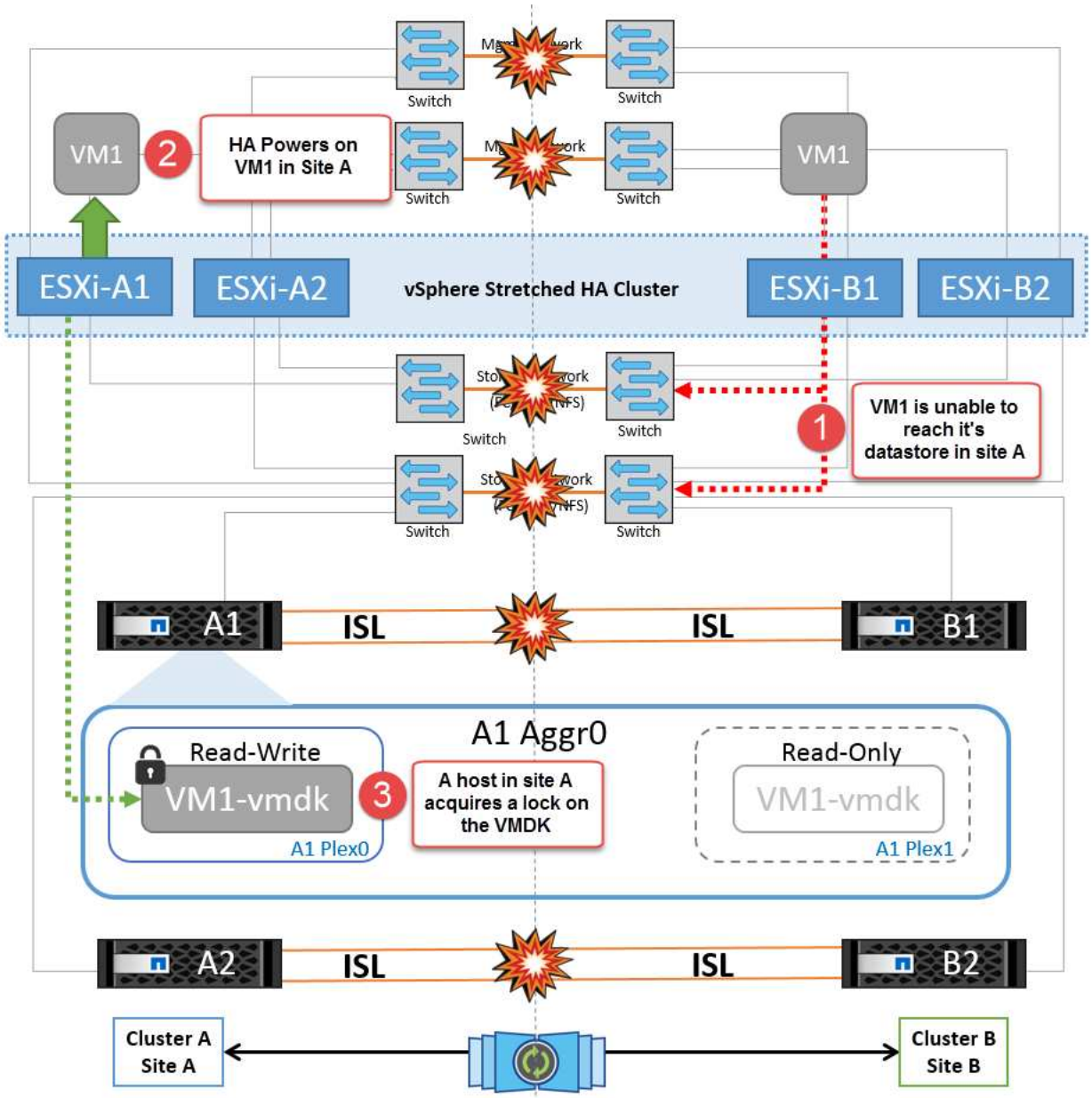
このシナリオでは、サイト間のすべてのISLリンクが停止し、両方のサイトが相互に分離されます。管理ネットワークやストレージネットワークでのISL障害などのシナリオで説明したように、ISL全体で障害が発生しても仮想マシンは影響を受けません。

ESXiホストがサイト間でパーティショニングされると、vSphere HAエージェントがデータストアハートビートをチェックし、各サイトでローカルのESXiホストがデータストアハートビートを対応する読み書き可能なボリューム/ LUNに更新できるようになります。サイトAのホストは、ネットワーク/データストアハートビートがないため、サイトBの他のESXiホストで障害が発生したと見なします。サイトAのvSphere HAはサイトBの仮想マシンの再起動を試行しますが、ストレージISLの障害が原因でサイトBのデータストアにアクセスで

きなくなるため、再起動は失敗します。同様の状況がサイトBでも繰り返されます。



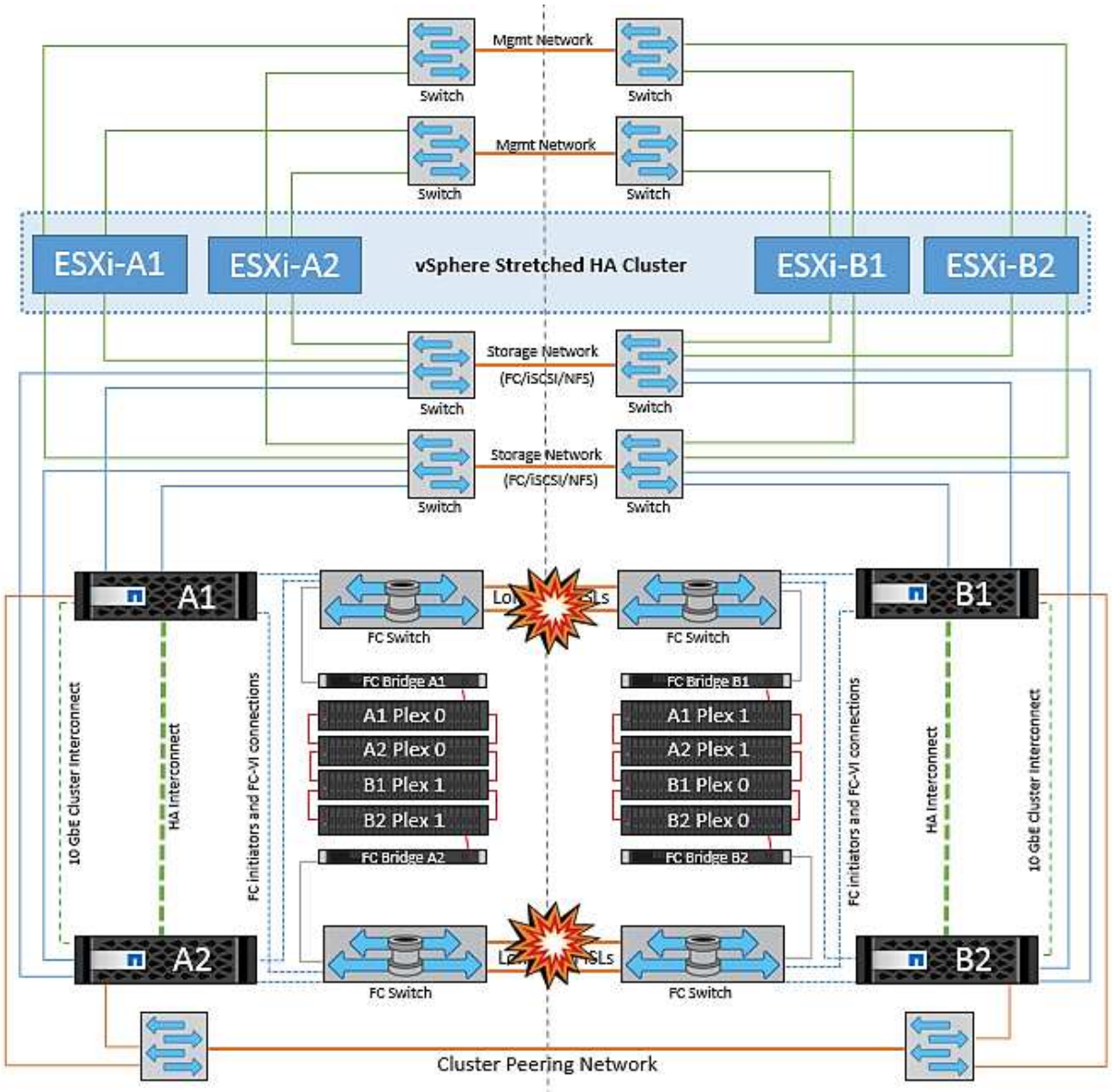

NetAppでは、DRSルールに違反した仮想マシンがないかどうかを確認することを推奨しています。リモートサイトから実行されている仮想マシンはデータストアにアクセスできないため停止し、vSphere HAはその仮想マシンをローカルサイトで再起動します。ISLリンクがオンラインに戻ると、同じMACアドレスで仮想マシンのインスタンスが2つ実行されることはないため、リモートサイトで実行されていた仮想マシンが強制終了されます。




