VMware

Enterprise applications

NetApp
January 02, 2026

目次

VMware . . . 1
ONTAP を使用した VMware vSphere . . . 1
ONTAP を使用した VMware vSphere . . . 1
ONTAP for VMware vSphereを選ぶ理由 . . . 1
ユニファイドストレージ . . . 3
ONTAP の仮想化ツール . . . 4
Virtual Volumes （ VVol ）と Storage Policy Based Management （ SPBM ） . . . 7
データストアおよびプロトコル . . . 8
ネットワーク構成： . . . 23
VM とデータストアのクローニング . . . 25
データ保護 . . . 27
サービス品質（ QoS ） . . . 30
クラウドへの移行とバックアップ . . . 35
vSphere データの暗号化 . . . 36
Active IQ Unified Manager . . . 37
ストレージポリシーベースの管理とVVOL . . . 38
VMware Storage Distributed Resource Scheduler の略 . . . 41
推奨される ESXi ホストとその他の ONTAP 設定 . . . 42
ONTAP toolsを使用した仮想ボリューム（VVol）10 . . . 45
概要 . . . 45
チェックリスト . . . 51
ONTAP でVVOLを使用する . . . 54
AFF、ASA、ASA R2、FASシステムへのVVOLの導入 . . . 59
VVOLを保護する . . . 70
トラブルシューティング . . . 75
VMware Site Recovery ManagerとONTAP . . . 76
ONTAPを使用したVMwareライブサイトリカバリ . . . 76
導入のベストプラクティス . . . 78
運用上のベストプラクティス . . . 79
レプリケーショントポロジ . . . 83
vVolレプリケーション使用時のVLSRM / SRMのトラブルシューティング . . . 93
追加情報 . . . 94
ONTAPを使用したvSphere Metroストレージクラスタ . . . 94
ONTAPを使用したvSphere Metroストレージクラスタ . . . 94
VMware vSphere解決策の概要 . . . 97
vMSC設計および実装ガイドライン . . . 102
計画的イベントと計画外イベントの耐障害性 . . . 113
vMSCとMetroClusterの障害シナリオ . . . 113
製品のセキュリティ . . . 125

VMware vSphere 用の ONTAP ツール . . . 125
SnapCenterプラグインVMware vSphere . . . 127
ONTAP tools for VMware vSphere向けセキュリティ強化ガイド . . . 129
ONTAP tools for VMware vSphere 9.13向けセキュリティ強化ガイド . . . 129
ONTAP Tools for VMware vSphere 9.13インストールパッケージの整合性の検証 . . . 130
ONTAP tools 9.13のポートとプロトコル . . . 132
ONTAP Tools for VMware vSphere 9.13アクセスポイント（ユーザ） . . . 133
ONTAP tools 9.13相互TLS（証明書ベースの認証） . . . 134
ONTAP tools 9.13 HTTPS証明書 . . . 140
ONTAP tools 9.13のログインバナー . . . 140
ONTAP tools 9.13での非アクティブ時のタイムアウト . . . 141
ユーザー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）VMware vSphere 9.13向けONTAPツール . . . 141
ONTAP tools 9.13のネットワークタイムプロトコル（NTP）の設定 . . . 142
ONTAP tools 9.13のパスワードポリシー . . . 142

VMware

ONTAP を使用した VMware vSphere

ONTAP を使用した VMware vSphere

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および最近ではCloud Foundation環境向けの主要なストレージソリューションとして機能してきました。管理を簡易化し、コストを削減する革新的な機能を継続的に導入しています。

本ドキュメントでは、vSphere向けONTAPソリューションについて説明し、導入の合理化、リスクの軽減、管理の簡易化を実現する最新の製品情報とベストプラクティスを紹介します。

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。特定のリリースに関する詳細については、および "VMware Compatibility Guide"を参照してください "Interoperability Matrix Tool （ IMT ）"。

ONTAP for VMware vSphereを選ぶ理由

お客様は、SAN と NAS の両方のストレージ ソリューションとして、自信を持ってONTAP for vSphere を選択しています。最新の All SAN Arrays に搭載されている新しい簡素化された分散型ストレージ アーキテクチャは、従来のONTAPシステムの統合と機能セットのほとんどを維持しながら、SAN ストレージ管理者に馴染みのある簡素化されたエクスペリエンスを提供します。 ONTAPシステムは、優れたスナップショット保護と強力な管理ツールを提供します。 ONTAP は機能を専用ストレージにオフロードすることで、ホスト リソースを最大限に活用し、コストを削減し、最適なパフォーマンスを維持します。さらに、Storage vMotion を使用して、VMFS、NFS、またはvVols間でワークロードを簡単に移行できます。

ONTAP for vSphereを使用するメリット

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。

ONTAP をvSphere と併用すると、ホスト ハードウェアと VMware ソフトウェアの費用を削減できる優れた組み合わせになります。一貫した高い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であるため、Storage vMotion を使用して、同じストレージ システム上の VMFS、NFS、またはvVols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検討できます。

現在、顧客が重視する重要な要素は次のとおりです。

- 統合ストレージ ONTAP 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。もともとこのアプローチは NAS プロトコルと SAN プロトコルの両方を指しており、 ONTAP はNAS における本来の強みとともに、SAN の主要プラットフォームであり続けています。 vSphere の世界では、このアプローチは、仮想デスクトップ インフラストラクチャ (VDI) と仮想サーバー インフラストラクチャ (VSI) を統合したシステムを意味することもあります。 ONTAP を実行するシステムは、通常、従来のエンタープライズ アレイよりも VSI が安価でありながら、同じシステムで VDI を処理できる高度なストレージ効率機能を備えています。 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、クラウドに簡単に拡張できます。パフォーマンス用にストレージ オペレーティング システムを購入したり、アーカイブ用に別のストレージ オペレーティング システムを購入したり、クラウド用にさらに別のストレージ オペレーティング システムを購入したりする必要はありません。 ONTAP はこれらすべてを結び付けます。
- *オールSANアレイ（ASA）*最新のONTAP ASAシステム（A1K、A90、A70、A50、A30、A20以降）は、アグリゲートとボリュームの管理という従来のONTAPストレージのパラダイムを排除する新しいストレージアーキテクチャを基盤として構築されています。ファイルシステム共有がないため、ボリュームは必要ありません。HAペアに接続されたすべてのストレージは共通のStorage Availability Zone（SAZ；ストレージアベイラビリティゾーン）として扱われ、そのゾーン内でLUNおよびNVMeネームスペースが「Storage Unit」（SUS；ストレージユニット）としてプロビジョニングされます。最新のASAシステムは管理が容易になるように設計されており、SANストレージ管理者は使い慣れた環境を利用できます。この新しいアーキテクチャは、ストレージリソースの管理を容易にし、SANストレージ管理者の操作を簡易化できるため、vSphere環境に最適です。ASAアーキテクチャは最新のNVMe over Fabrics（NVMe-oF）テクノロジもサポートしているため、vSphereワークロードのパフォーマンスと拡張性がさらに向上します。
- * Snapshotテクノロジ。*ONTAPは、データ保護のためのスナップショットテクノロジを業界で初めて提供し、現在も業界で最も先進的なテクノロジです。スペース効率に優れたこのデータ保護アプローチは、VMware vSphere APIs for Array Integration（VAAI）をサポートするために拡張されました。この統合により、ONTAPのスナップショット機能をバックアップおよびリストア操作に活用し、本番環境への影響を軽減できます。このアプローチでは、スナップショットを使用してVMを迅速にリカバリできるため、データのリストアに必要な時間と労力が軽減されます。さらに、ONTAPのスナップショットテクノロジは、VMwareのライブサイトリカバリ（VLSR、旧Site Recovery Manager [SRM]）ソリューションと統合されており、仮想化環境に包括的なデータ保護戦略を提供します。
- 仮想ボリュームとストレージのポリシーベースの管理。 NetApp は、vSphere Virtual Volumes (vVols) の開発において VMware の初期の設計パートナーであり、 vVolsと VMware vSphere APIs for Storage Awareness (VASA) に対するアーキテクチャ上のインプットと初期サポートを提供しました。このアプローチにより、VMFS にきめ細かな VM ストレージ管理がもたらされただけでなく、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 管理者が簡単に使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 スケールにおいてストレージ業界をリードしており、単一のクラスタで数十万のvVols をサポートしています。一方、エンタープライズ アレイや小規模フラッシュ アレイ ベンダーは、アレイあたりわずか数千のvVolsしかサポートしていません。 NetAppは、今後の機能により、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 は実稼働ワークロードの重複排除を初めて実現しましたが、このイノベーションはこの分野における最初でも最後でもありません。それは、パフォーマンスに影響を与えないスペース効率の高いデータ保護メカニズムであるスナップショットと、実稼働およびバックアップ用に VM の読み取り/書き込みコピーを即座に作成するFlexCloneテクノロジーから始まりました。 NetApp 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 から最大限のストレージ

容量を絞り出しました。 ONTAP、圧縮を使用して、より小さな I/O 操作とファイルをディスク ブロックにパックする機能も追加されました。これらの機能の組み合わせにより、お客様は一般的に VSI で最大 5:1、VDI で最大 30:1 の節約を実現しています。最新世代のONTAPシステムには、ハードウェア アクセラレーションによる圧縮と重複排除も含まれており、これによりストレージ効率がさらに向上し、コストが削減されます。このアプローチにより、より少ないスペースに多くのデータを保存できるため、全体的なストレージコストが削減され、パフォーマンスが向上します。 NetAppはストレージ効率機能に非常に自信を持っているため、リンクを提供しています:https://www.netapp.com/pdf.html?item=/media/79014-ng-937-Efficiency-Guarantee-Customer-Flyer.pdf [効率保証^]。

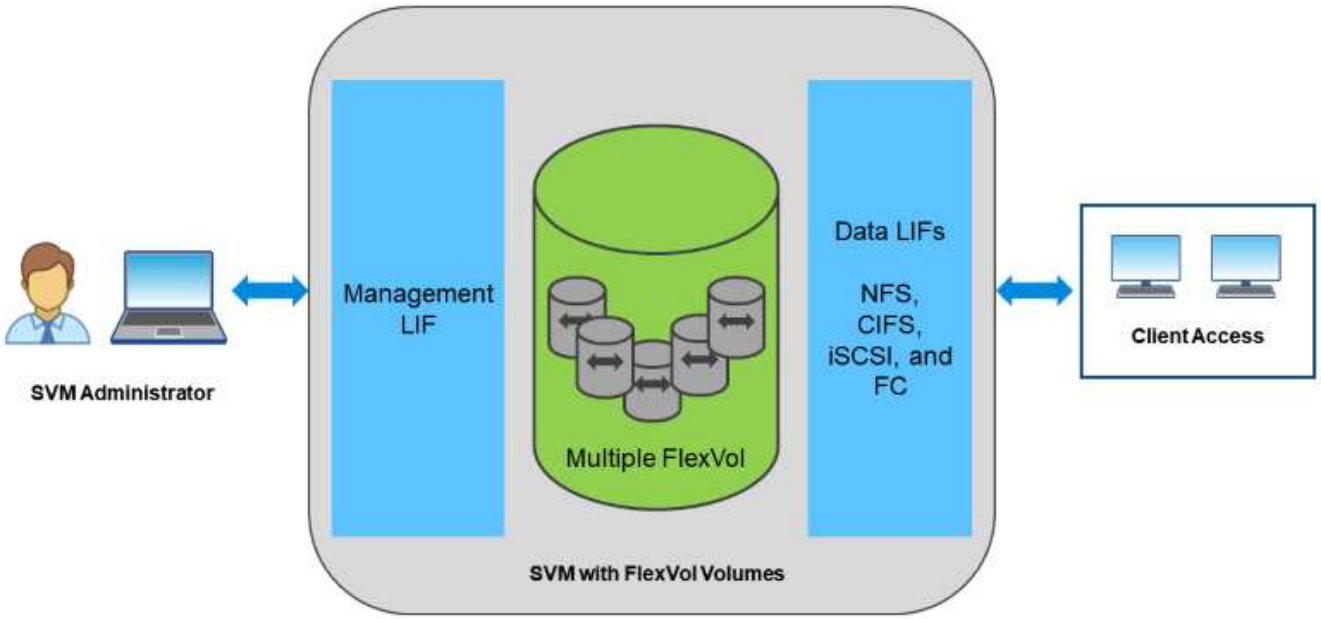
- マルチテナント ONTAP は長年マルチテナンシーのリーダーであり、単一のクラスタ上に複数のストレージ仮想マシン (SVM) を作成できます。このアプローチにより、ワークロードを分離し、テナントごとに異なるレベルのサービスを提供できるため、サービス プロバイダーや大企業に最適です。最新世代のONTAPシステムには、テナント容量管理のサポートも含まれています。この機能を使用すると、各テナントに容量制限を設定できるため、単一のテナントが利用可能なリソースをすべて消費することがなくなります。このアプローチにより、すべてのテナントが期待するレベルのサービスを確実に受けられるようになると同時に、テナント間の高度なセキュリティと分離も実現できます。さらに、ONTAPのマルチテナント機能はVMwareのvSphereプラットフォームと統合されており、仮想化環境を簡単に管理および監視できます。 "VMware vSphere 用の ONTAP ツール"そして "データインフラの分析情報"。
- *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、またはその両方の長所を組み合わせたハイブリッド クラウドのいずれに使用する場合でも、ONTAPソリューションはデータ ファブリックを構築してデータ管理を合理化し、最適化するのに役立ちます。高性能オールフラッシュ システムから始めて、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 システムまたはクラウド ストレージ システムと組み合わせます。 Azure、AWS、IBM 、Google Cloud からお選びいただくことで、コストを最適化し、ベンダー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ーの高度なサポートを活用できます。 NetApp は、運用コストを削減し、クラウドの広範な範囲を活用できるように、 ONTAP向けのクラウドベースのバックアップ (SnapMirror Cloud、 Cloud Backup Service、 Cloud Sync) とストレージ階層化およびアーカイブ ツール (FabricPool) も提供しています。
- * 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

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"S3構成の概要"ください。ユニファイドストレージという用語は、すべてのストレージリソースを単一のインターフェイスから管理する機能など、ストレージ管理に対するユニファイドアプローチを意味するように進化しました。これには、オンプレミスとクラウドの両方のストレージリソース、最新のオールSANアレイ（ASA）システム、複数のストレージシステムを単一のインターフェイスから管理する機能が含まれます。

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を実行す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を実行するシステムは、従来のエンタープライズアレイよりもVSIの方が一般的に安価であり、VDIを処理するための高度なStorage Efficiency機能を同じシステム内で備えています。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

NetAppには、従来のONTAPシステムとASAシステムの両方と互換性のあるスタンドアロンのソフトウェアツールがいくつか用意されており、vSphereを統合して仮想環境を効果的に管理できます。

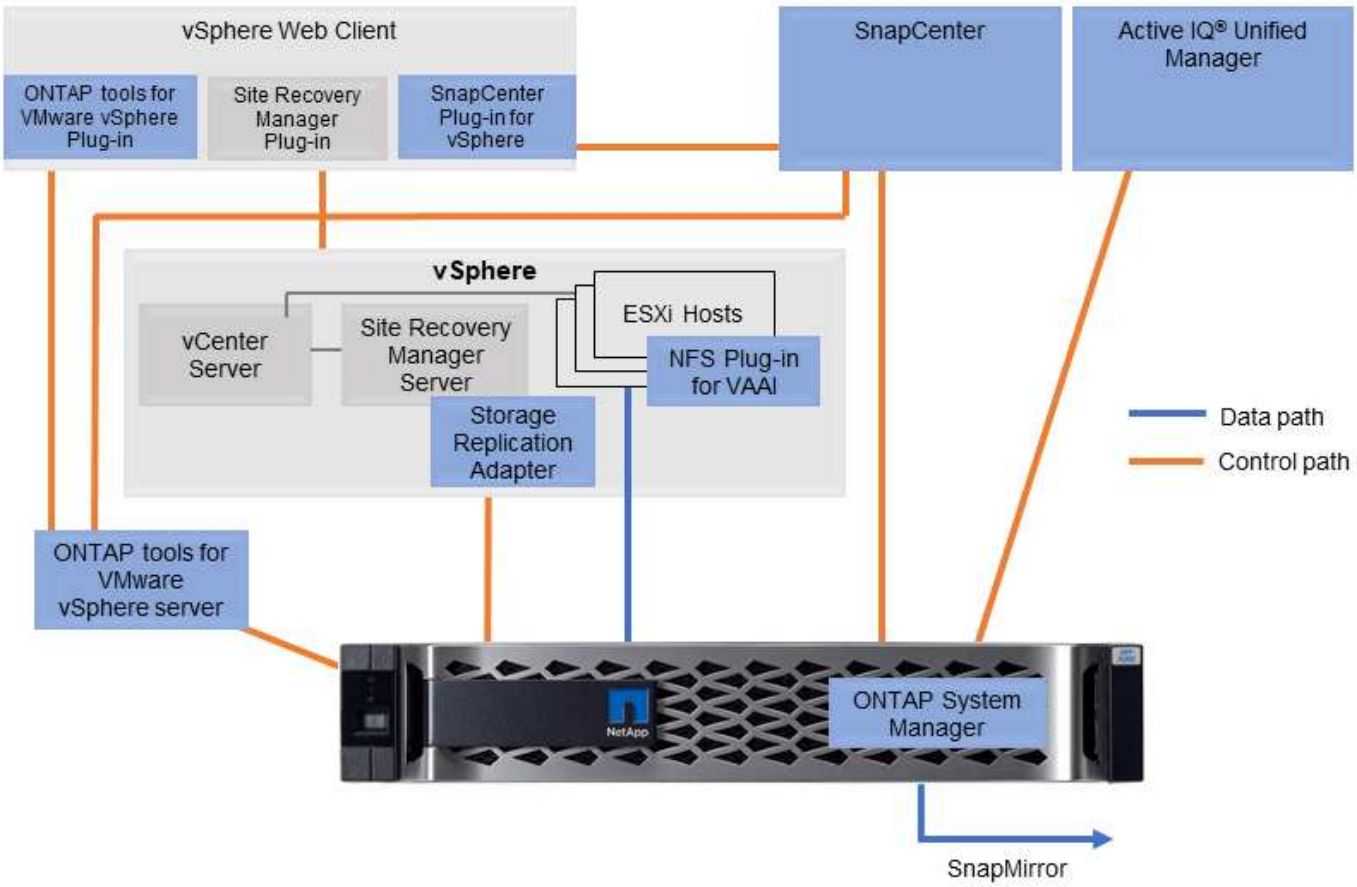
次のツールは、ONTAP Oneライセンスに含まれています。追加料金はかかりません。vSphere 環境でこれらのツールがどのように連携するかについては、図 1 を参照してください。

VMware vSphere 用の **ONTAP** ツール

"VMware vSphere 用の ONTAP ツール"は、ONTAPストレージとvSphereを併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。これらすべてのメリットについて、NetAppでは、ONTAP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ツールの使用を推奨しています。サーバアプライアンス、vCenter、VASA Provider 、Storage Replication Adapter向けのUI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拡張機能*ONTAP toolsのUI拡張機能は、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メニュー、情報ポートレット、および標準のアラート機能をvCenter UIに直接組み込むことで、運用チームやvCenter管理者の作業を簡易化し、ワークフローを合理化します。
- * 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。
- *ストレージ レプリケーション アダプタ*SRA は、VMware Live Site Recovery (VLSR)/Site Recovery Manager (SRM) と併用され、アレイベースのレプリケーションにSnapMirror を使用して、運用サイトと災害復旧サイト間のデータ レプリケーションを管理します。災害発生時のフェイルオーバー タスクを自動化し、DR レプリカを中断なくテストして DR ソリューションの信頼性を確保することができます。

次の図は、 vSphere 用の ONTAP ツールを示しています。



VMware vSphere向けSnapCenterプラグイン

その "VMware vSphere向けSnapCenterプラグイン" は、仮想マシン (VM) とデータストアのバックアップと復元を管理できる vCenter Server のプラグインです。複数のONTAPシステムにわたる VM およびデータストアのバックアップ、リストア、クローンを管理するための単一のインターフェイスを提供します。SnapCenterは、 SnapMirrorを使用してセカンダリ サイトへのレプリケーションとセカンダリ サイトからのリカバリをサポートします。最新バージョンでは、クラウド (S3) へのSnapMirror 、改ざん防止スナップショット、SnapLock、 SnapMirrorアクティブ同期もサポートされています。VMware vSphere 用のSnapCenterプラグインは、 SnapCenterアプリケーション プラグインと統合して、アプリケーション整合性のあるバックアップを提供できます。

NFS Plug-in for VMware VAAI のこと

は、 "NetApp NFS Plug-in for VMware VAAI"ESXiホストがONTAP上のNFSデータストアでVAAI機能を使用できるようにするプラグインです。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。

Premiumソフトウェアオプション

NetAppからは、次のプレミアム ソフトウェア製品が提供されています。これらはONTAP One ライセンスには含まれていないため、別途購入する必要があります。

- "NetApp Disaster Recovery(DR)"VMware vSphere 用。これは、VMware 環境の災害復旧とバックアップを提供するクラウドベースのサービスです。SnapCenterの有無にかかわらず使用でき、SAN または NAS を使用したオンプレミス間の DR、および NFS を使用したオンプレミスとクラウド間の DR (サポートされている場合) をサポートします。
- "Data Infrastructure Insights（DII）"。これは、VMware 環境の監視と分析を提供するクラウドベースのサービスです。異機種ストレージ環境における他のストレージ ベンダー、複数のスイッチ ベンダー、およびその他のハイパーバイザーをサポートします。DII は、VMware 環境のパフォーマンス、容量、健全性に関する完全なエンドツーエンドの分析情報を提供します。

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

2012年に最初に発表されたNetAppは、VMware vSphere APIs for Storage Awareness（VASA）の開発におけるVMwareの初期の設計パートナーであり、エンタープライズストレージアレイを使用するストレージポリシーベース管理（SPBM）の基盤となっています。このアプローチにより、VMFSおよびNFSストレージでVMのきめ細かなストレージ管理が制限されました。

テクノロジ設計パートナーとして、NetAppはアーキテクチャに関する情報を提供し、2015年にVVOLのサポートを発表しました。この新しいテクノロジにより、SPBMを使用してVM単位で真にアレイネイティブなストレージプロビジョニングを自動化できるようになりました。

仮想ボリューム（**VVol**）

VVOLは、VMのきめ細かなストレージ管理を可能にする革新的なストレージアーキテクチャです。ストレージは、VM単位（VMメタデータを含む）だけでなく、VMDK単位でも管理できます。VVOLは、VMware Cloud Foundation（VCF）の基盤となるSoftware-Defined Data Center（SDDC）戦略の重要なコンポーネントであり、仮想環境向けのより効率的で拡張性に優れたストレージアーキテクチャを提供します。

VVOLを使用すると、各VMストレージオブジェクトはNetApp ONTAP内で一意のエンティティであるため、VMはVM単位でストレージを消費できます。ボリューム管理が不要になったASA R2システムでは、各VMストレージオブジェクトがアレイ上の一意のストレージユニット（SU）であり、個別に制御できます。これにより、個 々 のVMまたはVMDK（つまり個別のSUS）に適用できるストレージポリシーを作成して、パフォーマンス、可用性、データ保護などのストレージサービスをきめ細かく制御できます。

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

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。これらのプールは、VM管理者が簡単に使用できます。管理者は、プロビジョニングされたストレージプールと仮想マシンのワークロード要件を照合できます。このアプローチにより、ストレージ管理が簡易化され、ストレージリソースの使用効率が向上します。

SPBMはVVOLの主要コンポーネントであり、ストレージサービスを管理するためのポリシーベースのフレームワークを提供します。ポリシーは、vSphere管理者が、ベンダーのVASA Provider（VP）が公開するルールと機能を使用して作成します。パフォーマンス、可用性、データ保護など、さまざまなストレージサービスに対してポリシーを作成できます。ポリシーは個 々 のVMまたはVMDKに割り当てることができるため、ストレージサービスをきめ細かく制御できます。

NetApp ONTAPとVVOL

NetApp ONTAPはVVOLの規模でストレージ業界をリードしており、1つのクラスタ*で数十万のVVOLをサポートしています。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では、アレイあたり数千のVVolしかサポートしていません。ONTAPは、VMware vSphere環境向けの拡張性と効率性に優れたストレージソリューションを提供します。データ重複排除、圧縮、シンプロビジョニング、データ保護などの豊富なストレージサービスでVVOLをサポートします。SPBMを使用すると、VMware vSphere環境とのシームレスな統合が可能になります。

前述したように、VM管理者は容量をストレージプールとして利用できるということです。これには、vSphereで論理データストアとして表されるストレージコンテナを使用します。

ストレージコンテナは、ストレージ管理者が作成し、VM管理者が使用できるストレージリソースをグループ化するために使用されます。ストレージコンテナは、使用しているONTAPシステムのタイプに応じて作成できます。従来のONTAP 9クラスタでは、コンテナに1つ以上の元のFlexVolボリュームが割り当てられ、ストレージプールを形成します。ASA R2システムでは、クラスタ全体がストレージプールになります。

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 』"。

*プラットフォームとプロトコルによって異なる

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をONTAPを実行するシステム上のデータストアに接続するには、次の6つのプロトコルを使用します。

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

FCP、NVMe/FC、NVMe/TCP、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 volume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。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。特定のvSphereリリースのを参照して、固有の制限を確認することもできます"VMware Configuration Maximumsツール"。

機能 / 特徴	FC	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	N/A
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	ホストあたり256のNFS接続（nconnectとセッショントランキングの影響を受ける）、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	300TB 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	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。
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。

容量 / 機能	FC	iSCSI	NVMe-oF	NFS
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[1]	はい[1]	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。
ライブサイトリカバリ/サイトリカバリマネージャ	はい。	はい。	いいえ[2]	v3のみ[2]
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。 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。	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	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。	はい。	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。	はい。	はい。
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。	はい。	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	iSCSI	NVMe-oF	NFS
ONTAPノSnapshot	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[2]	v3のみ[2]
Volume SnapMirrorの略	はい。	はい。	はい。	はい。
VMDK イメージアクセス	SnapCenterおよびVADP対応のバックアップソフトウェア	SnapCenterおよびVADP対応のバックアップソフトウェア	SnapCenterおよびVADP対応のバックアップソフトウェア	SnapCenterおよび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	SnapCenterおよびVADP対応のバックアップソフトウェア、Windowsのみ	SnapCenterおよびVADP対応のバックアップソフトウェア、Windowsのみ	SnapCenterおよびVADP対応のバックアップソフトウェア、Windowsのみ	SnapCenterおよび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

[1]* NetAppでは、マルチライター対応のVMDKをVMFSデータストアで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ています*。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）で優れた柔軟性を提供し、設定と自動化が簡単で、SnapCenterで保護できます。vSphere 7には、新しいclustered VMDKオプションが追加されています。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では、クラスタ化されたVMDKのサポートが有効になっているVMFS 6データストアが必要です。その他の制限が適用されます。構成のガイドラインについては、VMwareのドキュメントを参照してください"Windows Server フェールオーバークラスタリングのセットアップ"。

[2]NVMe-oFおよびNFS v4.1を使用するデータストアでは、vSphereレプリケーションが必要です。NFS v4.1のアレイベースのレプリケーションは、現在SRMでサポートされていません。NVMe-oFを使用したアレイベースのレプリケーションは、現在ONTAP tools for VMware vSphere Storage Replication Adapter（SRA）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を実行するシステムは、主要なすべてのストレージプロトコルをサポートしているため、既存および計画中のネットワークインフラと担当者のスキルに応じて、お客様の環境に最適なものを選択できます。歴史的に、NetAppテストでは、ほぼ同じ回線速度と接続数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。ただし、NVMe-oF（NVMe/TCPおよびNVMe/FC）は、IOPSの大幅な向上とレイテンシの低減を実現し、ストレージIOによるホストCPU消費量を最大50%以上削減します。一方、NFSは、特に多数のVMに対して、柔軟性と管理のしやすさを最大限に高めます。これらのプロトコルはすべて、データストアを作成および管理するためのシンプルなインターフェイスを提供するONTAP Tools for VMware vSphereで使用および管理できます。

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。

- *現在の動作環境*一般に、ITチームはイーサネットIPインフラの管理に精通していますが、FC SANファブ

リックの管理に精通し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プロトコルでスペースを増やす必要がある場合は、LUNの拡張、再スキャンによる新しいサイズの検出、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のサイズの縮小は可能ではありません。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deallocate /trim/unmapコマンドを使用してスペース再生を実行し、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。このようなスペース再生は、NFSデータストアでは難しくありません。
- * 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。ONTAPツールを使用してvSphere（の項を参照"推奨される ESXi ホストとその他の ONTAP 設定"）にデータストアをプロビジョニングする場合は、多くのONTAPのベストプラクティスが適用されますが、次のガイドラインも考慮する必要があります。

- 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、運用上のメリットも得られますが、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には、ノードごとに少なくとも4つのデータストア（FlexVolボリューム）を使用してVMを1台のONTAPコントローラに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。
- 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 300TB 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。ONTAP tools for VMware vSphereデータストアプロビジョニングウィザードでは、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、VMFSデータストアには、FC、iSCSI、NVMe/FC、NVMe/TCPからアクセスするLUNまたはNVMe

ネームスペース（新しいASAシステムではストレージユニットと呼ばれます）を設定することもできます。VMFSを使用すると、クラスタ内のすべてのESXサーバから同時にデータストアにアクセスできます。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、AFF、ASA、およびFASシステムで128TBです。NetAppでは、エクステントを使用するのではなく、データストアごとに大容量のLUNを1つ使用することを常に推奨しています。NFSの場合と同様に、複数のデータストア（ボリュームまたはストレージユニット）を使用して、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、NetAppサポートナレッジベースで「VMアライメント」と記載された記事を検索するか、NetAppの営業担当者またはパートナー担当者にTR-3747のコピーをリクエストしてください。
- 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。ゲストが所有するファイルシステム（ゲストが管理するNFS、SMB、NVMe/TCP、iSCSIのファイルシステムなど）を検討します。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。たとえば、に"ONTAP を基盤にした Oracle データベース"は仮想化に関するセクションがあり、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。さらに、VMがNetAppクラスタに配置されると、Storage vMotionでVAAIのオフロードを使用してクラスタ上のデータストア間でVMを移動できます。ホストベースのコピーは必要ありません。NFSでは、電源がオンになっているVMのStorage vMotionはオフロードされませんが、VMFSではオフロードされます。
- 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。詳細については、を参照してください "ONTAPストレージシステムへのOracleデータベースの移行" 。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、ONTAP Tools for VMware vSphereプラグイン（旧Virtual Storage Console）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またはNAS、ONTAP Select、AFF、FAS、さらにはASA（VMwareまたはKVM VMで実行されるソフトウェア定義バージョンのONTAP）のいずれの環境でも、ストレージ管理を簡易化し、可用性を高め、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。

> イメージベースのvSphereクラスタでは、ONTAPツールを使用してインストールする際にコンプライアンス違反にならないように、NFS Plug-inをイメージに追加する必要があります。

ONTAPツールは、VASA Provider for ONTAPの多くの機能の管理インターフェイスでもあり、VVOLを使用したポリシーベースのストレージ管理をサポートします。

一般に、* NetAppでは* vCenter内でONTAP Tools for VMware vSphereインターフェイス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うことを推奨*しています。

一般的なネットワーク

ONTAPを実行するシステムで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。
- NetAppでは、ONTAPクラスタ内のクラスタインターコネクトポートでのみネットワークフロー制御を無効にすることを推奨しています。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。フロー制御の詳細については、を参照してください "TR-4182"。

- 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場合は、NetApp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）エッジポートとして設定するか、Cisco PortFast機能を使用して設定することを推奨します。* NetAppでは、Cisco PortFast機能を使用し、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、スパニングツリーPortFastトランク機能を有効にすることを推奨*しています。
- * NetAppでは*リンクアグリゲーションに次のベストプラクティスを推奨しています。
  - 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。

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

vSphereでは、次の4つの方法でブロックストレージデバイスを使用できます。

- 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
- VMゲストOSのソフトウェアイニシエータによってアクセスおよび制御される、iSCSI接続のLUNまたはNVMe/TCP接続のネームスペース
- vVolデータストアとして使用

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。

エクステントとは、複数のLUNを「ステッチ」して1つの大容量データストアを作成できるvSphereストレージの概念です。エクステントを使用してデータストアの目的のサイズに到達しないでください。VMFSデータストアのベストプラクティスは、単一のLUNです。

vSphereには、ストレージデバイスへの複数のパスのサポートが組み込まれています。vSphereは、サポートされているストレージシステムのストレージデバイスのタイプを検出し、使用されているプロトコルに関係なく、またはASA、AFF、FAS、またはSoftware Defined ONTAPを使用している場合は、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マルチパススタックを自動的に構成します。

vSphere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）をサポートしてファイバチャネルとiSCSI用のアクティブ/最適パスとアクティブ/非最適パスを確立し、NVMe/FC

とNVMe/TCPを使用するNVMeネームスペース用のAsymmetric Namespace Access（ANA）をサポートしています。ONTAPでは、アクセスするLUNまたはネームスペース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またはANA最適パスになります。ALUA / ANAは、vSphereとONTAPの両方でデフォルトで有効になっています。vSphereのマルチパスソフトウェアは、ONTAPクラスタをALUAまたはANAとして認識し、ラウンドロビンの負荷分散ポリシーが設定された適切なネイティブプラグインを使用します。

NetAppのASAシステムでは、LUNとネームスペースは対称パスを使用してESXiホストに提供されます。つまり、すべてのパスがアクティブで最適化されています。vSphereのマルチパスソフトウェアはASAシステムを対称と認識し、適切なネイティブプラグインとラウンドロビンによる負荷分散ポリシーを使用します。

最適化されたマルチパス設定については、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"。

ESXiで、制限を超えたLUN、ネームスペース、パスは認識されません。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。

ESXiでサポートされる最新の制限については、を参照して"VMware Configuration Maximumsツール"ください。

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。NetAppのベストプラクティスでは、SVMごとにノードごとに少なくとも2つのLIFを配置し、アドバタイズされるパスをSLMを使用してLUNをホストするノードとそのHAパートナーに制限することを推奨します。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、コマンドを実行して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ことで、SLMを手動で適用し `lun mapping remove-reporting-nodes`ます。

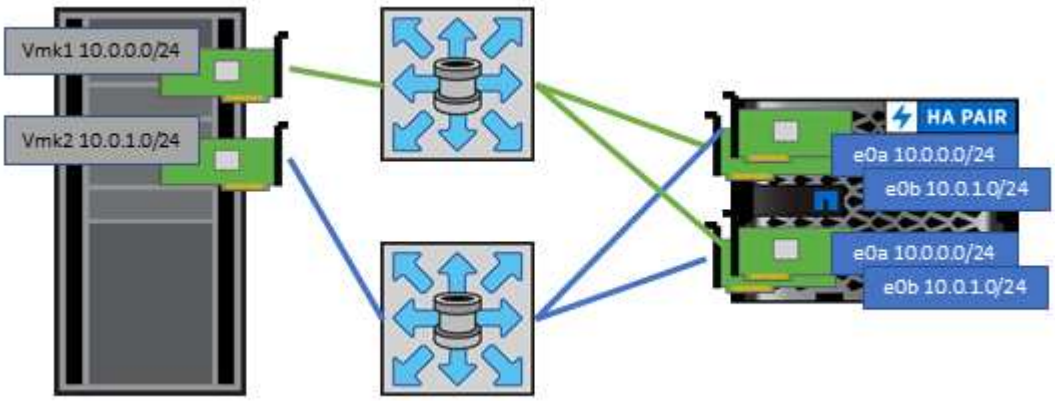
SCSIベースのブロックプロトコル（iSCSI、FC、FCoE）は、LUN IDとシリアル番号、および一意の名前を使用してLUNにアクセスします。FCとFCoEはWorldwide Name（WWNNとWWPN）を使用し、iSCSIはiSCSI Qualified Name（IQN）を使用して、ポートセットとSLMでフィルタリングされたLUNとigroupのマッピングに基づいてパスを確立します。NVMeベースのブロックプロトコルは、自動生成されたネームスペースIDを持つネームスペースをNVMeサブシステムに割り当て、そのサブシステムをホストのNVMe Qualified Name（NQN）にマッピングすることで管理されます。FCとTCPに関係なく、NVMeネームスペースはWWPNまたはWWNNではなくNQNを使用してマッピングされます。次に、ホストは、マッピングされたサブシステム用のSoftware-Definedコントローラを作成して、そのネームスペースにアクセスします。ONTAP内のLUNおよびネームスペースへのパスは、ブロックプロトコルでは意味がなく、プロトコルの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。