**NetApp MetroCluster**の両方のファブリックのスイッチ間リンク障害

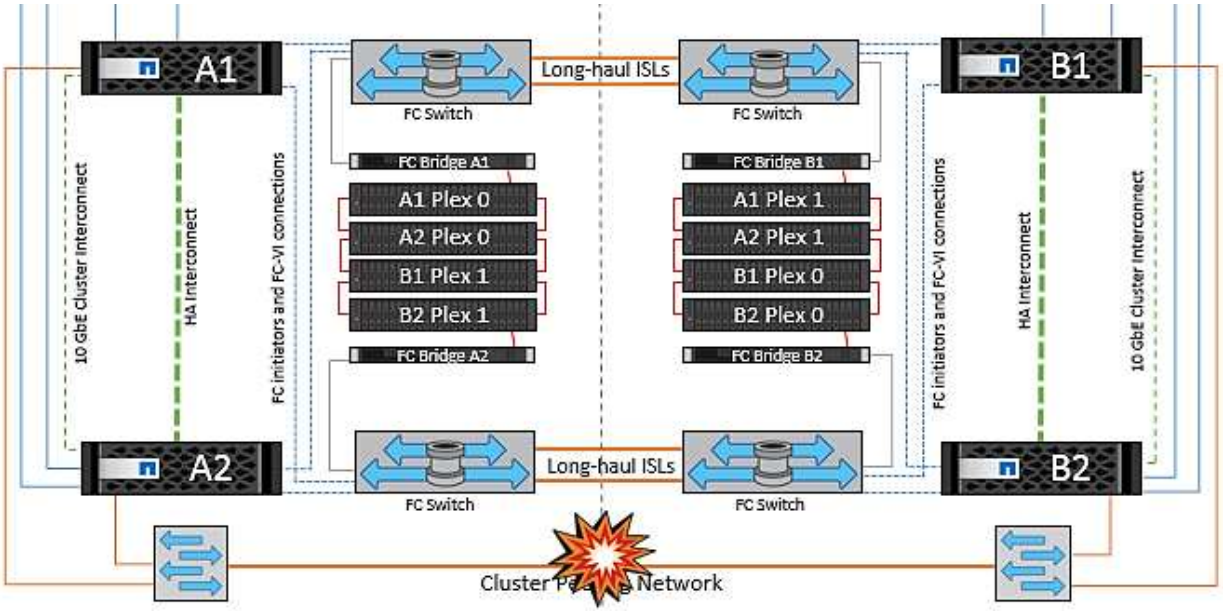
1つ以上のISLで障害が発生した場合、トラフィックは残りのリンクを経由して続行されます。両方のファブリックのすべてのISLで障害が発生し、ストレージとNVRAMのレプリケーション用のサイト間のリンクがなくなった場合、各コントローラはローカルデータの提供を継続します。少なくとも1つのISLをリストアすると、すべてのプレックスの再同期が自動的に実行されます。

すべてのISLが停止したあとに発生した書き込みは、もう一方のサイトにミラーリングされません。そのため、構成がこの状態のときに災害時にスイッチオーバーを実行すると、同期されていなかったデータが失われます。この場合、スイッチオーバー後のリカバリを手動で行う必要があります。ISLが長期間使用できなくなる可能性がある場合は、災害時のスイッチオーバーが必要な場合にデータ損失のリスクを回避するために、すべてのデータサービスをシャットダウンすることができます。この処理を実行するかどうかは、少なくとも1つのISLが使用可能になる前にスイッチオーバーが必要な災害が発生する可能性と比較して判断する必要があります。また、ISLで連鎖的に障害が発生した場合は、すべてのリンクで障害が発生する前に、いずれかのサイトへの計画的スイッチオーバーをトリガーすることもできます。




ピアクラスタのリンク障害

ピアクラスタのリンクで障害が発生した場合、ファブリックのISLはアクティブなままであるため、データサービス（読み取りと書き込み）は両方のサイトで両方のプレックスに対して継続されます。クラスタ設定の変更（新しいSVMの追加、既存のSVMでのボリュームやLUNのプロビジョニングなど）は、もう一方のサイトに伝播できません。これらはローカルのCRSメタデータボリュームに保持され、ピアクラスタリンクのリストア時にもう一方のクラスタに自動的に伝播されます。ピアクラスタのリンクがリストアされる前に強制スイッチオーバーが必要な場合は、スイッチオーバープロセスの一環として、サバイバーサイトにあるメタデータボリュームのリモートレプリケートコピーから、未処理のクラスタ構成変更が自動的に再生されます。



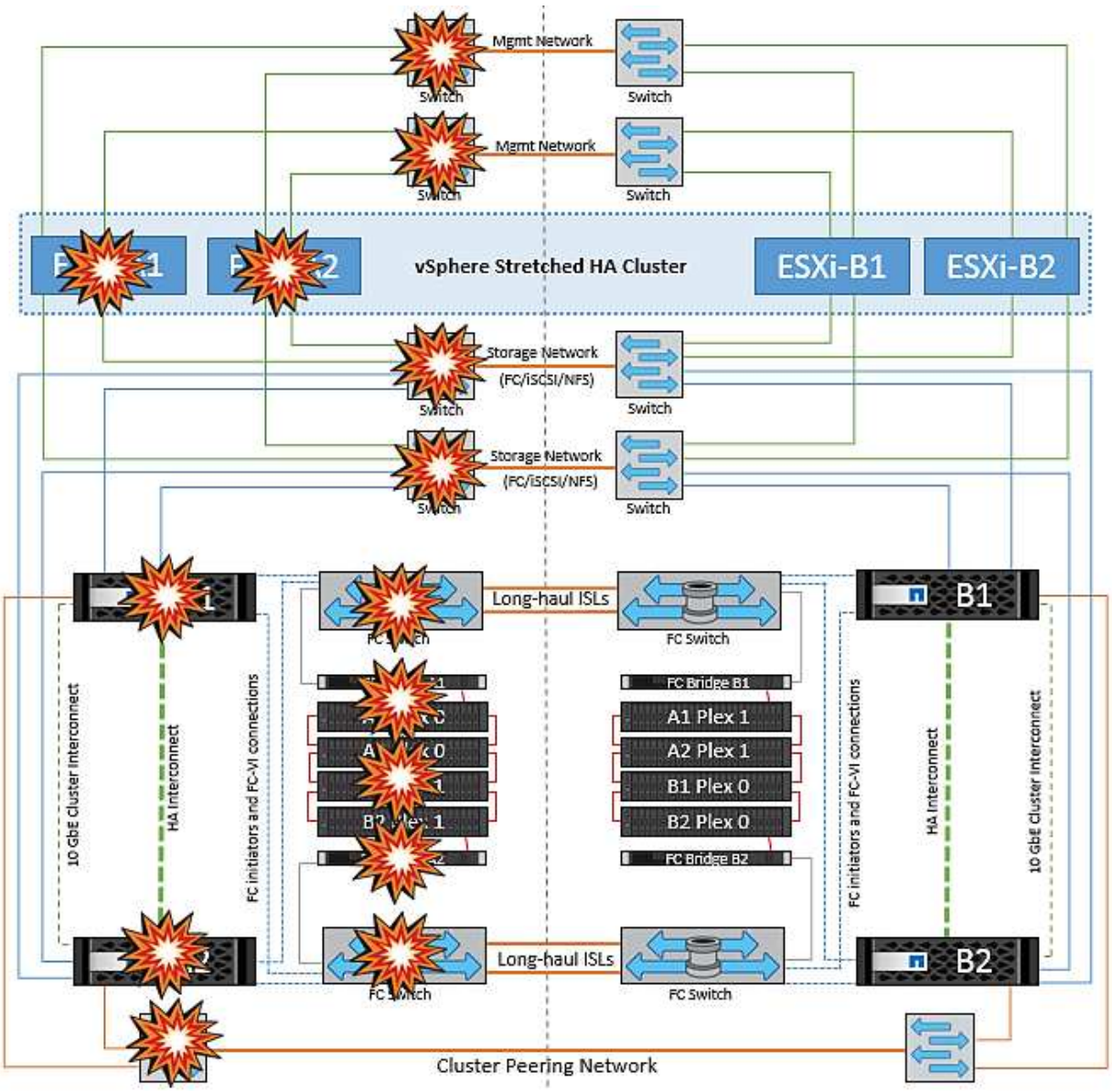

サイト全体の障害

サイトA全体で障害が発生した場合、サイトAのESXiホストが停止しているため、サイトBのESXiホストはサイトAのESXiホストからネットワークハートビートを受信しません。サイトBのHAマスターは、データストアハートビートが存在しないことを確認し、サイトAのホストで障害が発生したことを宣言して、サイトAの仮想マシンをサイトBで再起動しようとします。この間に、ストレージ管理者はスイッチオーバーを実行して障害が発生したノードのサービスをサバイバーサイトで再開し、サイトAのすべてのストレージサービスをサイトBでリストアします。サイトAのボリュームまたはLUNがサイトBで使用可能になると、HAマスターエージェントはサイトAの仮想マシンをサイトBで再起動しようとします。

vSphere HAマスターエージェントがVMの再起動（VMの登録と電源投入を含む）に失敗した場合、遅延後に再起動が再試行されます。再起動の間隔は、最大30分まで設定できます。vSphere HAは、再起動を最大試行回数（デフォルトでは6回）試行します。

注： HAマスターは、Placement Managerが適切なストレージを検出するまで再起動の試行を開始しません。したがって、サイト全体で障害が発生した場合は、スイッチオーバーの実行後に再起動が試行されます。

サイトAがスイッチオーバーされた場合は、サバイバーサイトBのいずれかのノードで障害が発生しても、サバイバーノードにフェイルオーバーすることでシームレスに対応できます。この場合、4つのノードの作業は1つのノードだけで実行されます。この場合のリカバリでは、ローカルノードへのギブバックを実行します。その後、サイトAがリストアされるとスイッチバック処理が実行され、構成の安定した運用が再開されます。