考慮すべきその他のベストプラクティス：

- VMwareと連携してNetAppが推奨する設定を確認します"推奨される ESXi ホストとその他の ONTAP 設

定"。

- 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

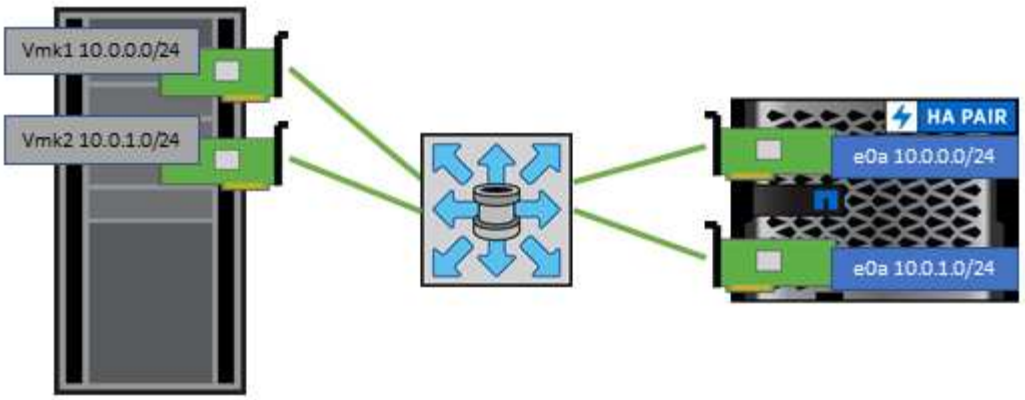
ONTAPは、とりわけエンタープライズクラスのスケールアウトNASアレイです。ONTAPは、VMware vSphereを強化し、多数のESXiホストからNFS接続データストアに同時にアクセスできるようにします。VMFSファイルシステムの制限をはるかに超えています。vSphereでNFSを使用すると、操作が容易になり、ストレージ効率を可視化できるというメリットがあります（を参照"データストア"）。

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。

- 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：
  - ONTAP tools for VMware vSphereを使用して、エクスポートポリシーの自動管理が簡易化されるため、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 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。
- fpolicyを使用する場合は、必ず.lckファイルを除外してください。これらのファイルは、VMの電源がオンになっているときにvSphereでロックするために使用されます。
- 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ではvSphere 8.0 Update 2、NFS v4.1ではUpdate 3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、を参照"NetAppおよびVMwareでのNFSv3 nconnect機能"してください。

  - vSphere 8のnconnectの最大値は4で、デフォルト値は1です。vSphereの最大値は、高度な設定を使用してホスト単位で上げることができますが、通常は必要ありません。
  - 1つのTCP接続で提供できるパフォーマンスよりも高いパフォーマンスを必要とする環境では、値を4にすることを推奨します。
  - ESXiのNFS接続数は256に制限されており、各nconnect接続数がその合計にカウントされることに注意してください。たとえば、nconnect=4の2つのデータストアは、合計8つの接続としてカウントされます。
  - 本番環境に大規模な変更を実装する前に、nconnectが環境に与えるパフォーマンスへの影響をテストすることが重要です。
- 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。
  - 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。
  - サポートに必要なESXiのパッチレベルについては、でNFS v4.1のInteroperabilityテーブルに関する注意事項を参照して"NetApp Interoperability Matrix Tool で確認できます"ください。
- で説明したように、"設定"vSphere CSI for Kubernetesを使用していない場合は、 "VMware KB 386364"

- NFSエクスポートポリシールールは、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。NFSの場合、ESXiではsys（UNIX）セキュリティ形式が使用され、VMを実行するにはルートマウントオプションが必要です。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。との `-allow-suid`値が異なるエクスポートポリシールールが設定されていると、ONTAP toolsでSVM検出の問題が発生する可能性があることに注意して `-anon`ください。IPアドレスをカンマで区切って指定し、データストアをマウントするvmkernelポートアドレスをスペースなしで指定する必要があります。ポリシールールの例を次に示します。
  - Access Protocol：nfs（nfs3とnfs4の両方を含む）
  - クライアント一致のホスト名、IPアドレス、ネットグループ、またはドメインのリスト：192.168.42.21,192.168.42.22
  - ROアクセスルール：任意
  - RWアクセスルール：任意
  - 匿名ユーザのマッピング先ユーザID：65534
  - スーパーユーザセキュリティタイプ：任意
  - SETATTRでsetuidビットを保持：TRUE
  - デバイスの作成を許可：true
- NetApp NFS Plug-in for VMware VAAIを使用する場合は、エクスポートポリシーを作成または変更するときにプロトコルをに設定する必要があります `nfs`。VAAIコピーオフロードが機能するためにはNFSv4プロトコルが必要です。プロトコルをに指定する `nfs`と、NFSv3とNFSv4の両方のバージョンが自動的に選択されます。これは、データストアタイプがNFS v3として作成されている場合でも必要です。
- 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。
  - アクセスプロトコル：NFS
  - クライアント一致の仕様：192.168.42.21、192.168.42.22
  - 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）
- 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	○（ONTAP 9.14.1）

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 9.8-9.13、およびSnapCenterプラグインfor VMware 4.4以降のリリースでは、vSphereでFlexGroupボリュームベースのデータストアがサポートされるようになりました。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。

完全なONTAPクラスタ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、クローンキャッシュを常にウォームアップすることでFlexGroupクローニングメカニズムのメリットが得られる非常に

大規模なクローニングワークロードがある場合は、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。このコンスティチュエント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ボリュームを設定する方法"

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ボリューム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、そのホストの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 Tool（IMT）に関する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、を参照して"NetAppおよびVMwareでのNFSv3 nconnect機能"ください。
- 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ボリュームとFlexGroupボリューム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 9.8-9.13を使用して、ONTAP指標（ダッシュボードおよび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を実行するシステムで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。ソリューションガイドで明確に指示されている場合を除き、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が介入なしで動作できるようにします。
- ネットワークでサポートされている場合は、ジャンボフレームを使用してください。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。
- NetAppでは、ONTAPクラスタ内のクラスタインターコネクトポートでのみネットワークフロー制御を無効にすることを推奨しています。NetAppでは、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のフロー制御に関するベストプラクティスについて、これ以外の推奨事項はありません。必要に応じて有効または無効にする必要があります。フロー制御の詳細については、を参照してください "TR-4182"。
- 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、NVMe/FC、iSCSI、NVMe/TCP）、RDM

ONTAPは、従来のiSCSIとファイバチャネルプロトコル（FCP）を使用してVMware vSphere向け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。また、効率性とパフォーマンスに優れた次世代ブロックプロトコルであるNVMe over Fabrics（NVMe-oF）を使用し、NVMe/FCとNVMe/TCPの両方をサポートしています。

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詳細なベストプラクティスについては、"データストアとプロトコル- SAN"

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。セクションで説明したように、"データストア "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いくつかあります。

推奨されるベストプラクティスについては、を参照してください。"データストアとプロトコル- NFS"

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。ただし、いくつかの制限事項と注意事項があります。

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はフリーズする必要があります。

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。

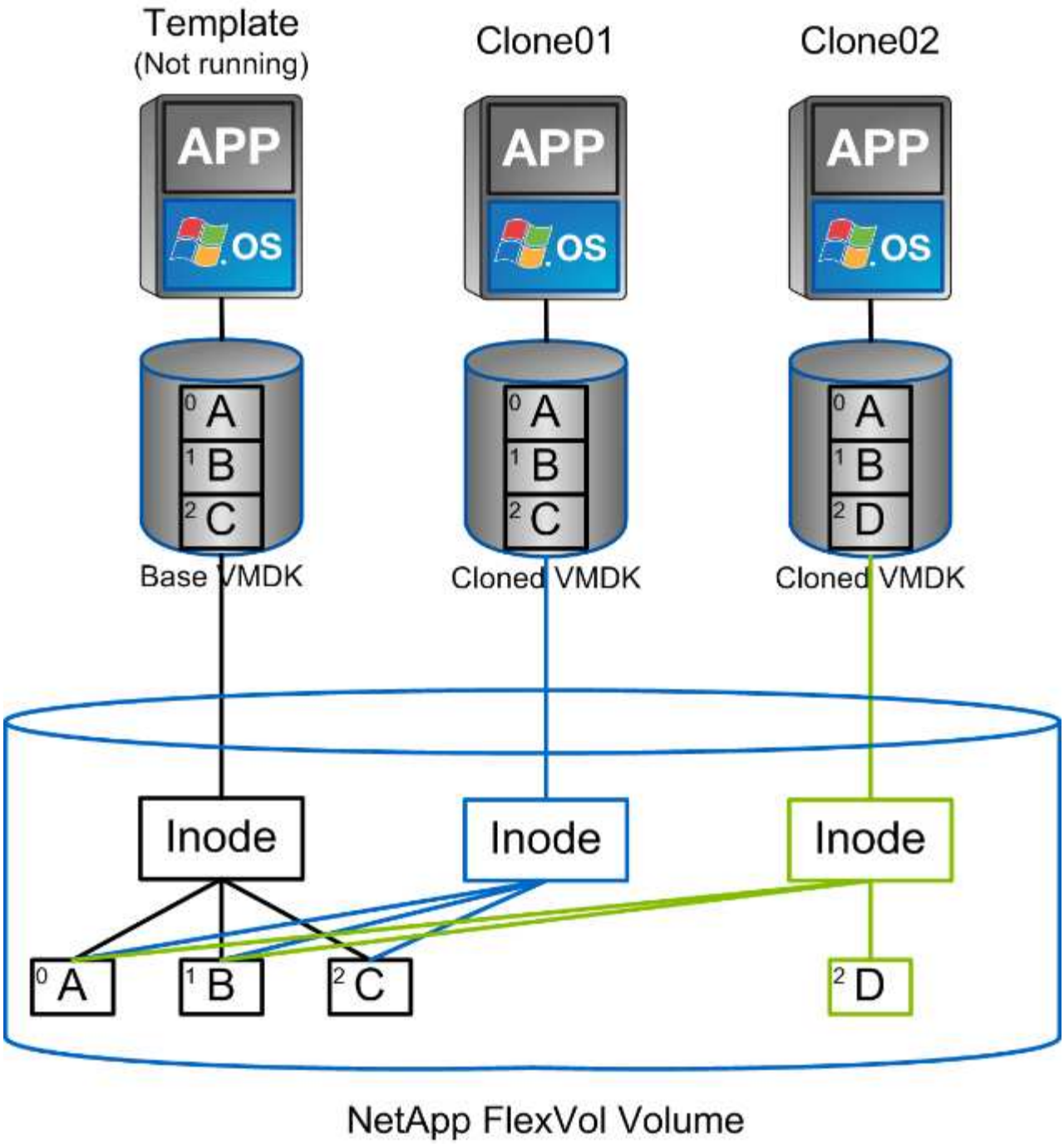
VM とデータストアのクローニング

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を実行するシステムにいくつか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できます。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：VMのクローニング処理は、SAN環境とNAS環境の両方でONTAPにオフロードできます（NetAppには、VAAI for NFSを有効にするESXiプラグインが用意されています）。vSphereはNASデータストア内のコールド（電源がオフになっている）VMに対する処理のみをオフロードしますが、ホットVMに対する処理（クローニング

とStorage vMotion）はSANに対してもオフロードされます。ONTAPでは、ソースとデスティネーションに基づいた最も効率的なアプローチを採用しています。この機能は、でも使用され "オムニッサホライゾンビュー""ます。

- SRA（VMware Live Site Recovery / 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、個 々 のファイルをリストアできるようにVMバックアップのマウントに使用されます。

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 volumeを使用した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（ONTAP Oneライセンスに含まれる）で高速かつ効率的に実行できますが、FlexVolボリューム間のコピーには時間がかかることがあります。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

ONTAP for vSphereを使用する主なメリットは、仮想マシン（VM）のバックアップと迅速なリカバリです。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。多くのお客様は、SnapCenterを使用してサードパーティ製バックアップソリューションを強化し、ONTAPのスナップショットテクノロジを活用しています。これは、ONTAPを使用してVMを迅速かつ簡単にリカバリできるためです。ONTAP Oneライセンスをお持ちのお客様は、SnapCenterを無料でご利用いただけます。その他のライセンスバンドルもご利用いただけます。

さらに、VMware向けSnapCenterプラグインは、 "仮想マシン向けNetApp Backup and Recovery"ほとんどのONTAPシステムで効果的な 3-2-1 バックアップ ソリューションを実現します。追加のバックアップ ストレージ用のオブジェクト ストアなどのプレミアム サービスを備えた仮想マシンのバックアップとリカバリを使

用する場合は、料金が適用される場合があることに注意してください。このセクションでは、VM とデータストアを保護するために使用できるさまざまなオプションについて説明します。

NetApp ONTAPホリユウムノSnapshot

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。

SnapshotはONTAPの重要な機能であり、データのポイントインタイムコピーを作成できます。スペース効率に優れ、短時間で作成できるため、VMやデータストアの保護に最適です。スナップショットは、バックアップ、リカバリ、テストなど、さまざまな目的に使用できます。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のvCenterで管理されるスナップショットは、パフォーマンスやその他の影響のため、短期的な使用にのみ推奨されます。"Snapshotの制限事項" 詳細については、を参照してください。

Snapshotはボリュームレベルで作成され、そのボリューム内のすべてのVMとデータストアを保護するために使用できます。つまり、データストア内のすべてのVMを含むデータストア全体のスナップショットを作成できます。

NFSデータストアの場合は、.snapshotsディレクトリを参照することで、Snapshot内のVMファイルを簡単に表示できます。これにより、特定のバックアップソリューションを使用することなく、スナップショットからファイルにすばやくアクセスしてリストアできます。

VMFSデータストアの場合は、必要なSnapshotに基づいてデータストアのFlexCloneを作成できます。これにより、Snapshotに基づく新しいデータストアを作成し、テストや開発に使用できます。FlexCloneは、Snapshotの作成後に行われた変更に対してのみスペースを消費するため、スペース効率に優れた方法でデータストアのコピーを作成できます。FlexCloneを作成したら、通常のデータストアと同様に、LUNまたはネームスペースをESXiホストにマッピングできます。これにより、特定のVMファイルをリストアできるだけでなく、本番環境のパフォーマンスに影響を与えることなく、本番データに基づいてテスト環境や開発環境を迅速に作成できます。

スナップショットの詳細については、 ONTAP のドキュメントを参照してください。詳細については、次のリンクをご覧ください。 "ONTAPローカルSnapshotコピー" "ONTAP SnapMirrorレプリケーションワークフロー"

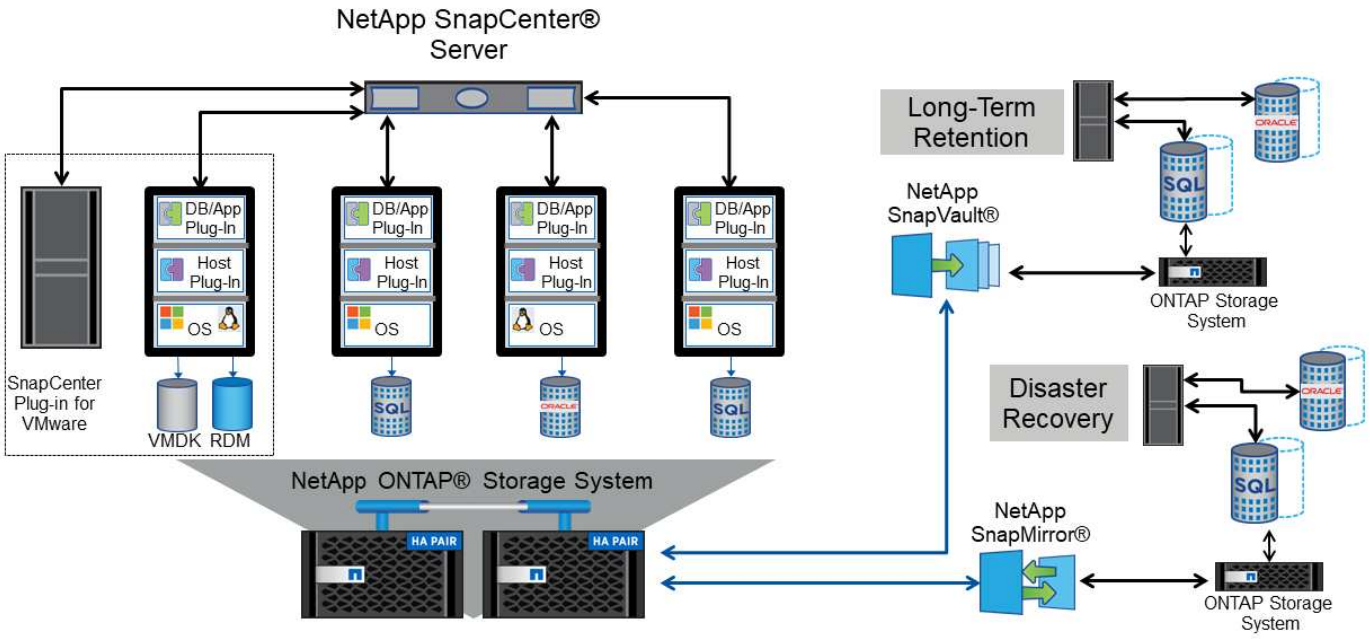
VMware vSphere向けSnapCenterプラグイン

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と整合性のある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アプリケーション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、vSphereを使用して、データがRDM LUN、VVOL、NVMe/TCPネームスペース、ゲストOSに直接接続されたiSCSI LUN、またはVMFSデータストアまたはNFSデータストア上のVMDKファイルに格納されているSQL ServerデータベースやOracleデータベースを保護できます。プラグインを使用すると、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たり、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たり、データベースファイルとログファイルを保護したりできます。このプラグインでは、バックアップとリカバリに加えて、開発やテストを目的としたデータベースのクローニングもサポートされていま

す。

次の図は、 SnapCenter の導入例を示しています。



サイジング情報については、 "VMware vSphere向けSnapCenterプラグインサイジングガイド"

VMware vSphere向けONTAPツールとVMware Live Site Recovery

ONTAP Tools for VMware vSphere（OT4VS）は、VMware vSphereとNetApp ONTAPをシームレスに統合するための無償プラグインです。vSphere Web ClientからONTAPストレージを直接管理できるため、ストレージのプロビジョニング、レプリケーションの管理、パフォーマンスの監視などのタスクを簡単に実行できます。

ディザスタリカバリ機能を強化するには、VMware Live Site Recovery（旧称Site Recovery Manager）とともに、VMware vSphere向けONTAPツールの一部であるNetApp SRA for ONTAPを利用することを検討してください。このツールでは、SnapMirrorを使用したディザスタリカバリサイトへのデータストアのレプリケーションがサポートされているだけでなく、レプリケートされたデータストアをクローニングしてDR環境で無停止でテストを実行できます。また、災害からのリカバリや、システム停止を解決したあとの本番環境の再保護も、組み込みの自動化機能により合理化されています。

NetApp Disaster Recovery

災害復旧 (DR) は、災害発生時にデータとアプリケーションを保護するための包括的なソリューションを提供するクラウドベースのサービスです。自動フェイルオーバーとフェイルバック、複数のポイントインタイムリカバリポイント、アプリケーション整合性のある災害復旧、オンプレミスとクラウドベースの両方のONTAPシステムのサポートなど、さまざまな機能を提供します。NetApp Disaster Recovery は、 ONTAPおよびVMware vSphere 環境とシームレスに連携するように設計されており、災害復旧のための統合ソリューションを提供します。

vSphere Metro Storage Cluster（vMSC）とNetApp MetroClusterおよびSnapMirrorのアクティブな同期

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）構成を検討してください。vMSCは、同期レプリケーションを使用するVMware認定

のNetAppサポートソリューションです。高可用性クラスタと同じメリットを提供しながら、別々のサイトに分散してサイト障害から保護します。NetApp SnapMirrorアクティブ同期（ASAおよびAFFを使用）、およびAFFを使用したMetroClusterでは、同期レプリケーションのコスト効率に優れた構成が提供され、単一のストレージコンポーネント障害からの透過的なリカバリ、SnapMirrorアクティブ同期の場合の透過的なリカバリ、またはMetroClusterを使用したサイト障害発生時の単一コマンドによるリカバリが可能です。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 ）

スループット制限は、サービスレベルの制御や不明なワークロードの管理に役立ちます。また、導入前にアプリケーションをテストして、本番環境の他のワークロードに影響しないように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 QoSポリシーのサポート

ONTAPを実行しているシステムでは、ストレージQoS機能を使用して、ファイル、LUN、ボリューム、SVM全体などのさまざまなストレージオブジェクトのスループットをMBpsやIOPS（1秒あたりのI/O数）で制限できます。

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。

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

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。

を参照してください "パフォーマンスの監視と管理の概要" を参照してください。

VVOL以外のNFSデータストア

ONTAP QoSポリシーは、データストア全体またはデータストア内の個々のVMDKファイルに適用できます。ただし、従来の（VVOL以外の）NFSデータストア上のすべてのVMが、特定のホストの共通のI/Oキューを共

有していることを理解しておくことが重要です。ONTAP QoSポリシーで調整されているVMがある場合、実際にはそのホストでは、そのデータストアのすべてのI/Oが調整されているように見えます。

- 例： *
  *ホストESXi-01によって従来のNFSデータストアとしてマウントされているボリュームに対して、vm1.vmdkにQoS制限を設定します。
  *同じホスト（esxi-01）がVM2.vmdkを使用しており、同じボリューム上にあります。
  *vm1.vmdkがスロットルされると、vm1.vmdkと同じIOキューを共有するため、vm2.vmdkもスロットルされているように見えます。

VVOLには適用されません。

vSphere 6.5以降では、Storage I/O Control（SIOC）v2を使用したStorage Policy-Based Management（SPBM）を使用して、VVol以外のデータストアに対するファイル単位の制限を管理できます。

SIOCポリシーとSPBMポリシーを使用したパフォーマンスの管理の詳細については、次のリンクを参照してください。

"SPBMのホストベースルール：SIOC v2"
"vSphereによるストレージI/Oリソースの管理"

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。

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。従来のNFSデータストアでは、前述したQoSの制限が引き続き適用されることに注意してください。

VMFSテタストア

ONTAP LUNを使用すると、LUNを含むFlexVolボリュームまたは個 々 のLUNにQoSポリシーを適用できますが、ONTAPではVMFSファイルシステムが認識されないため、個 々 のVMDKファイルには適用できません。

vVolテエタストア

最小/最大QoSは、Storage Policy-Based ManagementとVVOLを使用することで、他のVMやVMDKに影響を与えることなく、個 々 のVMやVMDKに簡単に設定できます。

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。

VVOLを使用するには、VASA Provider for ONTAPとして機能するONTAP Tools for VMware vSphereを使用する必要があります。VVOLのベストプラクティスについては、を参照して"VMware vSphere Virtual Volume（VVOL）とONTAP"ください。

ONTAP の QoS と VMware の SIOC

ONTAP QoSとVMware vSphere Storage I/O Control（SIOC）は、vSphere管理者とストレージ管理者が連携して使用し、ONTAPを実行するシステムでホストされている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。	○（データストアは調整可能）
ボリューム（ NFS データストア）への QoS の設定	はい。	○（データストアは調整可能）
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。

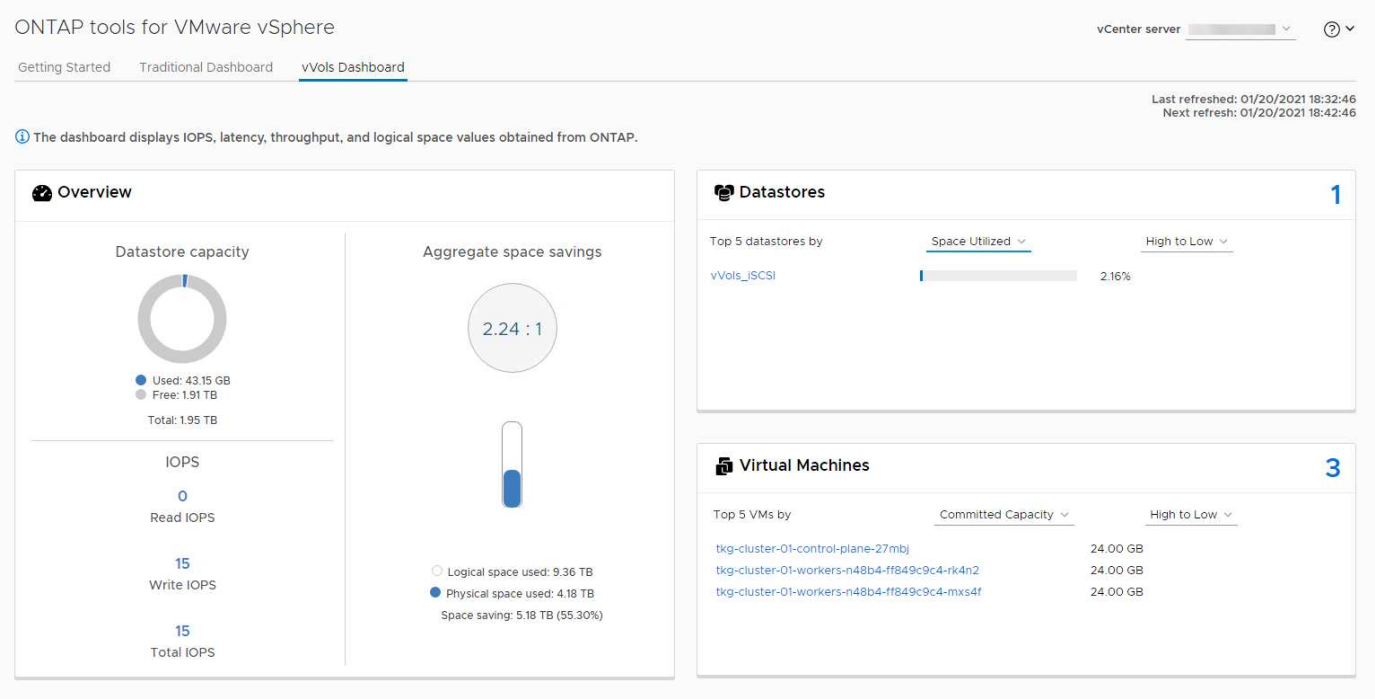
ストレージポリシーベースの管理と**VVOL**

VMware vSphere APIs for Storage Awareness（VASA）を使用すると、ストレージ管理者は適切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管理者は必要なときにいつでもそれらのデータストアを使用してVMをプロビジョニングできます。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がリリースされる前は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、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。

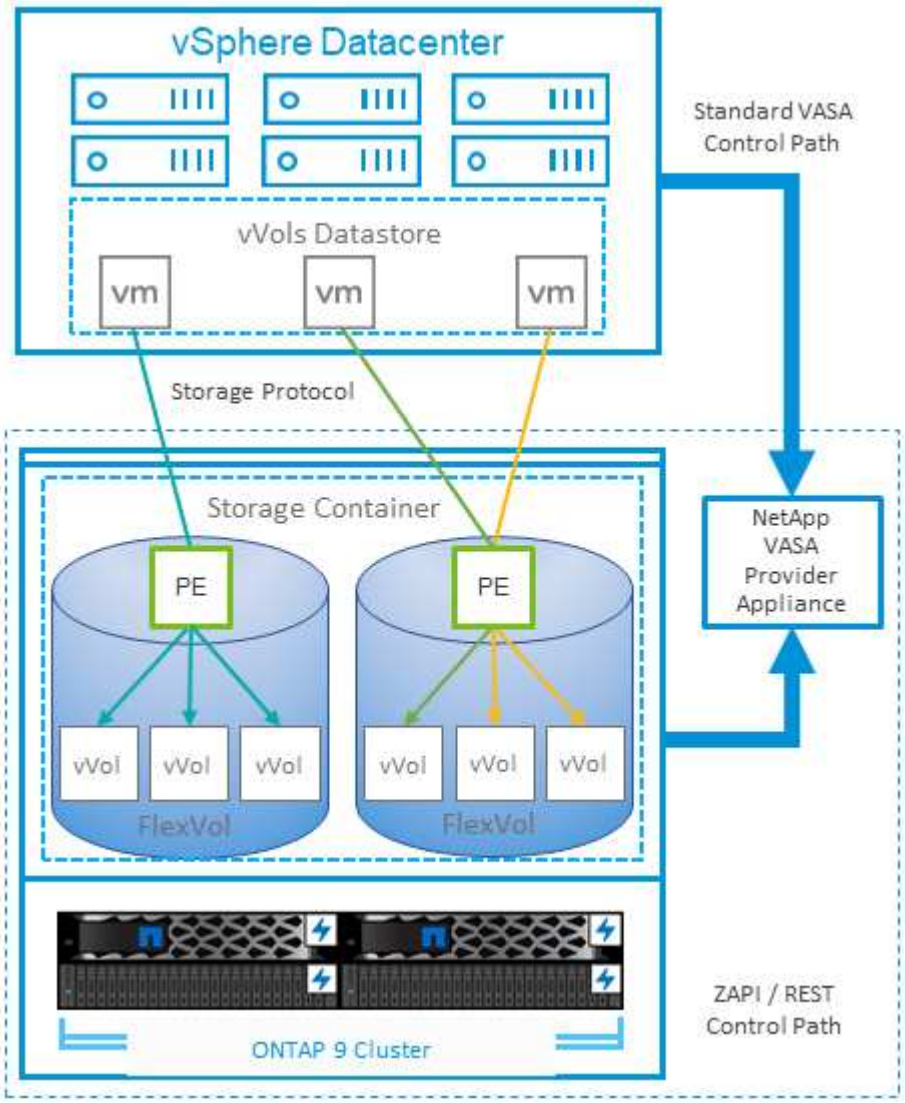
ONTAP は、 VMFS データストアと NFS データストアの両方をサポートしています。SAN データストアで VVOL を使用すると、 VM レベルのきめ細かさなど、 NFS のメリットの一部を活用できます。ここでは考慮すべきベストプラクティスをいくつか示します。また、追加情報はにあります "TR-4400"：

- 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。

- *ファーストパーティ製品*Amazon FSx for NetApp ONTAP、 Google Cloud NetApp Volumes、 Azure NetApp Files は、主要なパブリッククラウド環境で高性能なマルチプロトコルのマネージド ストレージ サービスを提供します。これらは、VMware Cloud on AWS (VMC on AWS)、Azure VMware Solution (AVS)、Google Cloud VMware Engine (GCVE) で、ゲスト オペレーティング システム (GOS) およびコンピューティング インスタンスのデータストアまたはストレージとして直接使用できます。

- *クラウド サービス*NetApp Backup and RecoveryまたはSnapMirror Cloud を使用して、パブリック クラウド ストレージを使用するオンプレミス システムからデータを保護します。NetApp Copy and Sync は、NAS およびオブジェクト ストア間でのデータの移行と同期に役立ちます。NetApp Disaster Recovery は、クラウドへの DR、オンプレミスへの DR、オンプレミス間の DR に対応した堅牢で高性能な災害復旧ソリューションの基盤としてNetAppテクノロジーを活用する、コスト効率が高く効率的なソリューションを提供します。
- * 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ときは、将来のクラウド 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、データには別の LUN または NFS エクスポートを使用します。これにより、VM とデータを個別にクラウド サービスに移行できます。

セキュリティトピックの詳細については、次のリソースを参照してください。

- "ONTAP Select のドキュメント"
- "バックアップとリカバリのドキュメント"
- "災害復旧ドキュメント"
- "NetApp ONTAP 対応の Amazon FSX"
- "AWS 上の VMware Cloud"
- "Azure NetApp Filesとは何ですか?"
- "Azure VMware 解決策の略"
- "Google Cloud VMware Engine"
- "Google Cloud NetApp Volumeとは"

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を実行するシステムでは、保存データ暗号化によってあらゆるデータを簡単に保護できます。NetAppストレージ暗号化（NSE）では、ONTAPで自己暗号化ドライブ（SED）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を含むFIPS 140-2レベル1標準に準拠していることが確認されています。

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が付属しています。*NetAppソフトウェアの暗号化機能にはオンボードキーマネージャが追加料金なしで含まれているため、購入や使用が複雑な高可用性キー管理サーバがなくても簡単に使用を開始できます。
- * 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。ライセンスをインストールしたら、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。

セキュリティトピックの詳細については、次のリソースを参照してください。

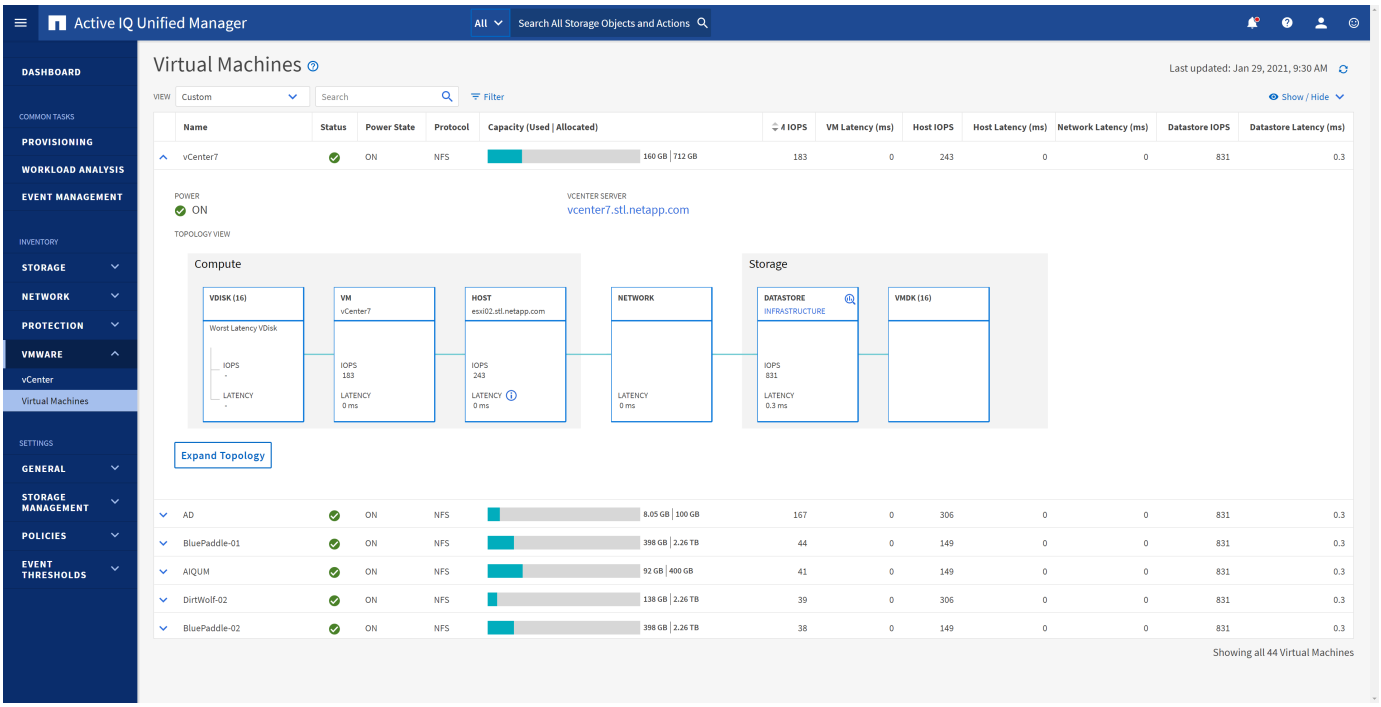
- "セキュリティテクニカルレポート"
- "セキュリティ強化ガイド"
- "ONTAPセキュリティとデータ暗号化の製品ドキュメント"