# 製品のセキュリティ

## VMware vSphere 用の ONTAP ツール

ONTAP Tools for VMware vSphereを使用したソフトウェアエンジニアリングでは、次のセキュアな開発アクティビティを採用しています。

- * 脅威モデリング。 * 脅威モデリングの目的は、ソフトウェア開発ライフサイクルの早い段階で、機能、コンポーネント、または製品のセキュリティ上の欠陥を発見することです。脅威モデルとは、アプリケーションのセキュリティに影響するすべての情報を構造化したものです。本質的に、これはセキュリティの観点から見たアプリケーションとその環境です。
- * Dynamic Application Security Testing （ DAST ）。 * このテクノロジーは、実行中のアプリケーションで脆弱な状態を検出するように設計されています。DAST は、 Web 対応アプリケーションの公開 HTTP および HTML インターフェイスをテストします。
- * サードパーティーのコード通貨。 * オープンソース・ソフトウェア（ OSS ）を使用したソフトウェア開発の一環として、製品に組み込まれた OSS に関連するセキュリティ上の脆弱性に対処する必要がありま

す。これは継続的な取り組みです。新しい OSS バージョンには、いつでも新たに検出された脆弱性が報告される可能性があります。

- * 脆弱性スキャン。 * 脆弱性スキャンは、お客様にリリースされる前にネットアップ製品の一般的なセキュリティの脆弱性と既知のセキュリティの脆弱性を検出するためのものです。
- * ペネトレーションテスト。 * ペネトレーションテストは、システム、 Web アプリケーション、またはネットワークを評価して、攻撃者によって悪用される可能性のあるセキュリティの脆弱性を検出するプロセスです。ネットアップでのペネトレーションテスト（ペンテスト）は、承認された信頼できる第三者企業のグループが実施します。テスト範囲には、高度な攻撃方法やツールを使用した悪意のある侵入者やハッカーと同様のアプリケーションまたはソフトウェアに対する攻撃の開始が含まれます。

製品のセキュリティ機能

ONTAP Tools for VMware vSphereの各リリースには、次のセキュリティ機能が含まれています。

- * ログインバナー。 * SSH はデフォルトでは無効になっており、 VM コンソールから有効になっている場合は 1 回限りのログインしか許可されません。ユーザがログインプロンプトでユーザ名を入力すると、次のログインバナーが表示されます。
- 警告： * このシステムへの不正アクセスは禁止されており、法律で訴追されます。このシステムにアクセスすることで、不正な使用が疑われる場合に、ユーザーのアクションが監視される可能性があることに同意したものとみなされます。

  ユーザがSSHチャネルを介したログインを完了すると、次のテキストが表示されます。

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * ロールベースアクセス制御 (RBAC) 。 * ONTAP ツールには、次の 2 種類の RBAC 制御が関連付けられています。
  - vCenter Server 標準の権限
  - vCenter プラグインに固有の権限。詳細については、を参照してください "リンクをクリックしてください"。
- * 暗号化された通信チャネル。 * すべての外部通信は、バージョン 1.2 の TLS を使用して HTTPS 経由で行われます。
- * 最小限のポート露出。 * 必要なポートのみがファイアウォールで開かれています。

  次の表に、オープンポートの詳細を示します。

| **TCP v4 / V6** ポート番号 | 方向（ **Direction** ） | 機能 |
|---|---|---|
| 8143 | インバウンド | REST API 用の HTTPS 接続 |
| 8043 | インバウンド | HTTPS 接続 |

| TCP v4 / V6 ポート番号 | 方向（ Direction ） | 機能 |
| --- | --- | --- |
| 9060 | インバウンド | HTTPS 接続<br>SOAP over https 接続に使用されます<br>クライアントがONTAP tools APIサーバに接続できるようにするには、このポートを開く必要があります。 |
| 22 | インバウンド | SSH （デフォルトでは無効） |
| 9080 | インバウンド | HTTPS 接続 - VP および SRA - ループバックからの内部接続のみ |
| 9083年だ | インバウンド | HTTPS 接続 - VP および SRA<br>SOAP over https 接続に使用されます |
| 一一六二 | インバウンド | VP SNMP トラップパケット |
| 1527年 | 内部のみ | Derby データベースポート。このコンピュータとそれ自体の間のみ、外部接続は許可されません — 内部接続のみ |
| 443 | 双方向 | ONTAP クラスタへの接続に使用します |

- * 認証局（ CA ）署名証明書のサポート。 * VMware vSphere 用の ONTAP ツールは CA 署名証明書をサポートしています。を参照してください "こちらの技術情報アーティクル" を参照してください。
- * 監査ログ。 * サポートバンドルはダウンロード可能で、非常に詳細です。ONTAP ツールは、すべてのユーザログインおよびログアウトアクティビティを個別のログファイルに記録します。VASA API 呼び出しは、専用の VASA 監査ログ（ローカルの cxf.log ）に記録されます。
- * パスワードポリシー。 * 次のパスワードポリシーが適用されます。
  - パスワードはどのログファイルにも記録されません。
  - パスワードはプレーンテキストで伝達されません。
  - パスワードは、インストールプロセスで設定します。
  - パスワード履歴は設定可能なパラメータです。
  - パスワードの最小有効期間は 24 時間に設定されます。
  - パスワードフィールドの自動入力は無効です。
  - ONTAP ツールは、保存されているすべてのクレデンシャル情報を SHA256 ハッシュで暗号化し

## SnapCenterプラグインVMware vSphere

NetApp SnapCenter Plug-in for VMware vSphereのソフトウェアエンジニアリングでは、次のような安全な開発作業を行います。

- * 脅威モデリング。 * 脅威モデリングの目的は、ソフトウェア開発ライフサイクルの早い段階で、機能、コンポーネント、または製品のセキュリティ上の欠陥を発見することです。脅威モデルとは、アプリケー

ションのセキュリティに影響するすべての情報を構造化したものです。本質的に、これはセキュリティの観点から見たアプリケーションとその環境です。

- *動的アプリケーションセキュリティテスト(DAST)。*実行中のアプリケーションの脆弱な状態を検出するように設計されたテクノロジ。DAST は、 Web 対応アプリケーションの公開 HTTP および HTML インターフェイスをテストします。
- *サードパーティのコード通貨。*ソフトウェアの開発およびオープンソースソフトウェア（OSS）の使用の一環として、製品に組み込まれているOSSに関連するセキュリティの脆弱性に対処することが重要です。これは、OSSコンポーネントのバージョンに、いつでも新たに検出された脆弱性が報告される可能性があるため、継続的な取り組みです。
- * 脆弱性スキャン。 * 脆弱性スキャンは、お客様にリリースされる前にネットアップ製品の一般的なセキュリティの脆弱性と既知のセキュリティの脆弱性を検出するためのものです。
- *ペネトレーションテスト。*ペネトレーションテストは、システム、Webアプリケーション、またはネットワークを評価して、攻撃者によって悪用される可能性のあるセキュリティの脆弱性を検出するプロセスです。ネットアップでのペネトレーションテスト（ペンテスト）は、承認された信頼できる第三者企業のグループが実施します。このテスト範囲には、高度な攻撃方法やツールを使用した悪意のある侵入者やハッカーなどのアプリケーションやソフトウェアに対する攻撃の開始が含まれます。
- *製品セキュリティインシデント対応アクティビティ。*セキュリティの脆弱性は社内外で発見され、タイムリーに対処しなければ、ネットアップの評判に深刻なリスクをもたらす可能性があります。このプロセスを容易にするために、Product Security Incident Response Team（PSIRT）は脆弱性を報告して追跡します。

製品のセキュリティ機能

NetApp SnapCenter Plug-in for VMware vSphereの各リリースには、次のセキュリティ機能が含まれています。

- 制限付きシェルアクセス。 SSHはデフォルトで無効になっており、1回限りのログインはVMコンソールから有効にした場合にのみ許可されます。
- *ログインバナーのアクセス警告*ログインプロンプトにユーザ名を入力すると、次のログインバナーが表示されます。
- 警告： * このシステムへの不正アクセスは禁止されており、法律で訴追されます。このシステムにアクセスすることで、不正な使用が疑われる場合に、ユーザーのアクションが監視される可能性があることに同意したものとみなされます。

  ユーザがSSHチャネルを介したログインを完了すると、次の出力が表示されます。

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * ロールベースアクセス制御 (RBAC) 。 * ONTAP ツールには、次の 2 種類の RBAC 制御が関連付けられています。
  - vCenter Server標準の権限。

- VMware vCenterプラグインに固有の権限。詳細については、を参照してください "ロールベースアクセス制御（ RBAC ）"。

- *暗号化された通信チャネル。*すべての外部通信は、TLSを使用してHTTPS経由で行われます。
- * 最小限のポート露出。 * 必要なポートのみがファイアウォールで開かれています。

次の表に、オープンポートの詳細を示します。

| TCP v4 / V6ポート番号 | 機能 |
|---|---|
| 8144 | REST API 用の HTTPS 接続 |
| 8080 です | OVA GUIでのHTTPS接続 |
| 22 | SSH（デフォルトでは無効） |
| 3306 | mysql（内部接続のみ。外部接続はデフォルトで無効） |
| 443 | nginx（データ保護サービス） |