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。

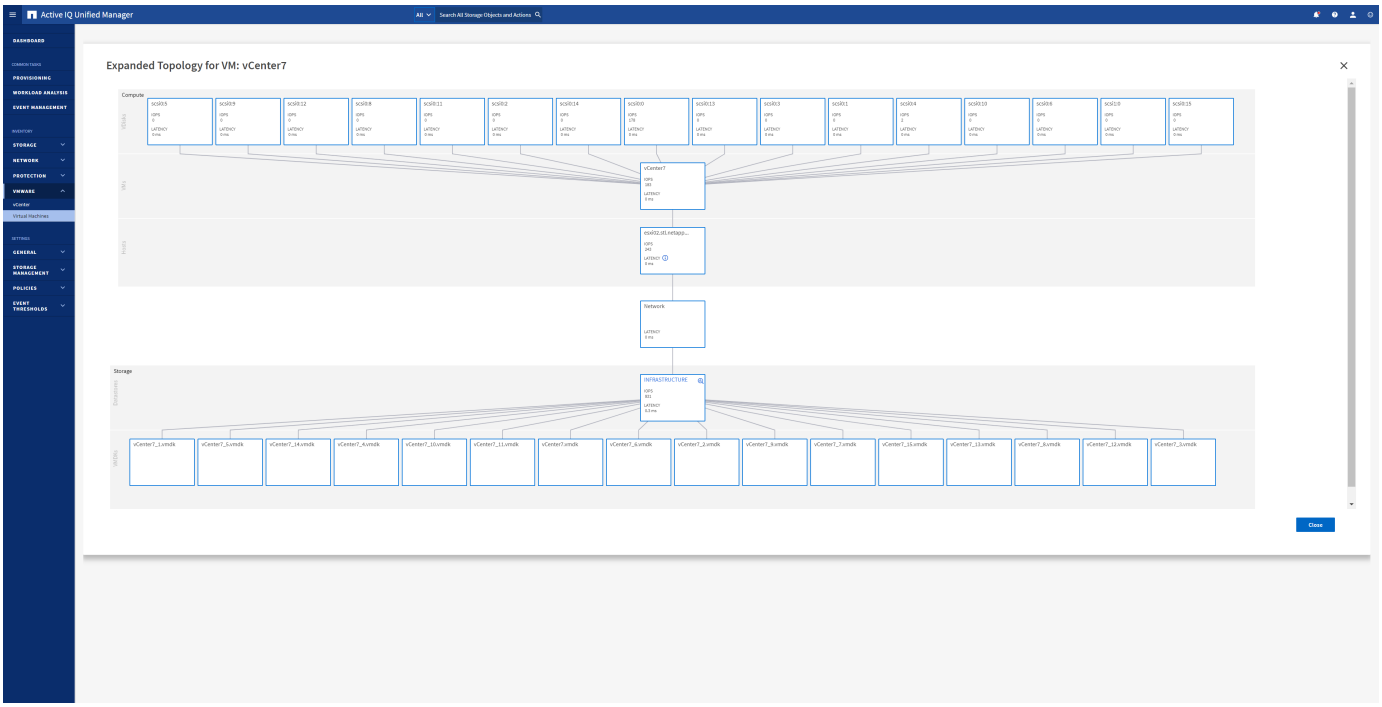
次のスクリーンショットは、 Active IQ Unified Manager の仮想マシンビューを示しています。



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

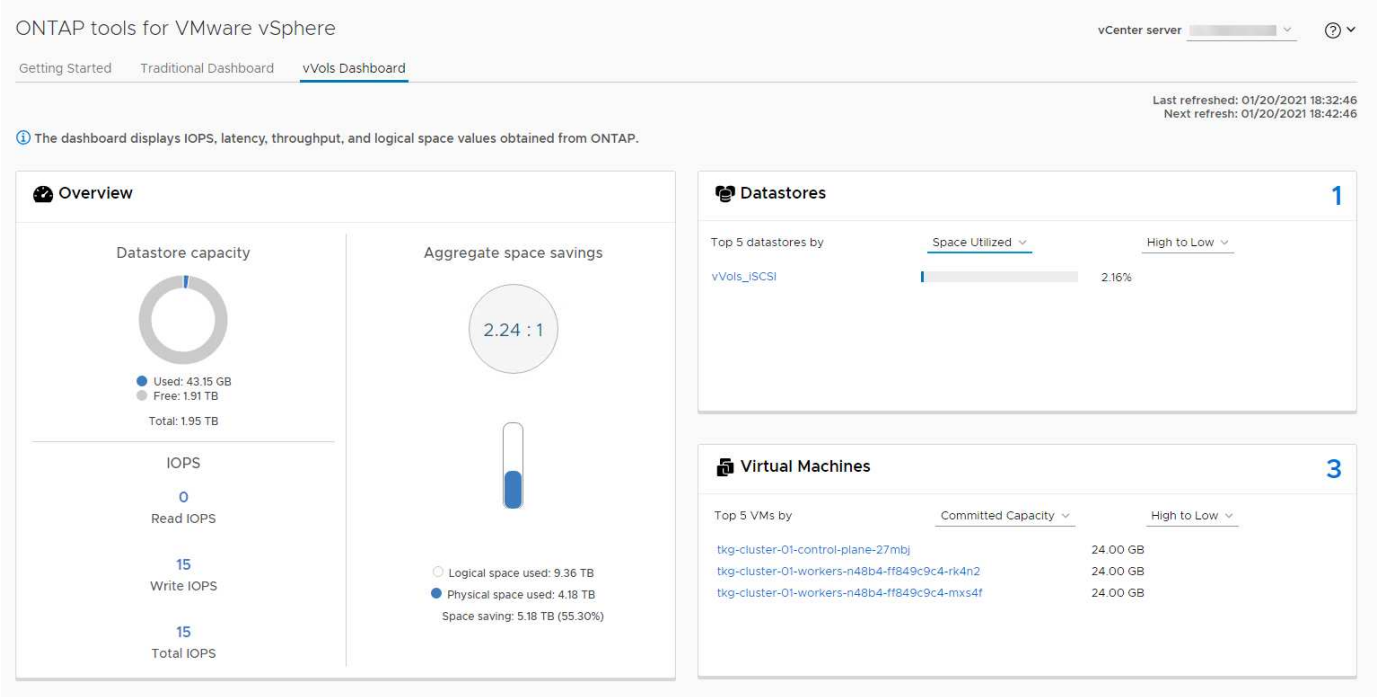
者は適切に定義された機能を使用してデータストアを簡単に設定でき、VM管理者は必要なときにいつでもそれらのデータストアを使用してVMをプロビジョニングできます。

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がリリースされる前は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、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。

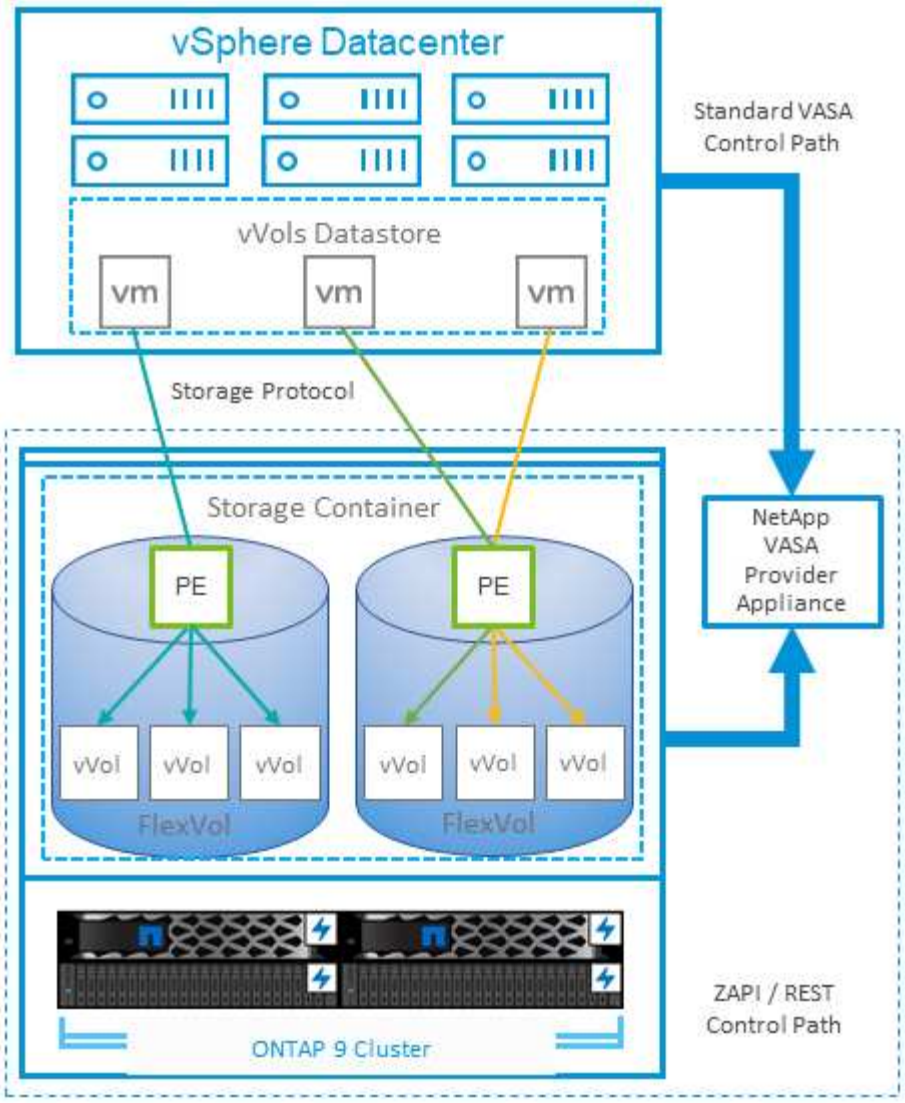
VASA は、ストレージを照会して一連のストレージ機能を vCenter に返すためのテクノロジを提供します。VASA ベンダープロバイダは、ストレージシステムの API およびコンストラクトと、 vCenter が認識可能な VMware API との間の変換機能を提供します。ネットアップのVASA Provider for ONTAPは、ONTAP Tools for VMware vSphereアプライアンスVMの一部として提供されます。vCenterプラグインは、VVOLデータストアをプロビジョニングおよび管理するためのインターフェイスと、ストレージ機能プロファイル（SCP）を定義する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

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データストアクラスタにVMを自動的に配置する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。

- 特定の要件がない限り、SDRSを使用しないでください。

- ONTAPを使用する場合、SDRは必要ありません。SDRは重複排除や圧縮などのONTAPのStorage Efficiency機能を認識しないため、環境に最適でない判断を下す可能性があります。
- SDRはONTAP QoSポリシーを認識しないため、パフォーマンスに最適でない判断を下す可能性があります。
- SDRはONTAP Snapshotコピーを認識しないため、Snapshotが急増する原因となるような判断を下す可能性があります。たとえば、VMを別のデータストアに移動すると、新しいデータストアに新しいファイルが作成されるため、スナップショットが拡張されます。これは、大容量ディスクまたは多数のスナップショットを持つVMに特に当てはまります。その後、VMを元のデータストアに戻すと、元のデータストア上のスナップショットがさらに大きくなります。

SDRSを使用する場合は、次のベストプラクティスを考慮してください。

- 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を移動する場合、デスティネーションでの重複排除または圧縮の度合いに応じて、ONTAPのクローニングや重複排除によるスペース削減量が削減されることがあります。
  - 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。

SDRSの詳細については、VMwareのドキュメントを参照してください "Storage DRS FAQ"。

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。ONTAP toolsの概要ページで、下にスクロールして[ESXi Host compliance]ポートレットの[Apply Recommended Settings]をクリックします。

現在サポートされているすべてのバージョンのONTAPに推奨されるホスト設定を次に示します。

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

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
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。 "VMFS5仮想マシンのスペース再生"	いいえ
VMFS3.EnableVMFS6Unmap	デフォルトのままにする（1）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*		
newSyncInterval	vSphere CSI for Kubernetesを使用していない場合は、 "VMware KB 386364"	いいえ
Net.TcpipHeapSize の場合	vSphere 6.0 以降： 32 に設定 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、および7.0以降ではデフォルト（1024MB）に設定されます。	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 ～ 8.0 の場合、128 に設定。この設定は、ESXi 8.0 以降のリリースでは無視されます。	いいえ
* FC / FCoE 設定 *		

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
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。 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。 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。 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。 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。 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。 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。 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を使用している場合、NFSの詳細設定オプションMaxQueueDepthが意図したとおりに機能しないことがあります。詳細については、を参照"VMware KB 86331"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。

- 高パフォーマンス環境でASA以外のシステムを使用する場合、または単一の LUN データストアでパフォーマンスをテストする場合は、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 設定の 1000 から値 1 に変更することを検討してください。見る"VMware KB 2069356"詳細については。
- vSphere 6.7 Update 1 では、VMware はラウンド ロビン PSP 用の新しいレイテンシ ロード バランス メカニズムを導入しました。レイテンシ オプションは、NVMe 名前空間で HPP (高パフォーマンス プラグイン) を使用する場合、および vSphere 8.0u2 以降で iSCSI および FCP 接続された LUN を使用する場合にも利用できるようになりました。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 帯域幅とパスのレイテンシを考慮します。 NetApp、あるパスのネットワーク ホップが他のパスよりも多い場合や、 NetApp ASAシステムを使用している場合など、パス接続が等しくない環境では、レイテンシ オプションを使用することをお勧めします。見る "レイテンシラウンドロビンのデフォルトパラメータを変更"詳細についてはこちらをご覧ください。

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については、を参照してください。詳細については"VMware vSphere 8.xとONTAPの併用"、vSphere 7を使用するNVMe-oFについては、を参照してください。詳細については"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。"、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 toolsを使用した仮想ボリューム（VVol）10

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 3、ONTAP tools 10.4リリース、および新しいNetApp ASAシステムに搭載された新しいvVol機能が追加されました。

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、ファイルが含まれ、vSphere 8-NVMeネームスペース（ONTAP tools 9.13P2で使用）に対応できるようになりました。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VMwareと緊密に連携し、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も協力しました。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。

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。

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"

Virtual Volumeデータストア

| 仮想ボリューム データストアは、VASA プロバイダーによって作成および管理されるvVolsコンテナの論理データストア表現です。コンテナは、VASA プロバイダーによって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ツールは、複数のFlexVolボリューム (バックアップ ボリュームと呼ばれる) を単一のvVolsデータストアに割り当てることをサポートしており、これらのvVolsデータストアはONTAPクラスタ内の複数のノードにまたがって、異なる機能を持つフラッシュ 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ボリュームを作成するか、使用可能な場合はバックアップ ストレージとして事前に作成されたFlexVolボリュームを選択できます。

仮想ボリューム（**VVol**）

vVols は、 vVolsデータストアに保存される実際の仮想マシン ファイルとディスクです。vVol (単数形) という用語を使用すると、単一の特定のファイル、LUN、または名前空間を指します。ONTAP は、データストアが使用するプロトコルに応じて、NVMe 名前空間、LUN、またはファイルを作成します。vVolsにはいくつかの異なるタイプがあります。最も一般的なタイプは、Config（VMFS が存在する唯一のタイプで、VM の VMX ファイルなどのメタデータ ファイルが含まれます）、Data（仮想ディスクまたは VMDK）、および Swap（VM の電源オン時に作成される）です。VMware VM 暗号化によって保護されるvVols のタイプは Other になります。VMware VM 暗号化を、 ONTAPボリュームまたはアグリゲート暗号化と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あらゆるストレージ機能を簡単に使用できるようになります。VASA 以前は、VM 管理者は VM ストレージ ポリシーを定義できましたが、多くの場合、ドキュメントや命名規則を使用して、ストレージ管理者と協力して適切なデータストアを特定する必要がありました。VASA を使用すると、適切な権限を持つ vCenter 管理者は、vCenter ユーザーが VM のプロビジョニングに使用できるさまざまな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機能のマッピングにより、vCenter は選択可能な互換性のあるデータストアのリストを表示できるようになり、また、VCF (旧称 Aria および vRealize) Automation やVMware vSphere Kubernetes Service (VKS) などの他のテクノロジを使用して、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るようになります。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 プロバイダー ルールと VM ストレージ 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vVolsデータストアに焦点を当てます。