- 認証局（**CA**）署名証明書のサポート。 SnapCenter Plug-in for VMware vSphereは、CA署名証明書の機能をサポートしています。を参照してください "SnapCenter Plug-in for VMware vSphere（SCV）にSSL証明書を作成/インポートする方法"。
- *パスワードポリシー。*次のパスワードポリシーが有効です。
  - パスワードはどのログファイルにも記録されません。
  - パスワードはプレーンテキストで伝達されません。
  - パスワードは、インストールプロセスで設定します。
  - クレデンシャル情報はすべてSHA256ハッシュを使用して保存されます。
- *基本オペレーティングシステムイメージ。*この製品は、アクセス制限とシェルアクセスが無効になったOVA用のDebianベースOSに同梱されています。これにより、攻撃のフットプリントが削減されます。すべてのSnapCenter リリースベースのオペレーティングシステムには、最大限のセキュリティを適用できる最新のセキュリティパッチが適用されています。

ネットアップでは、SnapCenter Plug-in for VMware vSphereアプライアンスに関連するソフトウェア機能およびセキュリティパッチを開発し、その後、バンドルソフトウェアプラットフォームとしてお客様にリリースします。ネットアップでは、これらのアプライアンスにはLinuxのサブシステムに固有の依存関係と独自のソフトウェアが含まれているため、サブオペレーティングシステムを変更しないことを推奨します。これは、ネットアップアプライアンスに影響を及ぼす可能性が高いためです。これは、ネットアップがアプライアンスをサポートできるかどうかに影響します。アプライアンスはセキュリティ関連の問題にパッチを適用するためにリリースされているため、最新のコードバージョンをテストして導入することを推奨します。

# ONTAP tools for VMware vSphere向けセキュリティ強化ガイド

## ONTAP tools for VMware vSphere向けセキュリティ強化ガイド

ONTAP tools for VMware vSphereのセキュリティ強化ガイドには、最も安全な設定を構成するための包括的な手順が記載されています。

これらのガイドは、アプライアンス自体のアプリケーションとゲストOSの両方に適用されます。

## ONTAP Tools for VMware vSphereインストールパッケージの整合性の検証

ONTAP toolsインストールパッケージの整合性を検証するには、2つの方法があります。

1. チェックサムの確認
2. シグネチャの検証

チェックサムは、OTVインストールパッケージのダウンロードページで提供されています。ダウンロードしたパッケージのチェックサムを、ダウンロードページに表示されているチェックサムと照合して確認する必要があります。

### ONTAP tools OVAの署名の確認

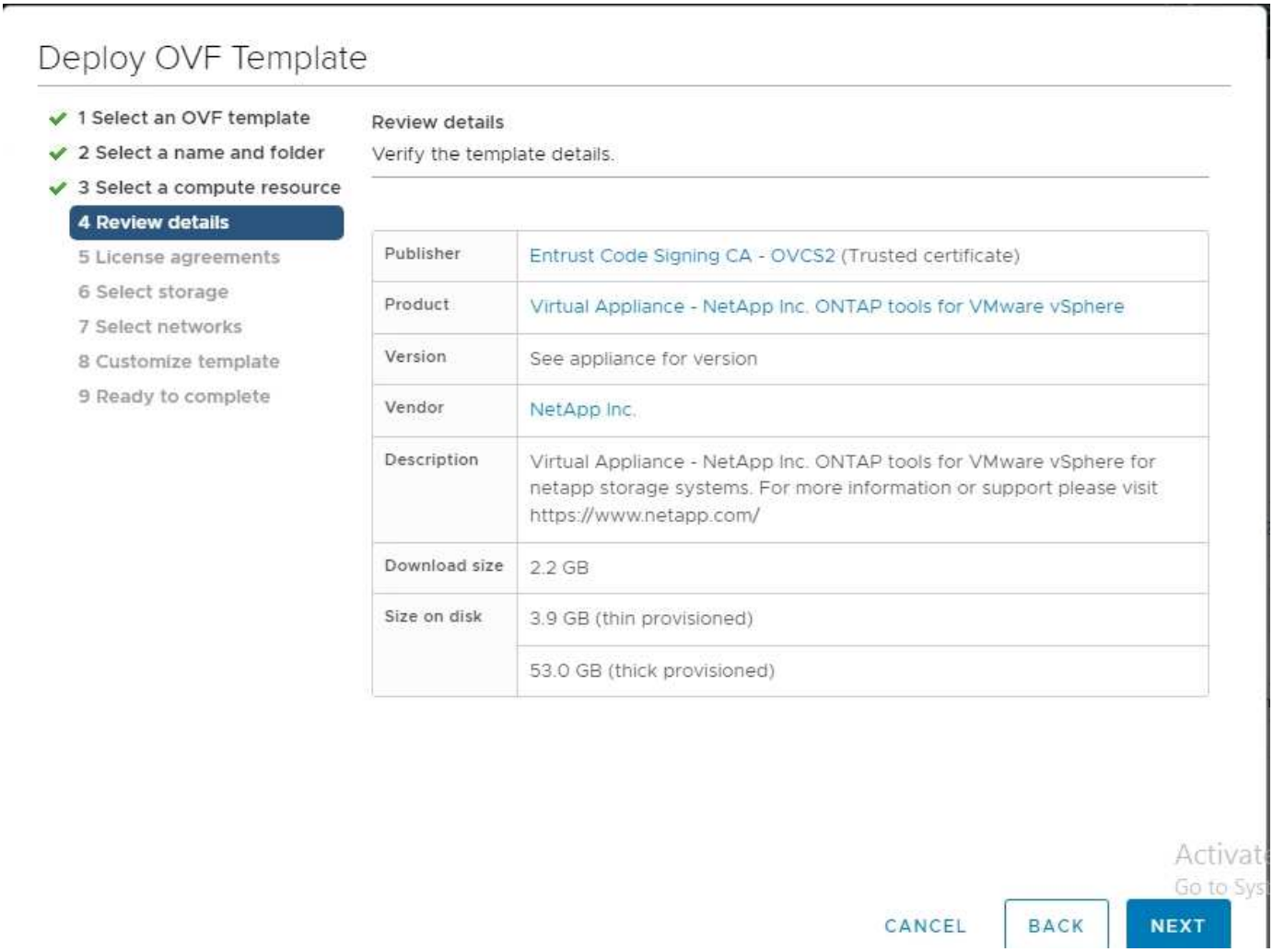
vAppインストールパッケージはtarball形式で提供されます。このtarballには、仮想アプライアンスの中間証明書とルート証明書、READMEファイル、OVAパッケージが含まれています。READMEファイルには、vApp OVAパッケージの整合性を検証する方法が記載されています。

また、提供されたルート証明書と中間証明書をvCenterバージョン7.0U3E以降にアップロードする必要があります。 vCenterのバージョン7.0.1から7.0.U3Eの場合、証明書を検証する機能はVMwareではサポートされていません。vCenterバージョン6.xの証明書はアップロードする必要はありません。

#### 信頼されたルート証明書の**vCenter**へのアップロード

1. VMware vSphere ClientでvCenter Serverにログインします。
2. administrator@vsphere.localまたはvCenter Single Sign-On Administratorsグループの別のメンバーのユーザ名とパスワードを指定します。インストール時に別のドメインを指定した場合は、administrator@mydomainとしてログインします。
3. 証明書管理ユーザーインターフェイスに移動します。a.[ホーム]メニューから[管理]を選択します。B[証明書]で、[証明書管理]をクリックします。
4. プロンプトが表示されたら、vCenter Serverのクレデンシャルを入力します。
5. [信頼されたルート証明書]で、[追加]をクリックします。
6. [browse]をクリックし、証明書の.pemファイル（otv_ova_inter_root_cert_chain.pem）の場所を選択します。
7. 追加をクリックします。証明書がストアに追加されます。

を参照してください "証明書ストアへの信頼されたルート証明書の追加" を参照してください。（OVAファイルを使用して）vAppを導入する際、vAppパッケージのデジタル署名は[Review details]ページで確認できます。ダウンロードしたvAppパッケージが正規のものである場合は、[発行者]列に[信頼された証明書]と表示されます（次のスクリーンショットを参照）。




**ONTAP tools ISO**および**SRA tar.gz**の署名の確認

NetAppは、製品ダウンロードページでコード署名証明書をお客様と共有し、OTV-ISOおよびsra.tgzの製品zipファイルも提供しています。

コード署名証明書から、ユーザーは次のように公開鍵を抽出できます。

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-key name>
```

公開鍵を使用して、以下のように`ISO`および`tgz`製品`zip`の署名を検証する必要があります。

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file> <binary-name>
```

例

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

# ポートとプロトコル

## ここでは、ONTAP tools for VMware vSphereサーバと、管理対象のストレージシステム、サーバ、その他のコンポーネントなどのエンティティ間の通信に必要なポートとプロトコルを示します。

**OTV**に必要なインバウンドおよびアウトバウンドポート

次の表に、ONTAP toolsが適切に機能するために必要なインバウンドポートとアウトバウンドポートを示します。表に記載されているポートだけがリモートマシンからの接続用に開いていることを確認し、他のすべてのポートはリモートマシンからの接続用にブロックする必要があります。これにより、システムのセキュリティと安全性が確保されます。