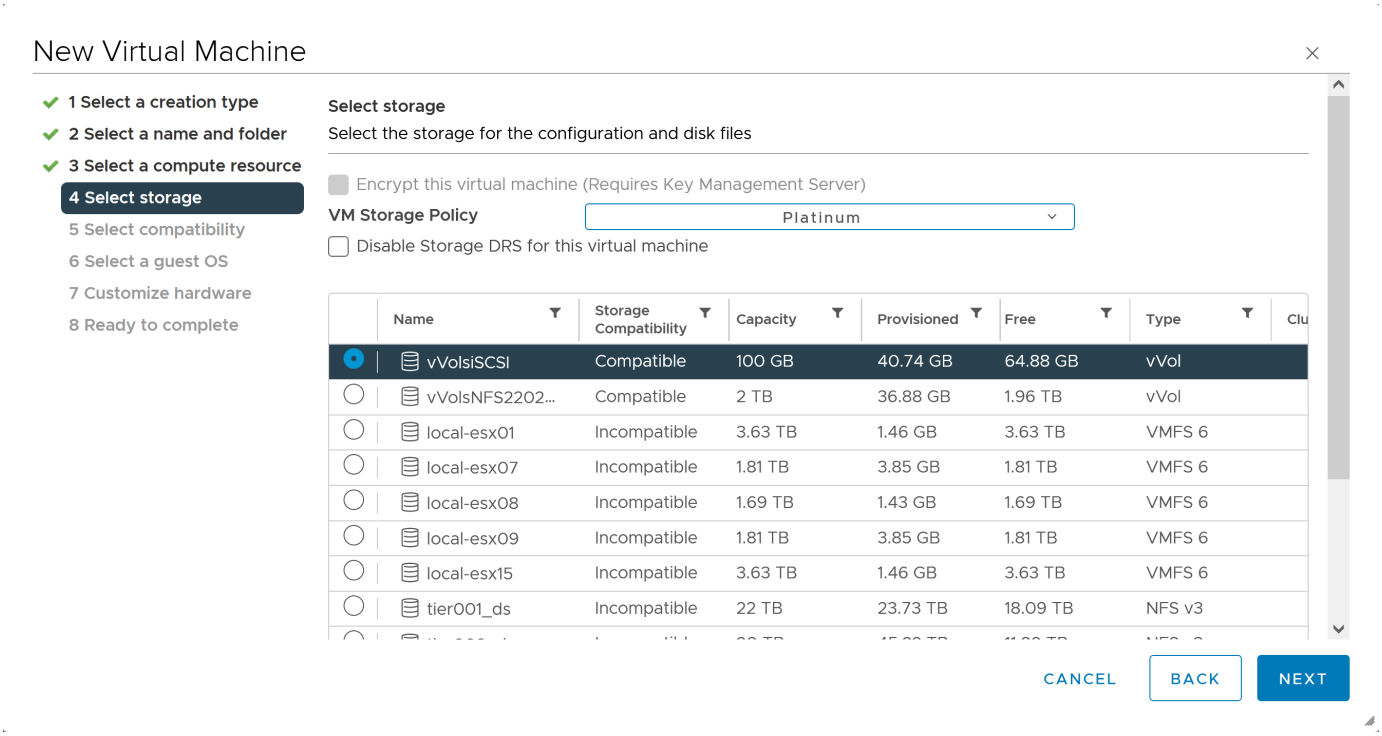
VMストレージ ポリシー

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 tools 10.Xでは、VMストレージポリシー自体にストレージ属性を直接指定できるため、ONTAP tools 9.Xよりもシンプルなアプローチが採用されています。

前述したように、ポリシーを使用すると、VMまたはVMDK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

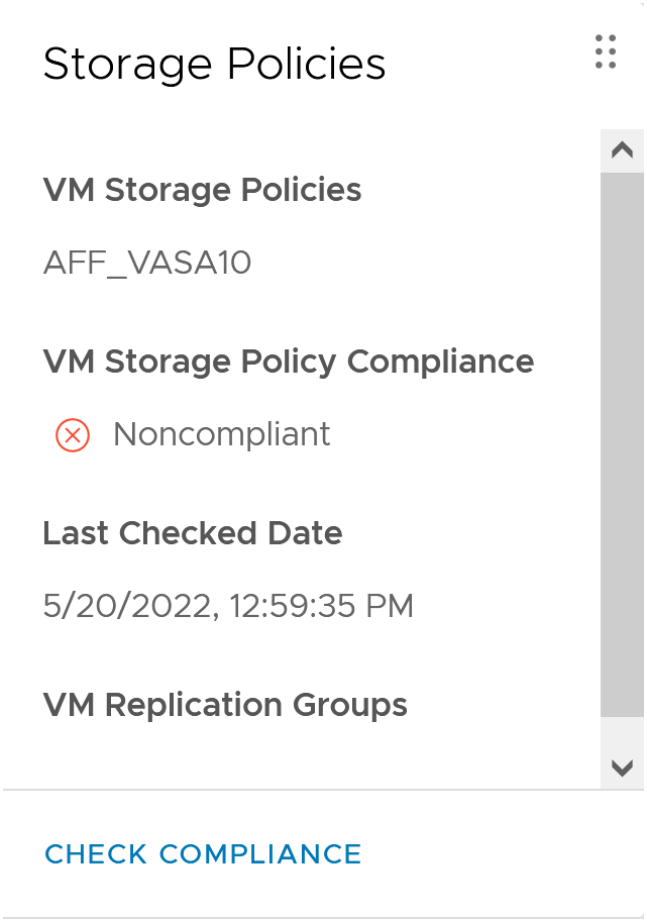
れ、準拠している個 々 のFlexVol volumeにvVolが配置されます。

ストレージポリシーを使用して**VM**を導入します



VM がプロビジョニングされると、VASA プロバイダーはコンプライアンスを継続的にチェックし、バックアップ ボリュームがポリシーに準拠しなくなった場合は vCenter でアラームを発行して VM 管理者に警告します。

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以来、VASA 仕様をサポートしています。他のNetAppストレージ システムでも VASA がサポートされている可能性がありますが、このドキュメントでは現在サポートされているONTAP 9 のリリースに焦点を当てています。

ONTAP

NetApp は、 AFF、 ASA、 FASシステム上のONTAP 9 に加えて、 ONTAP Select、VMware Cloud on AWS を使用したAmazon FSx for NetApp 、Azure VMware Solution を使用したAzure NetApp Files 、 Google Cloud NetApp Volumes 、Equinix のNetApp Private Storage 上の VMware ワークロードをサポートしていますが、具体的な機能はサービス プロバイダーや利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。

公開時点では、ハイパースケーラー環境は従来の NFS v3 データストアのみに制限されているため、 vVolsはオンプレミスのONTAPシステム、またはオンプレミスシステムの全機能を提供するクラウド接続システム (世界中のNetAppパートナーやサービス プロバイダーがホストしているシステムなど) 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

VMware は 2015 年に VASA 2.0 でvVolsサポートを導入したとき、これを「外部ストレージ (SAN/NAS) の新しい運用モデルを提供する統合および管理フレームワーク」と説明しました。この運用モデルは、 ONTAPストレージと組み合わせることで、いくつかの利点をもたらします。

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により、VM をプロビジョニングし、その後、事前定義されたポリシーを使用して管理できるようになります。これは、いくつかの点で IT 運用に役立ちます。

- *速度を上げます。*ONTAPツールを使用すると、vCenter 管理者がストレージ プロビジョニングアクティビティのためにストレージ チームにチケットを開く必要がなくなります。ただし、vCenter およびONTAPシステムでのONTAPツール 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により、独立したチーム (ストレージ チームなど) または同じチームによる独立したアクティビティが引き続き許可されます。
- *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。
- *より優れた容量管理*VASAツールとONTAPツールを使用すると、必要に応じて個 々 のアグリゲートレベルまでストレージ容量を表示し、容量が少なくなり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

ファイバ チャネルと iSCSI を使用する SAN ストレージ システムは、VMware が ESX 用にサポートした最初のシステムでしたが、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がありませんでした。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。このため、ストレージ システムが個々の VM ストレージのパフォーマンス、クローン作成、および保護を直接管理することは困難です。vVolsは、NFS ストレージを使用しているお客様が既に享受しているストレージの細分性と、ONTAPの堅牢でハイパフォーマンスSAN 機能を実現します。

現在、vSphere 8 およびONTAP tools for VMware vSphereと、従来の SCSI ベース プロトコルのvVolsで使用されるのと同じきめ細かい制御が、NVMe over Fabrics を使用する最新のファイバー チャネル SAN でも利用できるようになり、大規模なパフォーマンスがさらに向上します。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 変換を行わずに、 vVolsを使用して完全なエンドツーエンドのNVMe ソリューションを展開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 はストレージにオフロードされるさまざまな操作を提供しますが、VASA プロバイダーによって対処されるギャップがいくつかあります。SAN VAAI は、VMware 管理の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備えた VM には制限があります。vVols は仮想マシン ディスクに個別の LUN、名前空間、またはファイルを使用するため、 ONTAP はファイルまたは LUN を迅速かつ効率的にクローンして、デルタ ファイルを必要としない VM 単位のスナップショットを作成できます。NFS VAAI は、ホット (電源オン) Storage vMotion 移行のクローン操作のオフロードもサポートしていません。VAAI を従来の NFS データストアで使用する場合、移行のオフロードを可能にするには、VM の電源をオフにする必要があります。ONTAPツールの VASA プロバイダーは、ホット移行とコールド移行のためのストレージ効率の高いクローンをほぼ瞬時に作成できるほか、 vVolsのボリューム間移行のためのほぼ瞬時のコピーもサポートします。これらの大きなストレージ効率の利点により、 vVolsワークロードを最大限に活用できる可能性があります。

"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は要件を満たせない場合でも、 vVolsによるコピーエクスペリエンスの改善により、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 vSphere Kubernetes Service (VKS) 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のようなサービスを提供します。
- 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、単一のボリューム内、またはONTAPクラスタ内の複数のボリュームにわたって迅速に作成されます。これは、従来の VAAI 対応クローンに比べて利点があります。ストレージ効率も優れています。ボリューム内のクローンでは、 FlexCloneボリュームに似たONTAPファイル クローンを使用し、ソース vVol ファイル/LUN/名前空間からの変更のみを保存します。そのため、本番環境やその他のアプリケーション用の長期的な VM は、迅速に作成され、最小限のスペースで済み、VM レベルの保護 (VMware vSphere用の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) のメリットを享受できます。VASA を使用すると、コピーが完了する前にクローンを作成し、宛先でそのクローンにアクセスできるため、ボリューム間のクローン作成は VAAI よりもvVolsの方がはるかに高速になります。データ ブロックはバックグラウンド プロセスとしてコピーされ、宛先 vVol に入力されます。これは、従来の LUN に対するONTAP の無停止 LUN 移動の動作と似ています。
- 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。
- FCD VMDK は、その名前が示すように vSphere の第一級オブジェクトであり、接続されている可能性のある VM とは別に独立して管理できるライフサイクルを備えているため、Amazon EBSのようなサービスを FCD を通じて提供できます。

チェックリスト

このインストールチェックリストを使用して、導入を確実に成功させることができます（10.3以降用に更新）。

1 初期計画

- インストールを開始する前に、を確認して、導入が認定されていることを確認する必要があり "Interoperability Matrix Tool （ IMT ）"ます。
- 環境に必要なONTAP toolsの設定のサイズとタイプを確認します。詳細については、を参照して "ONTAP tools for VMware vSphereを導入するための構成の制限"ください。
- マルチテナントSVMを使用するか、クラスタへのフルアクセスを許可するかを決定します。マルチテナントSVMを使用する場合は、使用するSVMごとにSVM管理LIFが必要です。このLIFには、ONTAP toolsからポート443経由で到達できる必要があります。
- ストレージ接続にFibre Channel（FC；ファイバチャネル）を使用するかどうかを決定します。その場合は、FCスイッチでESXiホストとSVMのFC LIFの間の接続を有効にする必要があります "ゾーニングの設定"。
- ONTAP tools Storage Replication Adapter（SRA）for VMware Site Recovery Manager（SRM）とLive Site Recovery（VLSR）のどちらを使用するかを決定します。その場合は、SRAをインストールするためにSRM/VLSRサーバ管理インターフェイスにアクセスする必要があります。
- ONTAPツールで管理されるSnapMirrorレプリケーション（のアクティブな同期など）を使用する場合は、SnapMirror "ONTAPでクラスタ間SVMピア関係を作成する"でONTAPツールを使用する前に、ONTAP管理者がSnapMirrorを使用する必要があります。 "ONTAPでクラスタピア関係を作成する"
- "ダウンロード"ONTAP toolsのOVA、および必要に応じてSRAのtar.gzファイル。

2 **IP**アドレスと**DNS**レコードのプロビジョニング

- ネットワークチームに次のIP情報を要求します。最初の3つのIPアドレスが必要です。ノード2とノード3はスケールアウトハイアベイラビリティ（HA）環境に使用されます。DNSホストレコードは必須であり、すべてのノード名とすべてのアドレスは同じVLANおよびサブネット上にある必要があります。
- ONTAPツールのアプリケーションアドレスはです。。。\\
- 内部サービスのアドレスはです。。。\\
- ノード1のDNSホスト名__
- ノード1のIPアドレスは_です。。。\\
- サブネットマスク_____。。。\\
- デフォルトゲートウェイはです。。。\\
- DNSサーバ1：。。_
- DNSサーバ2 。。。\\
- DNS検索ドメイン_____
- ノード2のDNSホスト名（オプション）_____
- ノード2のIPアドレス（オプション）_____。。。_____
- ノード3のDNSホスト名（オプション）_____
- ノード3のIPアドレス（オプション）_____。。。_____
- 上記のすべてのIPアドレスのDNSレコードを作成します。

3 ネットワークファイアウォールの設定

- ネットワークファイアウォールで、上記のIPアドレスに必要なポートを開きます。最新のアップデートについては、を参照してください "ポートの要件"。

4 ストレージ

- 共有ストレージデバイス上にデータストアが必要です。必要に応じて、ノード1と同じデータストア上のコンテンツライブラリを使用して、VAAIでテンプレートをすばやくクローニングすることができます。
- コンテンツライブラリ（HAにのみ必要）_____
- ノード1のデータストア__
- ノード2のデータストア（オプションですがHA用に推奨）_____
- ノード3のデータストア（オプションですがHAには推奨）_____

5 **OVA**の導入

- この手順の完了には最大45分かかることがあります。
- "OVAの導入"vSphere Clientを使用する。
- OVA導入のステップ3で、[customize this virtual machines's hardware]オプションを選択し、ステップ10で以下を設定します。
- "CPUホットアドを有効にする"
- "メモリホットプラグ"

6 **ONTAP**ツールへの**vCenter**の追加

- "vCenter Serverインスタンスの追加"ONTAPツールマネージャ。

7 **ONTAP**ツールにストレージバックエンドを追加

- "ONTAPユーザのロールと権限の設定"管理者を使用しない場合は、含まれているJSONファイルを使用します。
- vCenter でONTAPクラスタ認証情報を使用するのではなく、ストレージ マルチテナンシーを使用して特定の SVM を vCenter に割り当てる場合は、次の手順に従ってください。
- "オンホオトクラスタ"ONTAP tools Managerを使用し、vCenterに関連付けます。
- "オンボードSVM"ONTAP toolsのvCenter UIで、
- vCenter 内でマルチテナント SVM を使用していない*場合*:
- "オンホオトクラスタ"ONTAP toolsのvCenter UIで直接実行できます。または、このシナリオでは、VVOLを使用していないSVMを直接追加することもできます。

8 アプライアンスサービスの設定（オプション）

- VVOLを使用するには、最初に行う必要があり "アプライアンスの設定を編集してVASAサービスを有効にする"ます。同時に、次の2つの項目を確認します。

- 上記の2つのオプションのIPアドレスを使用して、本番環境でVVOLを使用する場合 "高可用性を実現"。
- VMware Site Recovery ManagerまたはLive Site Recovery用のONTAP tools Storage Replication Adapter（SRA）を使用する場合は、を参照してください "SRAサービスを有効にする"。

9 証明書（オプション）

- VMwareで複数のvCenterでVVOLを使用する場合は、CA署名証明書が必要です。
- VASAサービス_____
- 管理サービス_____

10 導入後のその他のタスク

- HA環境でVMの非アフィニティルールを作成します。
- HAを使用している場合は、Storage vMotionノード2と3を別 々 のデータストアに接続します（オプションですが推奨）。
- "証明書の管理を使用する"ONTAP tools Managerで、必要なCA署名証明書をインストールします。
- SRM / VLSRに対してSRAを有効にして従来のデータストアを保護した場合は、 "VMware Live Site Recoveryアプライアンスでの SRAの設定"。
- ネイティブバックアップを構成する "ほぼゼロRPO"。
- 他のストレージメディアへの定期バックアップを設定します。

ONTAP でVVOLを使用する

VVOLをNetAppで使用するための鍵はONTAP Tools for VMware vSphereです。VMware vSphereは、NetAppのONTAP 9システム用のVASA（vSphere API for Storage Awareness）プロバイダインターフェイスとしてサーバされます。

ONTAPツールには、vCenter UI拡張機能、REST APIサービス、VMware Site Recovery Manager / Live Site Recovery用のStorage Replication Adapter、監視ツールとホスト構成ツール、および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。

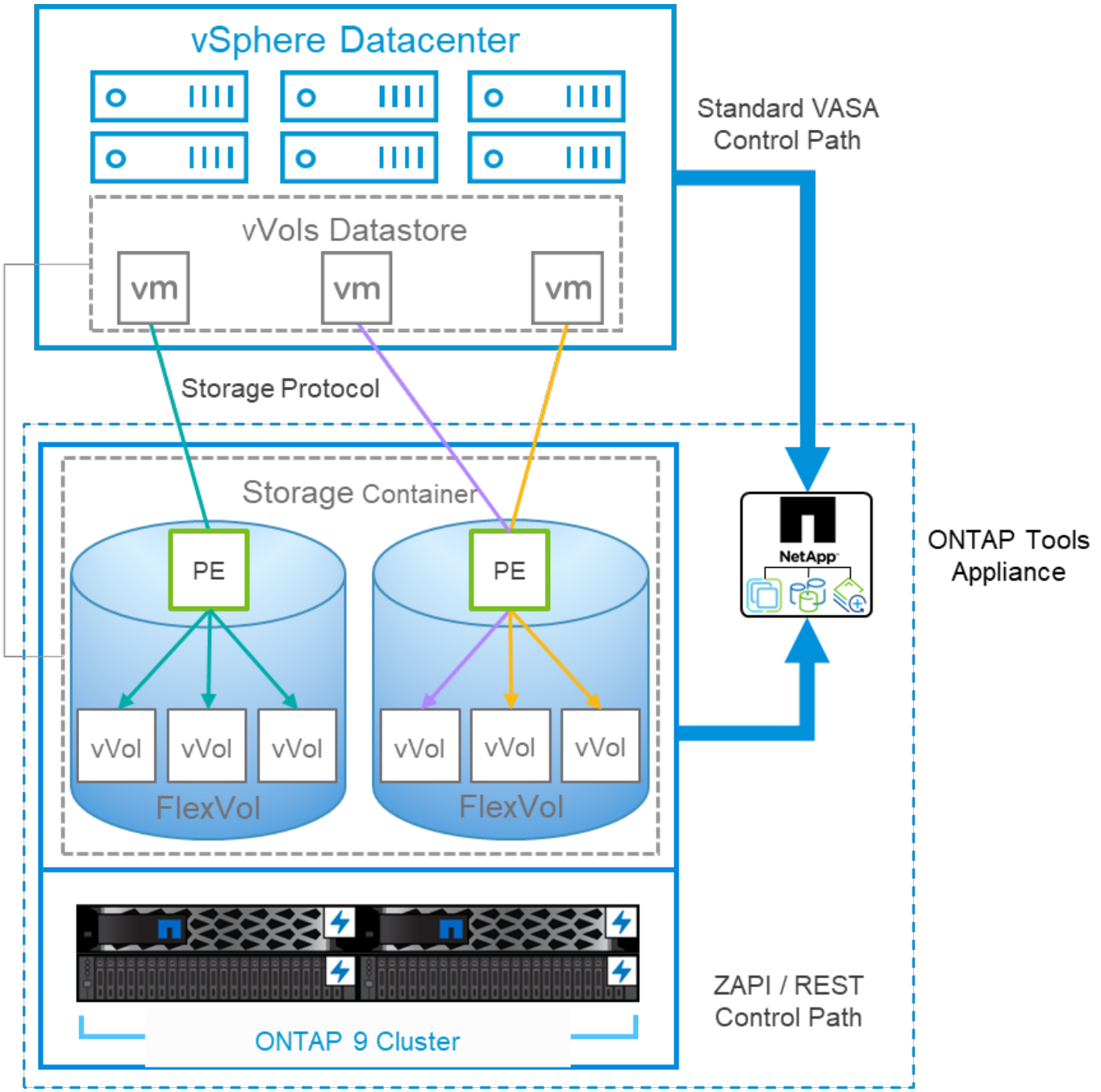
製品およびドキュメント

ONTAP Oneライセンスには、ONTAPシステムでVVOLを使用するために必要なすべてのライセンスが含まれています。追加で必要なのは、VASA Providerとして機能する無料のONTAP tools OVAだけです。VVOL環境では、VASA Providerソフトウェアによってアレイの機能がポリシーベースの属性に変換され、VASA APIを介して利用できるようになります。vSphere管理者は、機能がバックグラウンドでどのように管理されているかを知る必要はありません。これにより、割り当てられたストレージ容量がポリシーに基づいて動的に消費されるため、従来のデータストアを手動で作成したり、個 々 のストレージ消費率を管理したりする必要がなくなります。要するに、VVOLは、エンタープライズストレージの管理に伴う複雑さをすべて解消し、vSphere管理者から抽象化されて仮想化レイヤに注力できるようにします。

VMware Cloud FoundationとvSANを使用しているお客様の場合、vVolは補助ストレージとして任意の管理ドメインまたはワークロードドメインに追加できます。vVolは、共通のストレージポリシーベースの管理フレームワークを通じてvSANとシームレスに統合されます。

次世代のONTAP tools 10リリースファミリーは、ESXi上のシンプルなOVAフォーマットアプライアンスを通じて導入可能な、拡張性に優れたコンテナ化されたマイクロサービスベースのアーキテクチャにより、以前の機能を最新化します。ONTAP tools 10は、以前の3つのアプライアンスと製品のすべての機能を1つの環境に統合します。VVOLの管理には、ONTAP tools VASA Provider用のvCenter UI拡張機能またはREST APIを使用します。SRAコンポーネントは従来のデータストア用であることに注意してください。VMware Site Recovery Managerでは、vVolにSRAは使用されません。

ユニファイドシステムで**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。導入が完了したら、Manager UIにログインするか、REST APIを使用して、導入環境、vCenterのオンボード（プラグインがvCenterに登録されます）、ストレージシステムのオンボード、vCenterとのストレージシステムの関連付けを行うことがで

きます。ONTAP tools Manager UIでストレージシステムをオンボーディングし、vCenterとクラスタを関連付ける必要があるのは、専用のSVMでセキュアマルチテナンシーを使用する場合だけです。そうでない場合は、ONTAP tools vCenter UI拡張機能で目的のストレージクラスタをオンボーディングするか、REST APIを使用してオンボーディングできます。

このドキュメントの、またはを "ONTAP Tools for VMware vSphereのドキュメント"参照してください"vVolストレージの導入"。

> 相互依存関係の競合を避けるために、ONTAPツールとvCenterアプライアンスを従来のNFSまたはVMFSデータストアに格納することを推奨します。VVOLの処理ではvCenterとONTAPの両方のツールが相互に通信する必要があるため、ONTAP toolsアプライアンスまたはvCenter Serverアプライアンス（vCSA）を管理している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。この場合、vCenterまたはONTAP toolsアプライアンスをリブートすると、コントロールプレーンへのアクセスが中断し、アプライアンスをブートできなくなる可能性があります。

ONTAP toolsのインプレースアップグレードは、NetAppサポートサイトからダウンロード可能なアップグレードISOファイルを使用してサポートされ "ONTAP Tools for VMware vSphere 10 -ダウンロード"ます（ログインが必要です）。ガイドの手順に従って、 "ONTAP Tools for VMware vSphere 10.xから10.3へのアップグレード"アプライアンスをアップグレードします。ONTAP tools 9.13から10.3へのアップグレードを並行して実行することもできます。このテーマの詳細については、を参照して "ONTAP Tools for VMware vSphere 9.xから10.3への移行"ください。

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

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。

"ONTAP Tools for VMware vSphereのドキュメント"

はじめに

- "リリースノート"
- "ONTAP Tools for VMware vSphereの概要"
- "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

- "データストアのプロビジョニング"
- "ロールベースアクセス制御を設定する"
- "ハイアベイラビリティを設定する"
- "ESXiホストの設定を変更"

データストアの保護と管理

- "ONTAPツールとSnapMirror Active Syncを使用したvSphere Metro Storage Cluster（vMSC）の設定"

- "仮想マシンの保護"SRMを使用
- "クラスタ、データストア、仮想マシンの監視"

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。レイテンシ、IOPS、スループットなど、VVOLファイルおよびLUNに関する情報はONTAPから直接取得されます。現在サポートされているすべてのバージョンのONTAP 9を使用すると、デフォルトで有効になります。初期設定後、ダッシュボードにデータが読み込まれるまでに最大30分かかることがあります。

その他の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"）。LUN、ネームスペース、およびファイルの数とサイズに関する最新の制限については、を必ず確認してください "NetApp Hardware Universe の略"。

- 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、ONTAPのベストプラクティスに従ってFlexVolボリューム（ASA R2では不要）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vcenter 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。

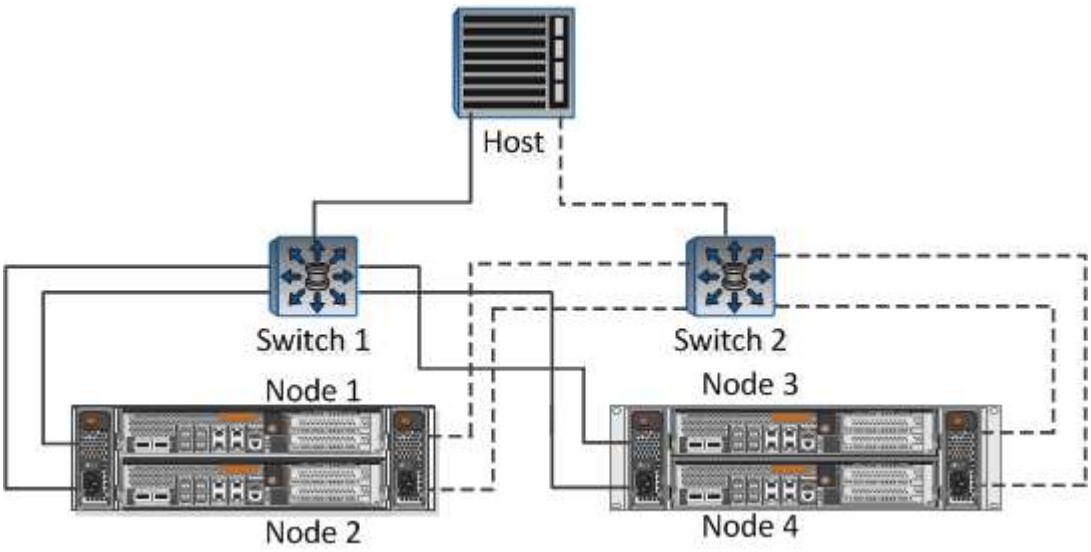
異なる**ONTAP** リリース間での**VVOL**処理は避けてください。

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"

必要に応じて、元の**FlexVol**ボリュームを計画します。

ASA R2以外のシステムでは、複数の元のボリュームをvVolデータストアに追加して、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、許可される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。

ASA R2システムでは、ボリュームやアグリゲートの概念がユーザから抽象化されるため、この複雑さは解消されます。動的配置は自動的に処理され、必要に応じてプロトコルエンドポイントが作成されます。追加の拡張が必要な場合は、追加のプロトコルエンドポイントをその場で自動的に作成できます。

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。

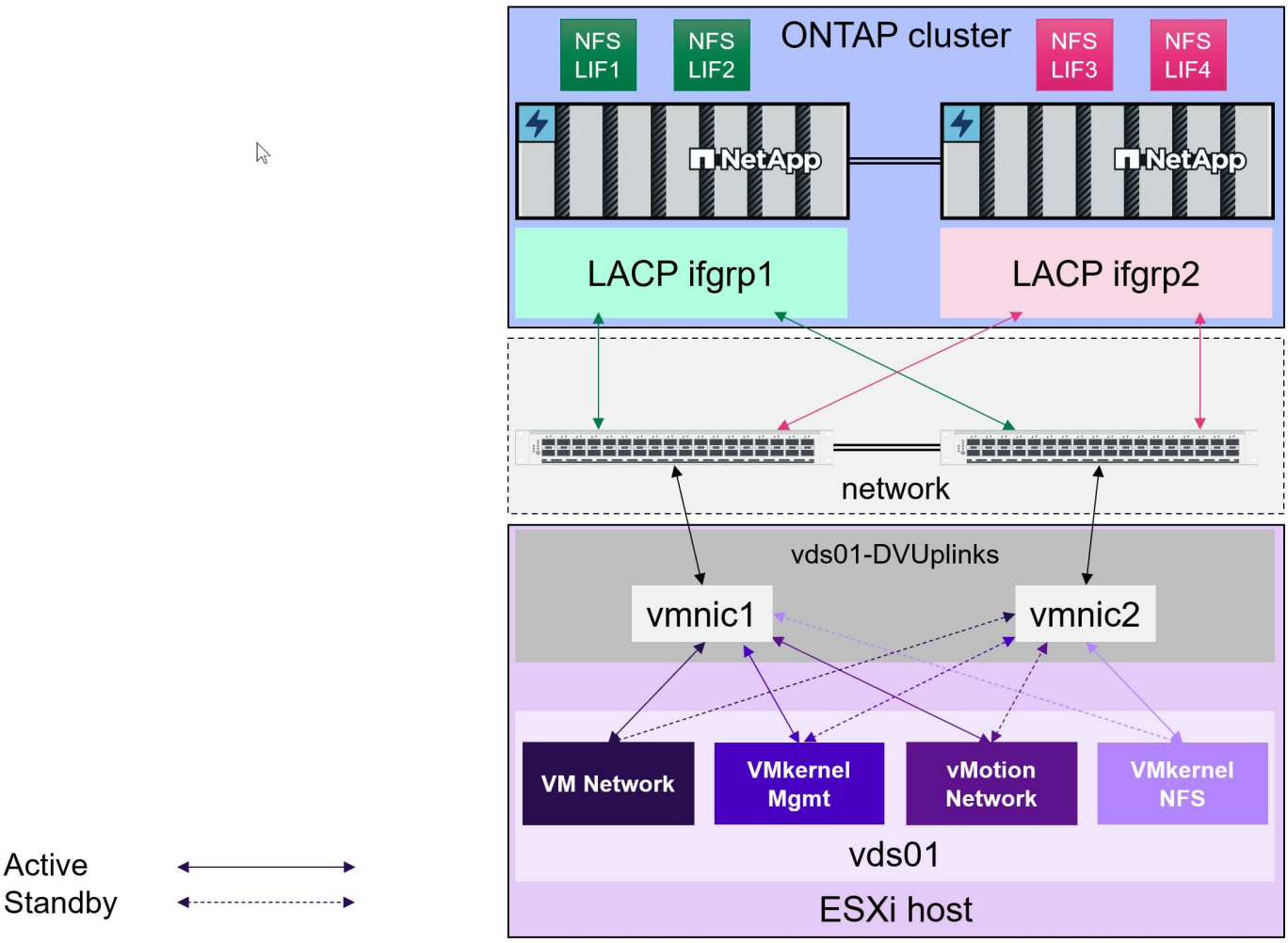
*十分な数のデータLIFがあることを確認してください。*を参照してください "vVolストレージの導入"。

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*



AFF、ASA、ASA R2、FASシステムへのVVOLの導入

仮想マシン用のVVOLストレージを作成する場合は、次のベストプラクティスに従ってください。

vVolデータストアのプロビジョニングはいくつかの手順で行います。NetAppのASA R2システムは、VMwareワークロード向けに設計されており、従来のONTAPシステムとは異なるユーザエクスペリエンスを提供します。ASA R2システムを使用している場合、ONTAP toolsバージョン10.3以降では、セットアップ手順が少なくて済み、新しいストレージアーキテクチャに合わせて最適化されたUI拡張機能とREST APIサポートが提供されます。

ONTAP toolsを使用してvVolデータストアを作成するための準備

すでにONTAPツールを使用して、既存のVMFSまたは従来のNFSベースのストレージの管理、自動化、レポート作成を行っている場合は、導入プロセスの最初の2つの手順を省略できます。ONTAPツールの導入と設定については、この完全版を参照することもできます"チェックリスト"。

1. ストレージ仮想マシン (SVM) とそのプロトコル構成を作成します。ASA r2 システムでは通常、データ サービス用の単一の SVM が既に存在するため、これは必要ありません。NVMe/FC (ONTAPツール 9.13 の

み)、NFSv3、NFSv4.1、iSCSI、FCP、またはこれらのオプションの組み合わせを選択します。NVMe/TCP および NVMe/FC は、 ONTAPツール 10.3 以降を使用した従来の VMFS データストアにも使用できます。ONTAP System Manager ウィザードまたはクラスタ シェル コマンド ラインのいずれかを使用できます。

- "ローカル階層（アグリゲート）をSVMに割り当て"ASA R2以外のすべてのシステム
- 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。NFSベースのVVOLにはノードごとに1つのLIFで十分ですが、このLIFはLACP ifgroupで保護する必要があります。詳細については、およびを "物理ポートを組み合わせてインターフェイスグループを作成"参照して "LIFの設定の概要"ください。
- テナント vCenter に SVM スコープの認証情報を使用する場合は、SVM ごとに少なくとも 1 つの管理 LIF が必要です。
- SnapMirrorを使用する場合は、ソースとターゲットを確認して "ONTAPクラスタとSVMのピア関係が設定されている"ください。
- ASA r2 以外のシステムでは、この時点でボリュームを作成できますが、 ONTAPツールの *Provision Datastore* ウィザードを使用してボリュームを作成するのがベスト プラクティスです。このルールの唯一の例外は、VMware Site Recovery Manager およびONTAPツール 9.13 でvVolsレプリケーションを使用する予定の場合です。これは、既存のSnapMirror関係を持つ既存のFlexVolボリュームを使用すると簡単に設定できます。vVolsに使用されるボリュームでは QoS を有効にしないように注意してください。これは、SPBM およびONTAPツールによって管理されることが意図されています。

2. "ONTAP Tools for VMware vSphereの導入"NetAppサポートサイトからダウンロードしたOVAを使用します。
   - ONTAPツール 10.0 以降では、アプライアンスごとに複数の vCenter サーバーがサポートされるため、vCenter ごとに 1 つのONTAPツール アプライアンスを展開する必要がなくなりました。
     - 複数の vCenter を単一のONTAPツール インスタンスに接続する場合は、CA 署名付き証明書を作成してインストールする必要があります。参照 "証明書の管理" 手順については。
   - 10.3 以降、 ONTAPツールは、ほとんどの非 vVols ワークロードに適した単一ノードの小型アプライアンスとして導入されるようになりました。

- 推奨されるベストプラクティスは "スケールアウトONTAPツール" 10.3 以降では、すべての本番ワークロードに対して 3 ノードの高可用性 (HA) 構成を使用できます。ラボやテストの目的では、単一ノードの展開を使用できます。
- 実稼働環境でのvVols の使用に推奨されるベスト プラクティスは、単一障害点を排除することです。ONTAPツール VM が同じホスト上で一緒に実行されないように、アンチアフィニティ ルールを作成します。初期導入後は、ストレージ vMotion を使用してONTAPツール VM を別のデータストアに配置することもお勧めします。詳細はこちら "vSphere DRSを使用しないアフィニティルールの使用" または "VM-VMアフィニティルールの作成"。また、頻繁にバックアップをスケジュールし、 "組み込みの構成バックアップユーティリティを使用する"。

1. 環境に合わせてONTAP tools 10.3を設定します。
   - "vCenter Serverインスタンスの追加"をクリックしONTAPます。
   - ONTAP tools 10.3ではセキュアマルチテナンシーがサポートされます。セキュアマルチテナンシーが必要ない場合は、vCenterのONTAP toolsメニューに移動して_Storage backends_をクリックし、_add_ボタンをクリックするだけ "ONTAPクラスタを追加"です。
   - セキュアなマルチテナント環境で特定のStorage Virtual Machine（SVM）を特定のvCenterに委譲する