次の表に、オープンポートの詳細を示します。

| * TCP v4/V6ポート番号* | * 方向 * | 機能 |
|---|---|---|
| 8143 | インバウンド | REST API 用の HTTPS 接続 |
| 8043 | インバウンド | HTTPS 接続 |
| 9060 | インバウンド | HTTPS接続+<br>SOAP over HTTPS接続に使用+<br>クライアントがONTAP tools APIサーバに接続できるようにするには、このポートを開く必要があります。 |
| 22 | インバウンド | SSH （デフォルトでは無効） |
| 9080 | インバウンド | HTTPS 接続 - VP および SRA - ループバックからの内部接続のみ |
| 9083年だ | インバウンド | HTTPS接続- VPおよびSRA+<br>SOAP over HTTPS接続に使用 |
| 一一六二 | インバウンド | VP SNMP トラップパケット |
| 8443 | インバウンド | リモートプラグイン |
| 1527年 | 内部のみ | Derbyデータベースポート、このコンピュータとそれ自体の間のみ、外部接続は許可されません-内部接続のみ |
| 8150 | 内部のみ | ログ整合性サービスはポートで実行されます |
| 443 | 双方向 | ONTAP クラスタへの接続に使用します |

**Derby**データベースへのリモートアクセスの制御

管理者は、次のコマンドを使用してDerbyデータベースにアクセスできます。ONTAP toolsのローカルVMとリ

モートサーバからアクセスするには、次の手順を実行します。

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

例：

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                     |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                     |
SYS                 |SYSCHECKS                      |
SYS                 |SYSCOLPERMS                    |
SYS                 |SYSCOLUMNS                     |
SYS                 |SYSCONGLOMERATES               |
SYS                 |SYSCONSTRAINTS                 |
SYS                 |SYSDEPENDS                     |
SYS                 |SYSFILES                       |
SYS                 |SYSFOREIGNKEYS                 |
SYS                 |SYSKEYS                        |
SYS                 |SYSPERMS                       |
```

## ONTAP Tools for VMware vSphereアクセスポイント（ユーザ）

ONTAP Tools for VMware vSphereをインストールすると、次の3種類のユーザが作成され、使用されます。

1. システムユーザ：rootユーザアカウント
2. アプリケーションユーザ：管理者ユーザ、maintユーザ、およびdbユーザアカウント
3. サポートユーザ：diagユーザアカウント

**1.**システムユーザ

システム(root)ユーザは、基盤となるオペレーティングシステム(Debian)にインストールされたONTAPツールによって作成されます。

- ONTAP toolsのインストールにより、デフォルトのシステムユーザ"root"がDebian上に作成されます。デフォルトでは無効になっており、「メンテナンス」コンソールから個別に有効にすることができます。

**2.**アプリケーションユーザ

ONTAP toolsでは、アプリケーションユーザの名前はローカルユーザです。これらは、ONTAP toolsアプリケーションで作成されたユーザです。次の表に、アプリケーションユーザのタイプを示します。

| * ユーザー * | * 概要 * |
| --- | --- |
| 管理者ユーザ | ONTAP toolsのインストール時に作成され、ONTAP toolsの導入時にユーザがクレデンシャルを指定します。ユーザは「maint」コンソールで「password」を変更できます。パスワードの有効期限は90日で、ユーザは同じパスワードを変更する必要があります。 |

| * ユーザー * | * 概要 * |
| --- | --- |
| メンテナンスユーザ | ONTAP toolsのインストール時に作成され、ONTAP toolsの導入時にユーザがクレデンシャルを指定します。ユーザは「maint」コンソールで「password」を変更できます。これはメンテナンスユーザで、メンテナンスコンソールの処理を実行するために作成されます。 |
| データベースユーザ | ONTAP toolsのインストール時に作成され、ONTAP toolsの導入時にユーザがクレデンシャルを指定します。ユーザは「maint」コンソールで「password」を変更できます。パスワードの有効期限は90日で、ユーザは同じパスワードを変更する必要があります。 |

**3.**サポートユーザ（**diag**ユーザ）

ONTAP toolsのインストール中に、サポートユーザが作成されます。このユーザを使用して、サーバで問題や停止が発生した場合にONTAPツールにアクセスしたり、ログを収集したりできます。デフォルトでは、このユーザは無効になっていますが、「メンテナンス」コンソールからアドホックで有効にすることができます。このユーザーは一定期間後に自動的に無効になることに注意することが重要です。

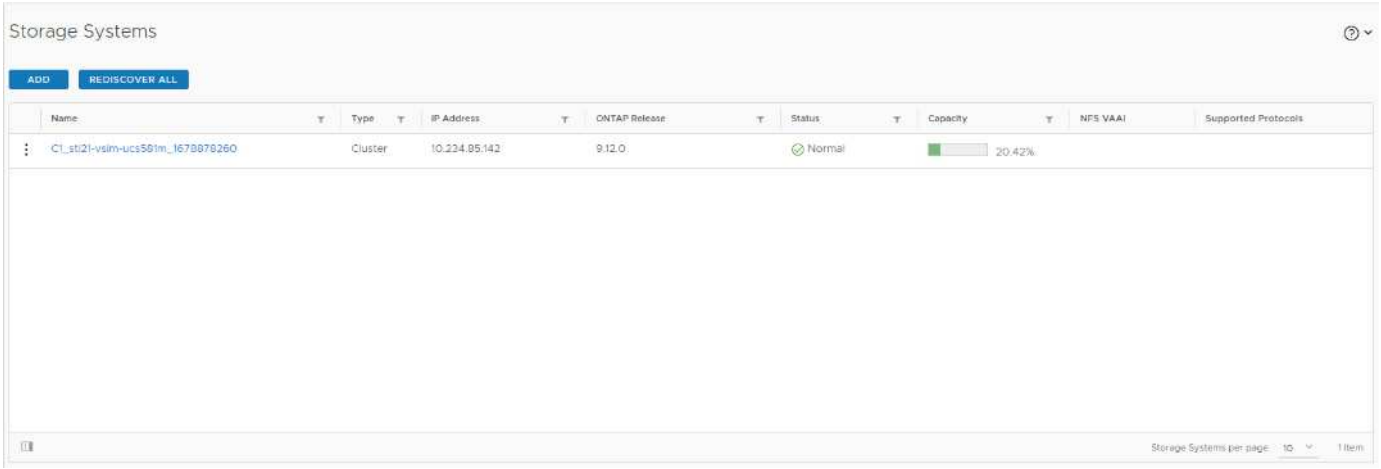
## 相互**TLS**（証明書ベースの認証）

ONTAPバージョン9.7以降では、相互TLS通信がサポートされます。ONTAP Tools for VMwareおよびvSphere 9.12以降では、新しく追加したクラスタとの通信に相互TLSが使用されます（ONTAPのバージョンによって異なります）。

### ONTAP

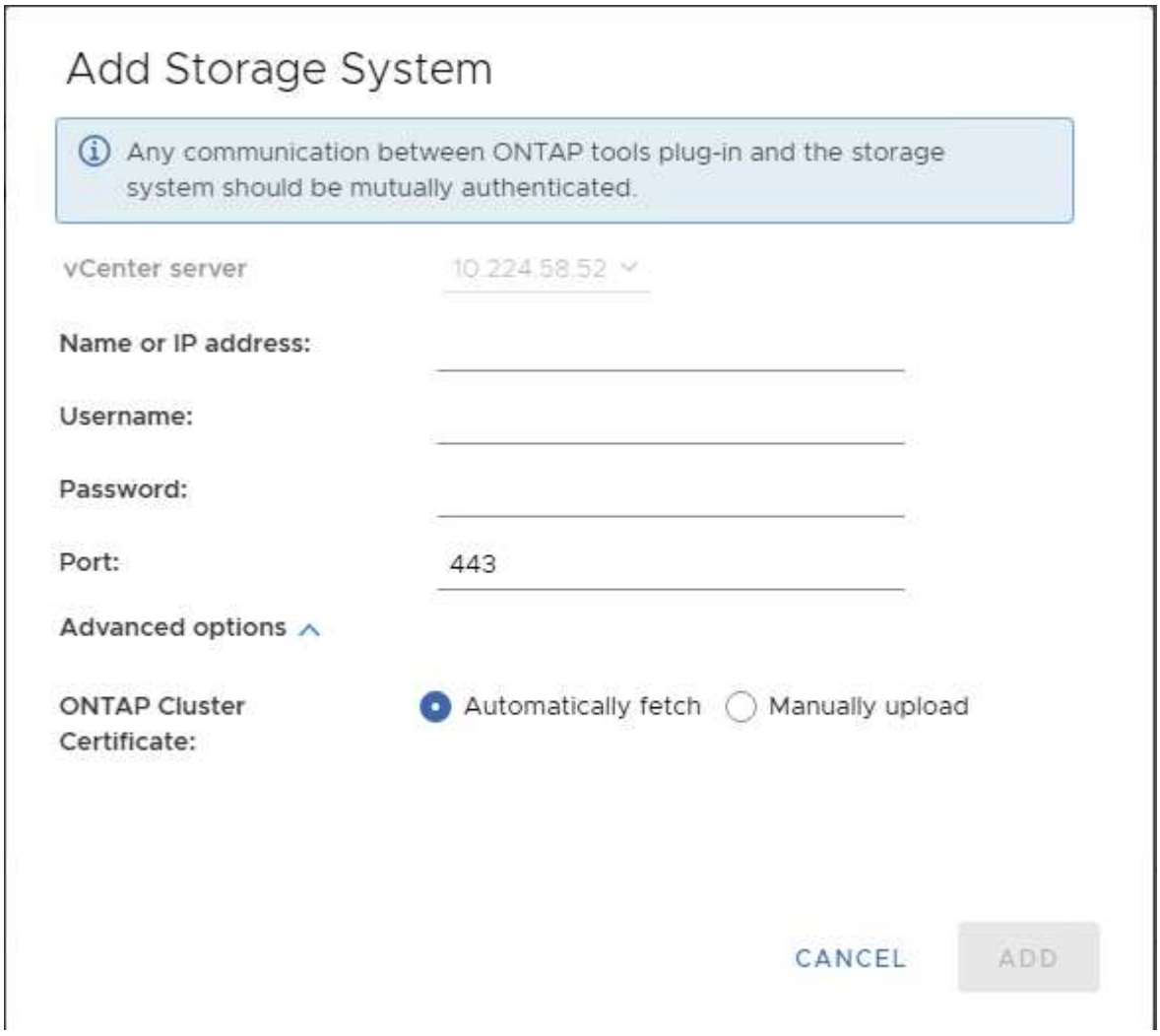
以前に追加されたすべてのストレージシステム：アップグレード中に、追加されたすべてのストレージシステムが自動信頼され、証明書ベースの認証メカニズムが設定されます。

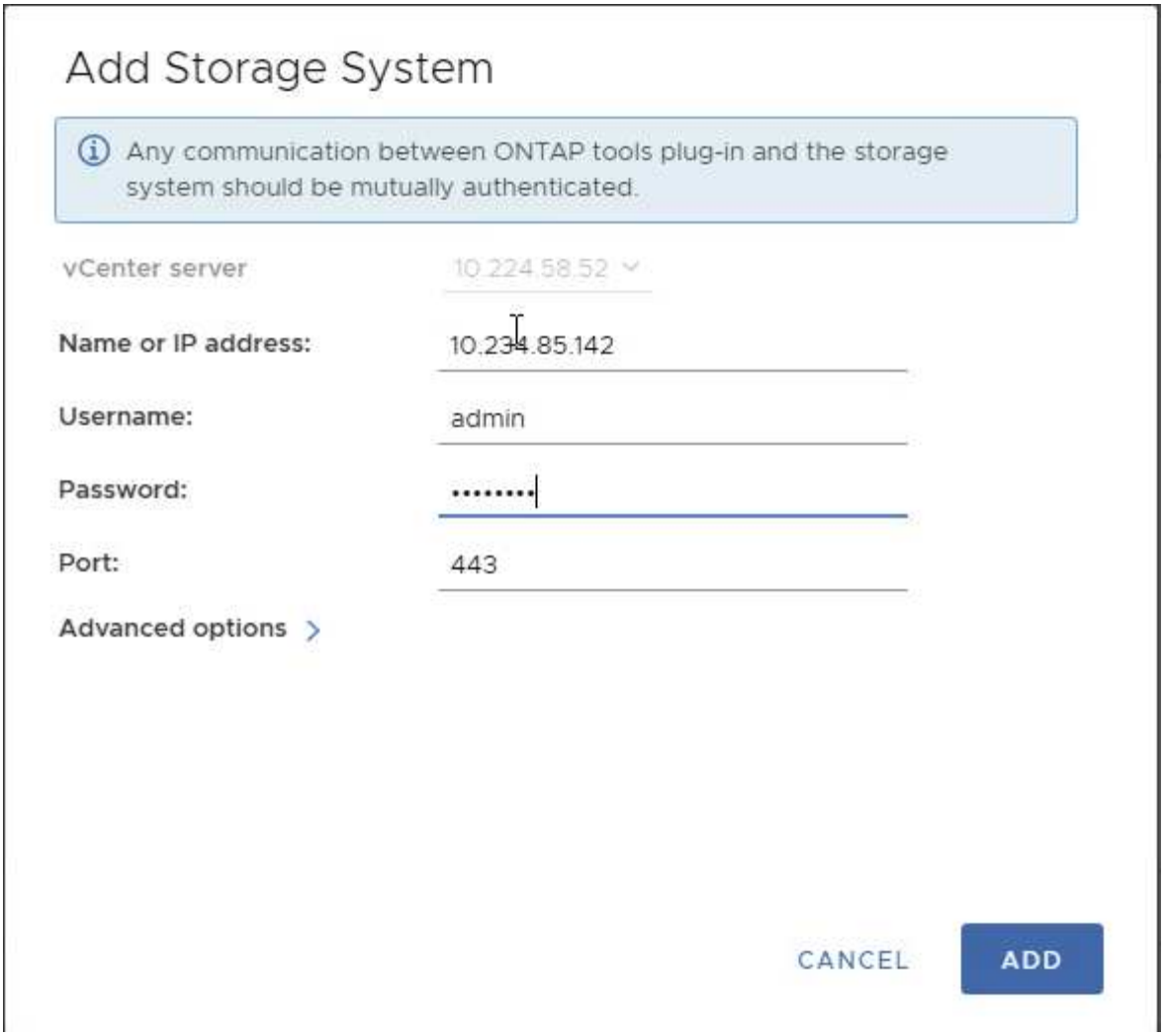
下のスクリーンショットのように、[クラスタセットアップ]ページには、各クラスタに対して設定されたMutual TLS（証明書ベースの認証）のステータスが表示されます。

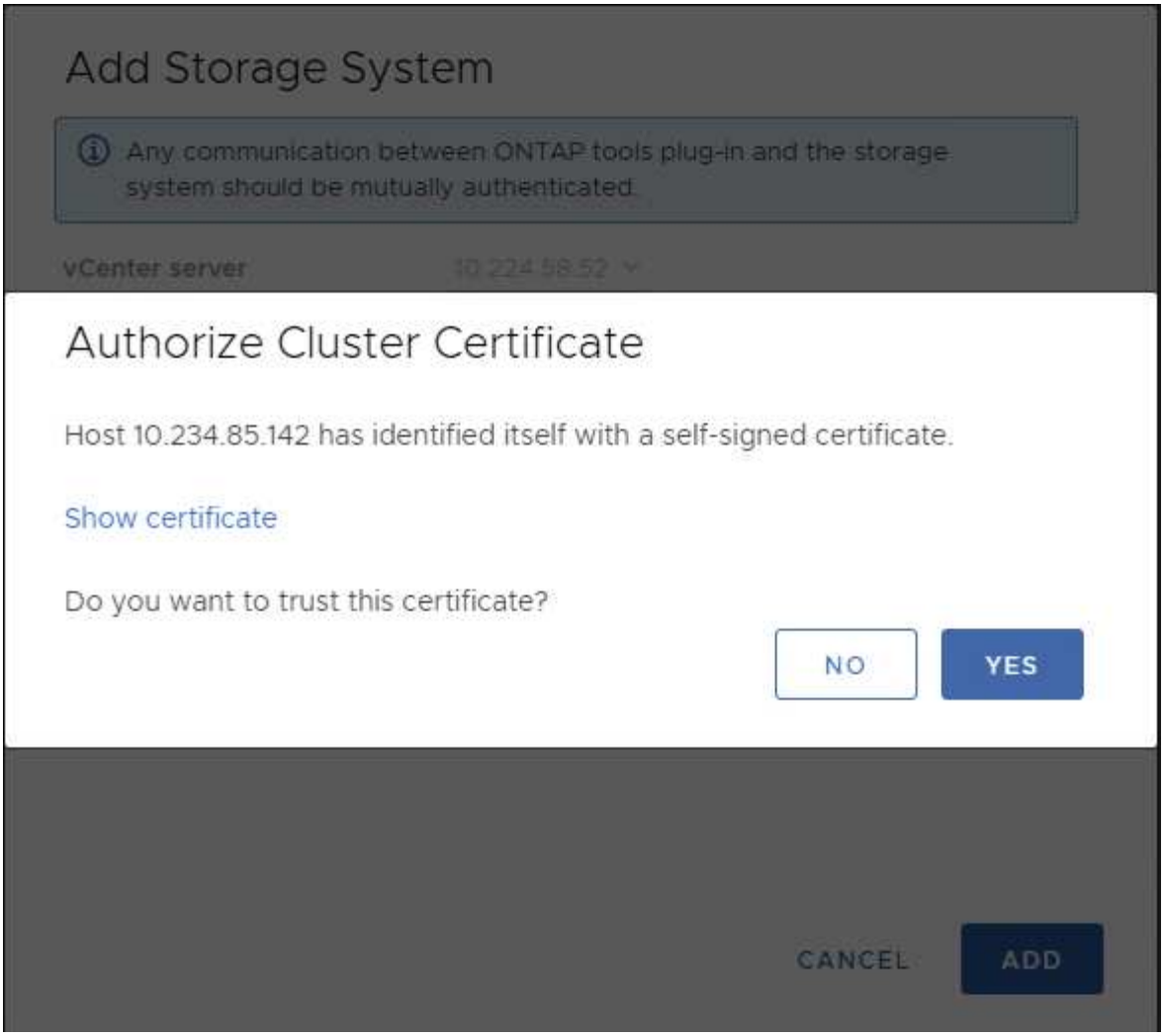


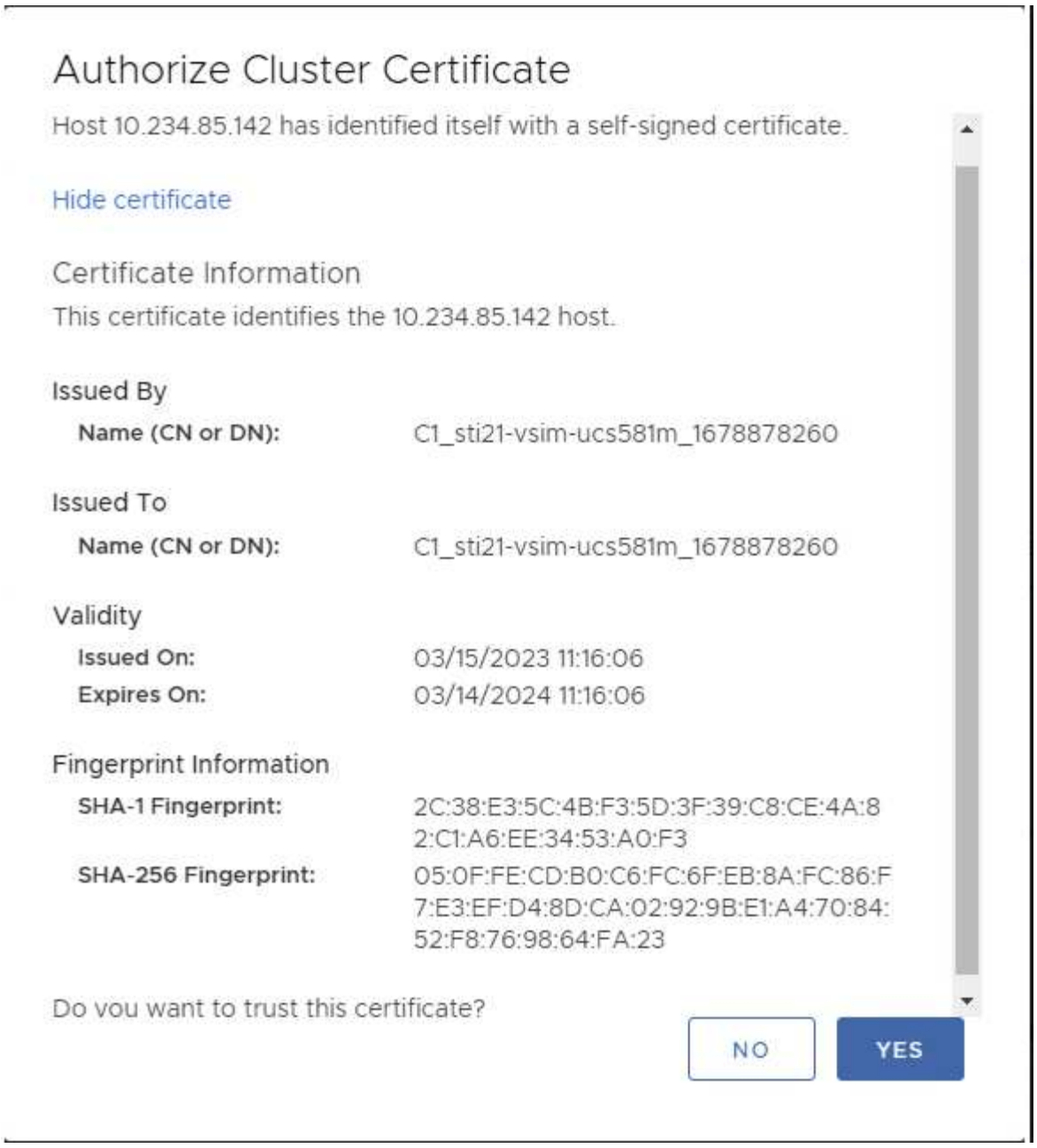

クラスタの追加

クラスタ追加のワークフロー中に、追加するクラスタがMTLSをサポートしている場合、MTLSはデフォルトで設定されます。ユーザはこの設定を行う必要はありません。次のスクリーンショットは、クラスタの追加時にユーザに表示される画面を示しています。


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
Username:
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
ADD


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

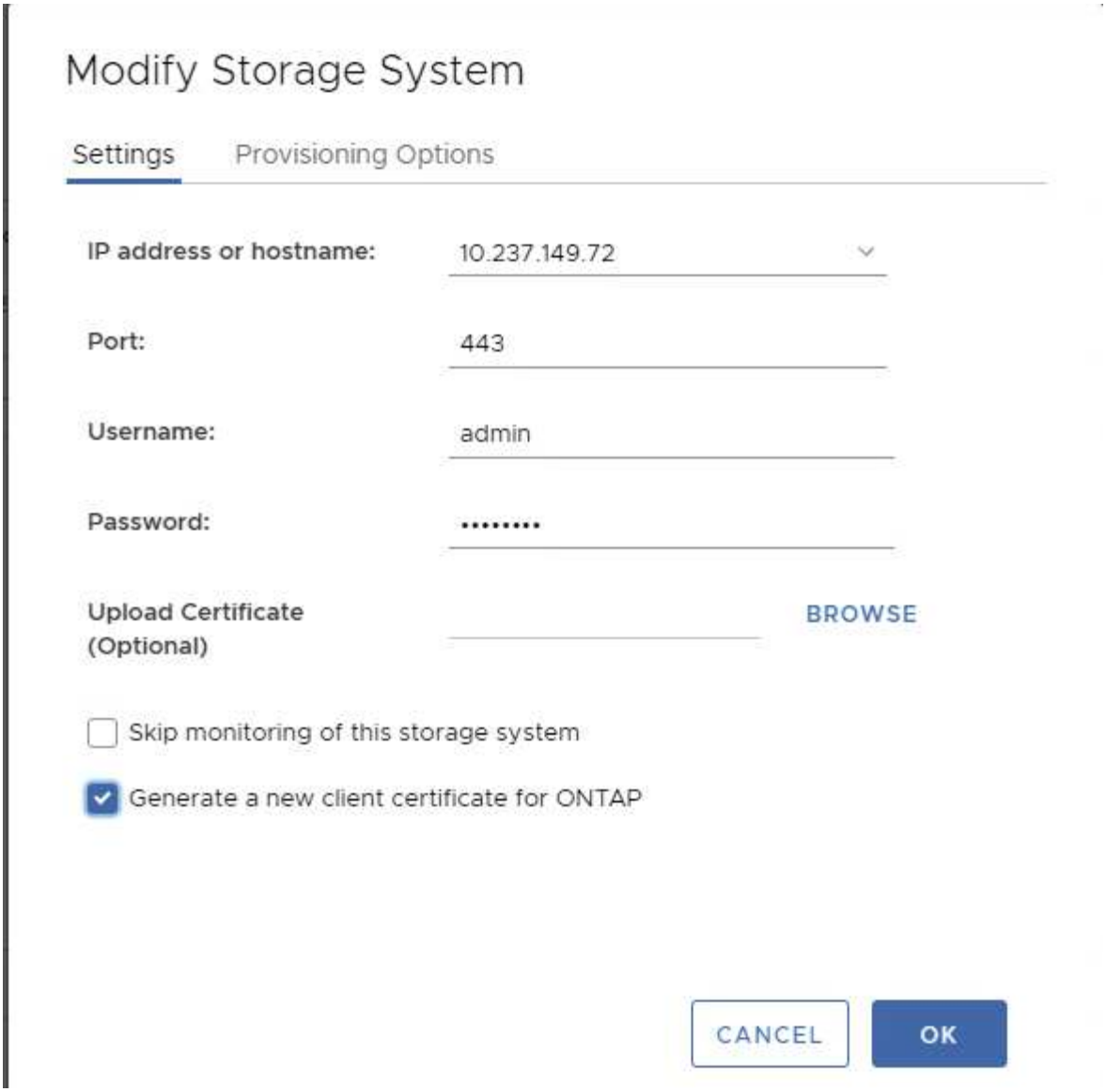

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

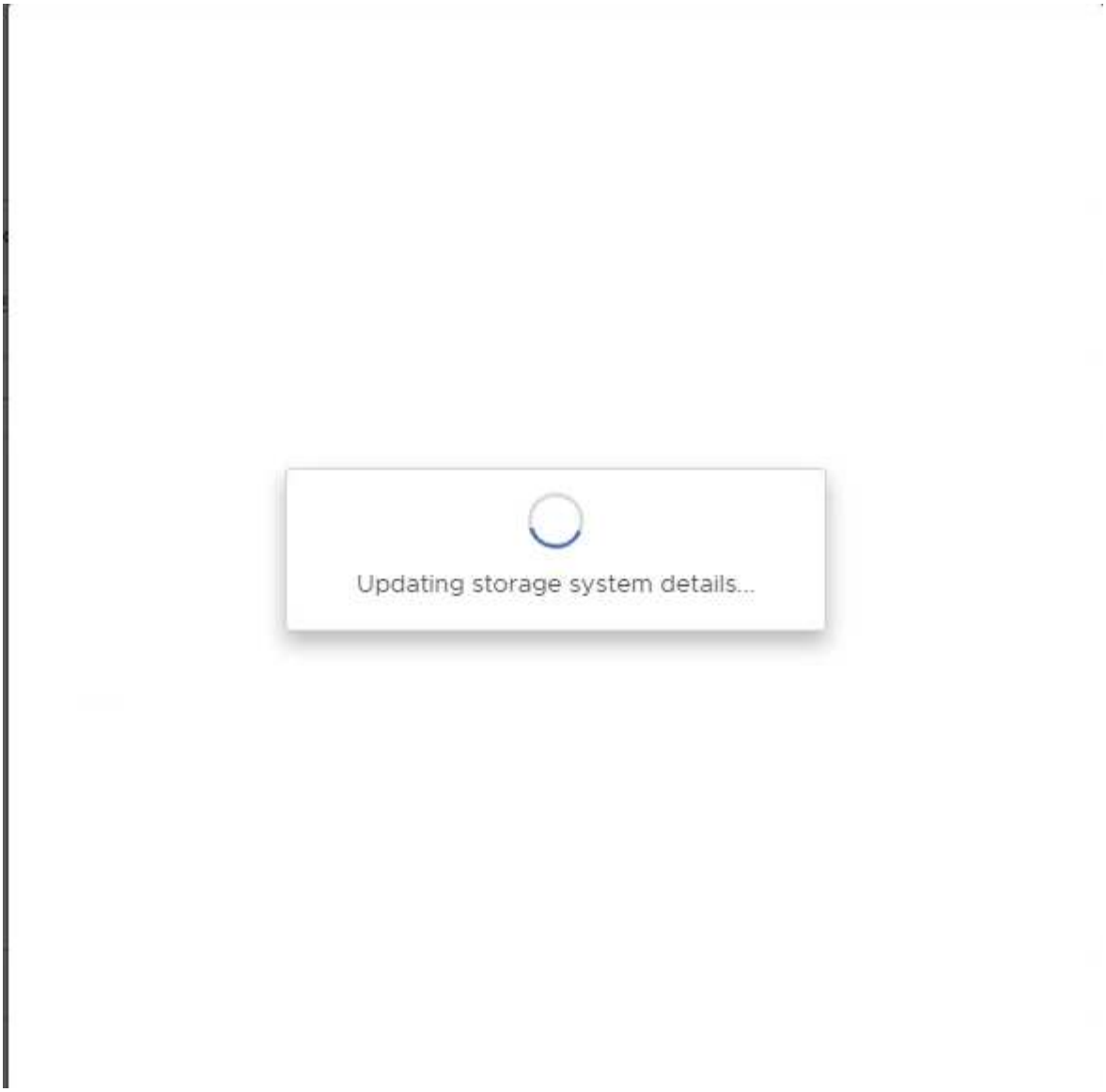



クラスタの編集

クラスタの編集処理には、次の2つのシナリオがあります。

- ONTAP証明書の有効期限が切れた場合、ユーザは新しい証明書を取得してアップロードする必要があります。
- OTV証明書の有効期限が切れた場合は、チェックボックスをオンにして証明書を再生成できます。
  - ONTAPの新しいクライアント証明書を生成します。_


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK




## ONTAP toolsのHTTPS証明書

デフォルトでは、ONTAP toolsは、Web UIへのHTTPSアクセスを保護するために、インストール時に自動的に作成される自己署名証明書を使用します。ONTAP toolsには次の機能があります。

1. HTTPS証明書の再生成

ONTAP toolsのインストール時に、HTTPS CA証明書がインストールされ、証明書がキーストアに格納されます。ユーザは、maintコンソールを使用してHTTPS証明書を再生成することができます。

上記のオプションは、'アプリケーション設定'→'証明書の再生成'に移動することで*_maint_console*でアクセスできます。

## ログインバナー

ユーザがログインプロンプトにユーザ名を入力すると、次のログインバナーが表示され

ます。SSHはデフォルトで無効になっており、VMコンソールから有効にすると1回限りのログインしか許可されないことに注意してください。

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

ユーザが SSH チャネルを介したログインを完了すると、次のテキストが表示されます。

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

## 非アクティブ時のタイムアウト

不正アクセスを防止するために、非アクティブタイムアウトが設定されます。このタイムアウトは、許可されたリソースを使用している間、一定期間非アクティブなユーザを自動的にログアウトします。これにより、許可されたユーザーのみがリソースにアクセスできるようになり、セキュリティの維持に役立ちます。

- デフォルトでは、vSphere Clientセッションはアイドル状態が120分続くと閉じます。そのため、ユーザは再度ログインしてクライアントの使用を再開する必要があります。タイムアウト値を変更するには、webclient.propertiesファイルを編集します。 vSphere Clientのタイムアウトを設定できます。 "vSphere Clientのタイムアウト値の設定"
- ONTAP toolsのWeb-CLIセッションのログアウト時間は30分です。

## ユーザあたりの最大同時要求数（ネットワークセキュリティ保護::DOS攻撃）

デフォルトでは、ユーザあたりの最大同時要求数は48です。ONTAP toolsのrootユーザは、環境の要件に応じてこの値を変更できます。この値は、**DoS**攻撃に対するメカニズムを提供するため、非常に大きな値に設定しないでください。

ユーザーは、最大同時セッション数やサポートされているその他のパラメーターを*_/opt/netapp/vscserver/etc/dosfilterParams.json _*ファイルで変更できます。

フィルタを設定するには、次のパラメータを使用します。

- ***delayMs***：レート制限を超えたすべての要求が考慮されるまでの遅延（ミリ秒単位）。要求を拒否するには-1を指定します。
- ***throttlems***:セマフォの非同期待機時間
- ***maxRequestms***：この要求の実行を許可する期間。
- ***ipWhitelist***：レート制限されないIPアドレスのカンマ区切りリスト。（vCenter、ESXi、SRAのIP）
- ***maxRequestsPerSec***：1秒あたりの接続からの最大要求数。

***dosfilterParams***ファイルのデフォルト値:

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

## ネットワークタイムプロトコル（**NTP**）の設定

ネットワーク時間設定の不一致が原因で、セキュリティの問題が発生する場合があります。このような問題を防ぐには、ネットワーク内のすべてのデバイスに正確な時間設定があることを確認することが重要です。

仮想アプライアンス

NTPサーバは、仮想アプライアンスのメンテナンスコンソールから設定できます。 ユーザは、*System Configuration⇒_* Add new NTP Server_optionでNTPサーバの詳細を追加できます。

デフォルトでは、NTPのサービスはntpdです。これはレガシーサービスであり、場合によっては仮想マシンでは適切に機能しません。

*** Debian ***

Debianでは、ユーザは/etc/ntp.confファイルにアクセスしてNTPサーバの詳細を確認できます。

## パスワードポリシー

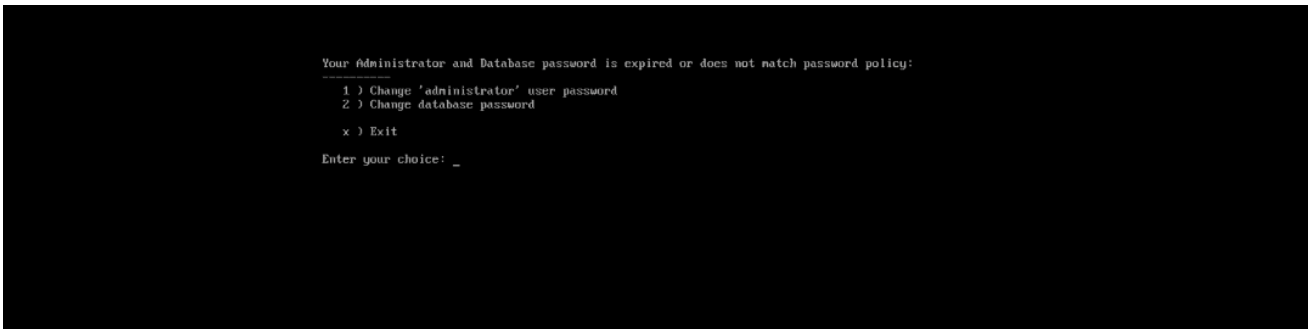
ONTAPツールを初めて導入するユーザ、またはバージョン9.12以降にアップグレードするユーザは、管理者ユーザとデータベースユーザの両方に対して、強力なパスワードポリシーに従う必要があります。導入プロセス中に、新しいユーザにパスワードの入力を求めるプロンプトが表示されます。バージョン9.12以降にアップグレードするBrownfieldユーザの場合は、メンテナンスコンソールで強力なパスワードポリシーに従うオプションを使用できます。

- ユーザがmaintコンソールにログインすると、パスワードが複雑なルールセットに照らしてチェックされ、従わなかった場合、ユーザは同じパスワードをリセットするように求められます。
- パスワードのデフォルトの有効期間は90日です。75日が経過すると、ユーザはパスワードを変更するため

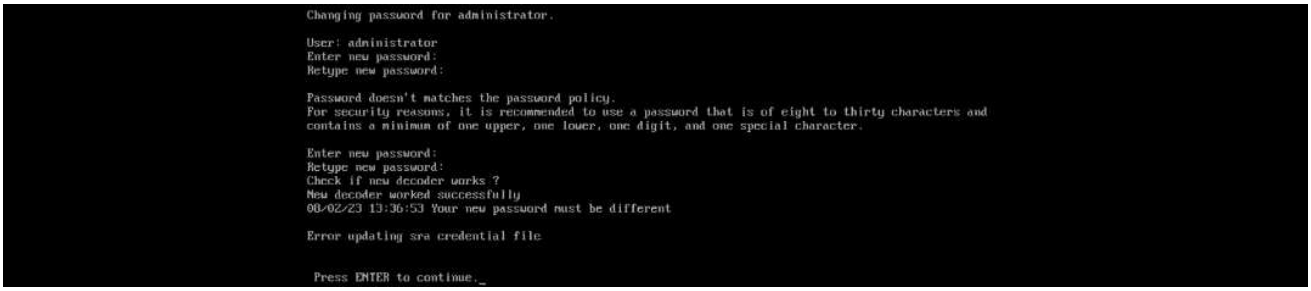
の通知を受け取り始めます。

- サイクルごとに新しいパスワードを設定する必要があります。システムは最後のパスワードを新しいパスワードとして受け取りません。
- ユーザがmaintコンソールにログインするたびに、メインメニューをロードする前に、次のスクリーンショットのようなパスワードポリシーがチェックされます。


- パスワードポリシーまたはONTAP tools 9.11以前からのアップグレードセットアップに従っていないことが検出された場合。パスワードをリセットするための次の画面が表示されます。




- ユーザが弱いパスワードを設定しようとするか、最後のパスワードをもう一度入力すると、次のエラーが表示されます。



## 著作権に関する情報



## 商標に関する情報