場合は、次の作業を行う必要があります。

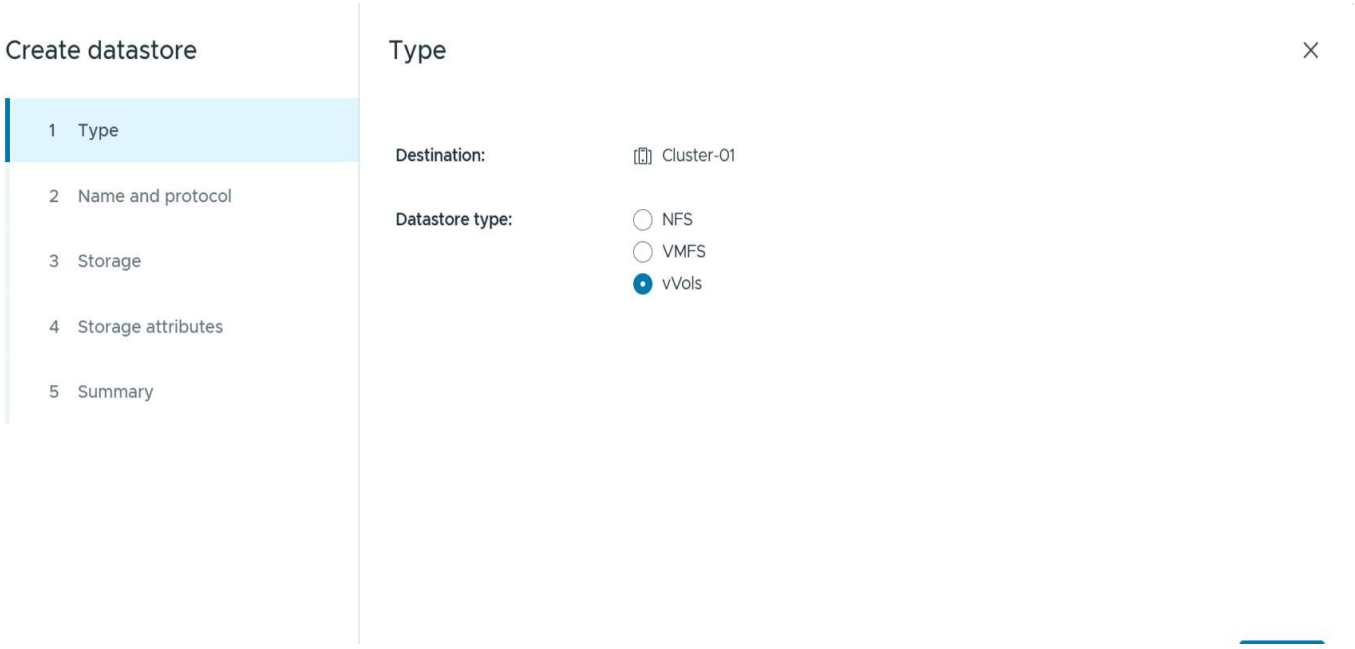
- ONTAP Tools Manager UIにログインします。
- "ストレージクラスタのオンボード"
- "ストレージバックエンドとvCenter Serverインスタンスの関連付け"
- 特定の SVM 認証情報を vCenter 管理者に提供すると、管理者は vCenter のONTAPツールのストレージ バックエンド メニューで SVM をストレージ バックエンドとして追加します。

- ストレージアカウント用のRBACロールを作成することを推奨します。
- ONTAPツールには、 ONTAPツール ストレージ アカウントに必要なロール権限を含む JSON ファイルが含まれています。JSON ファイルをONTAP System Manager にアップロードすると、RBAC ロールとユーザーの作成が簡素化されます。
- ONTAP RBACロールの詳細については、を参照してください "ONTAPユーザのロールと権限の設定"。

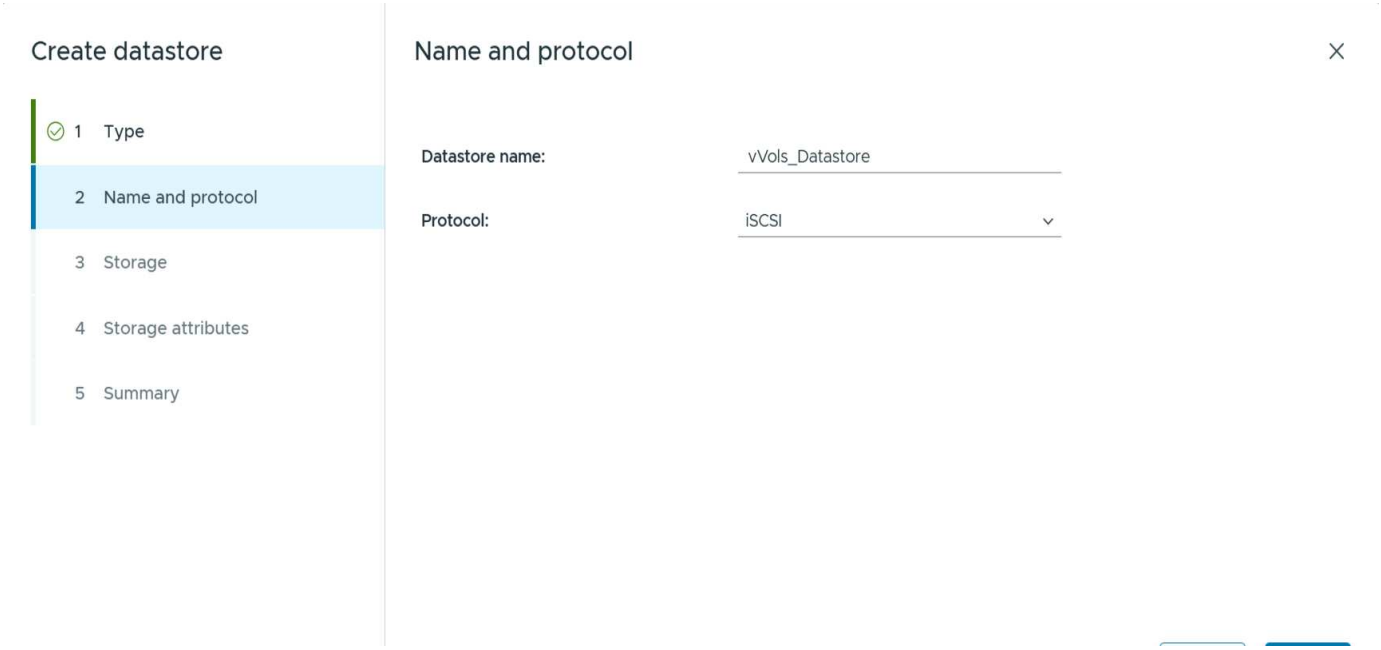
クラスタ全体をONTAPツール マネージャ UI にオンボードする必要がある理由は、 vVolsに使用される API の多くがクラスタ レベルでのみ使用できるためです。

ONTAP toolsを使用した**vVol**データストアの作成

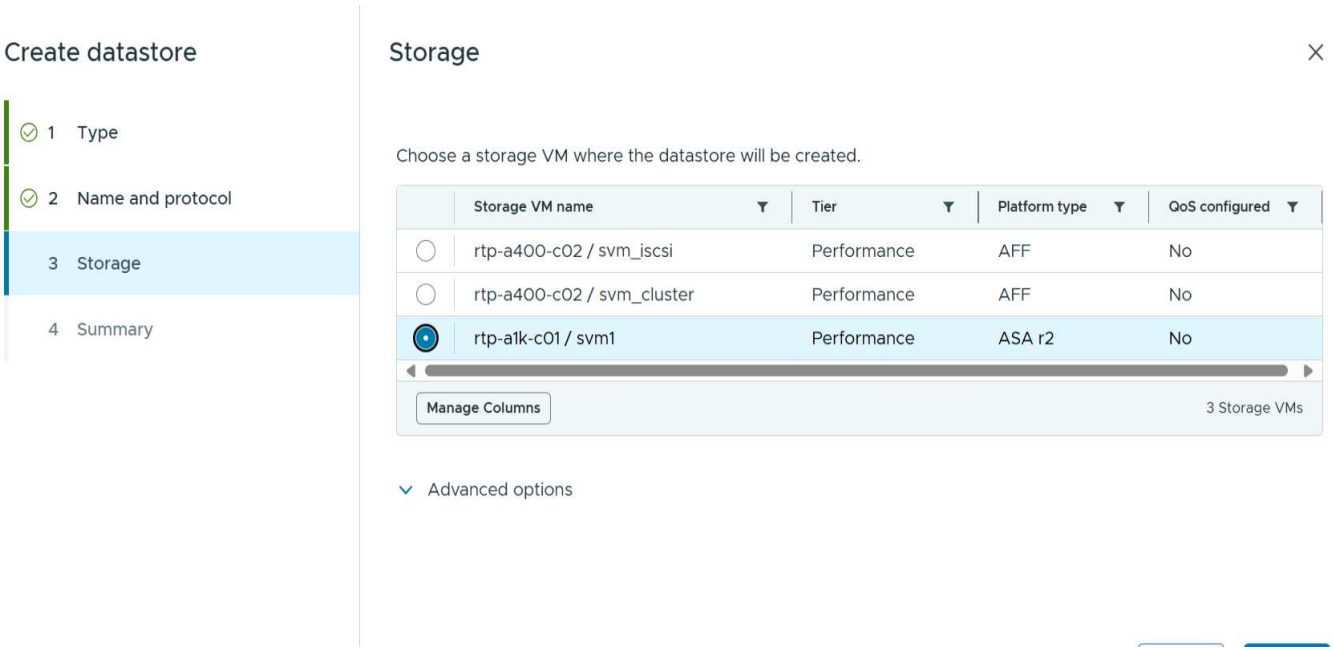
ONTAP データストアを作成するホスト、クラスタ、またはデータセンターを右クリックし、_vVol tools>>_Provision Datastore_を選択します。



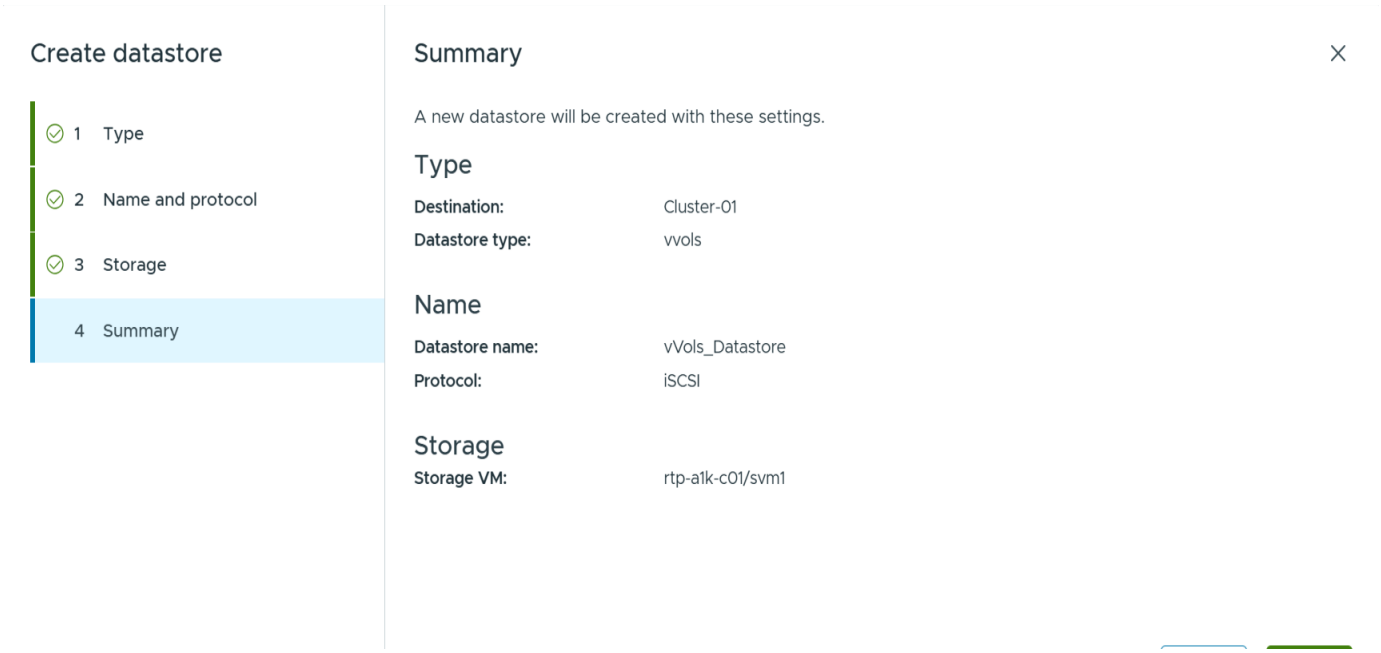
- [VVols]を選択し、わかりやすい名前を指定してプロトコルを選択します。データストアの概要 も指定できます。
  - ASA R2搭載のONTAP tools 10.3。



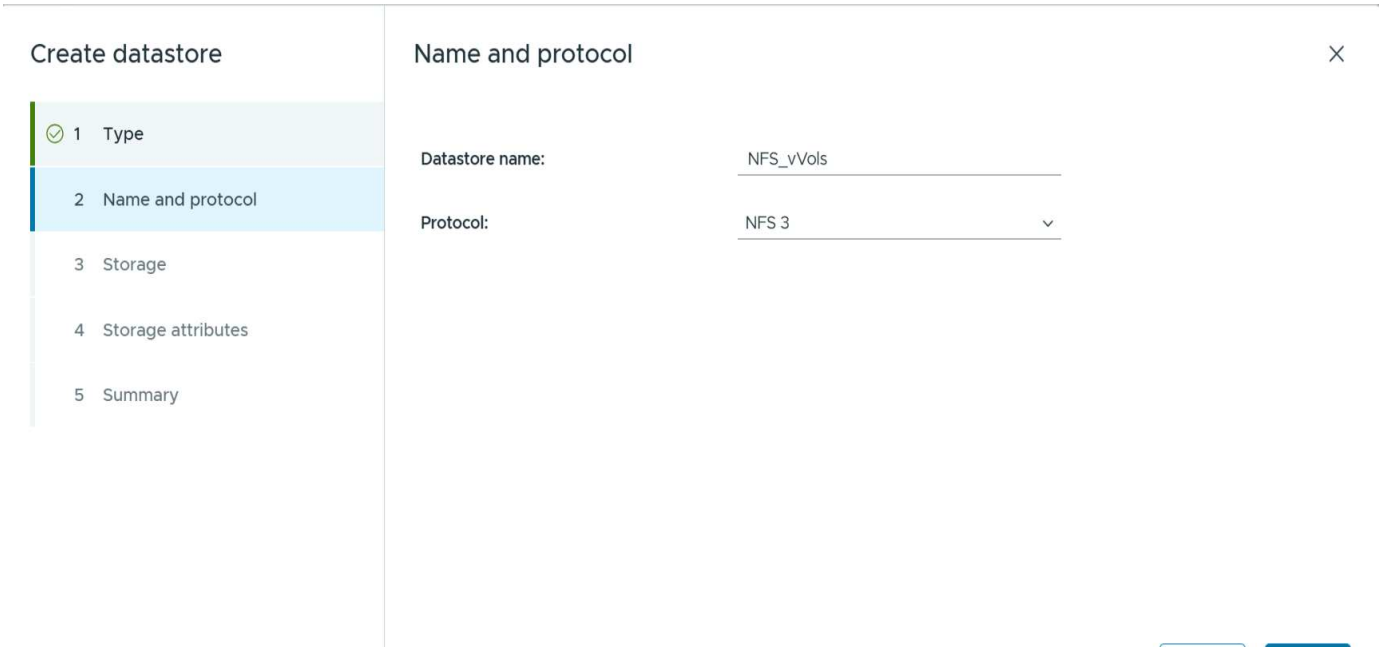
- ASA R2システムSVMを選択し、_next_をクリックします。



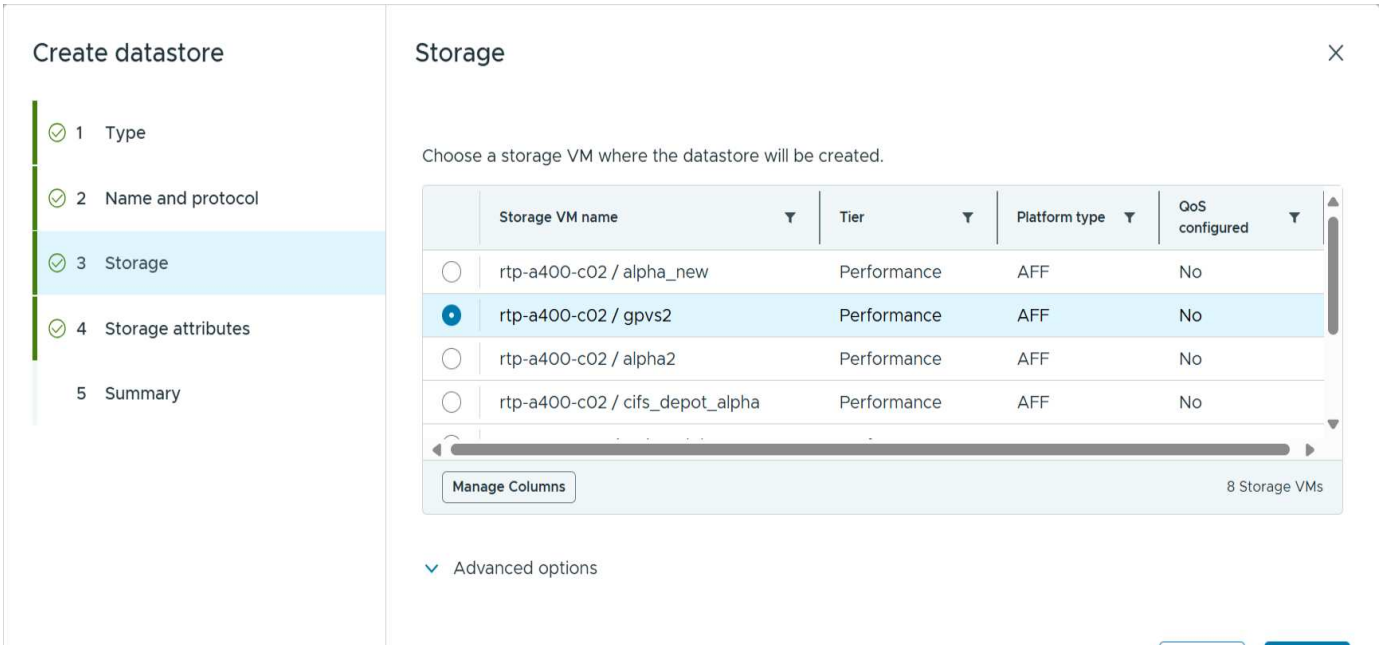
- [終了]をクリックします。



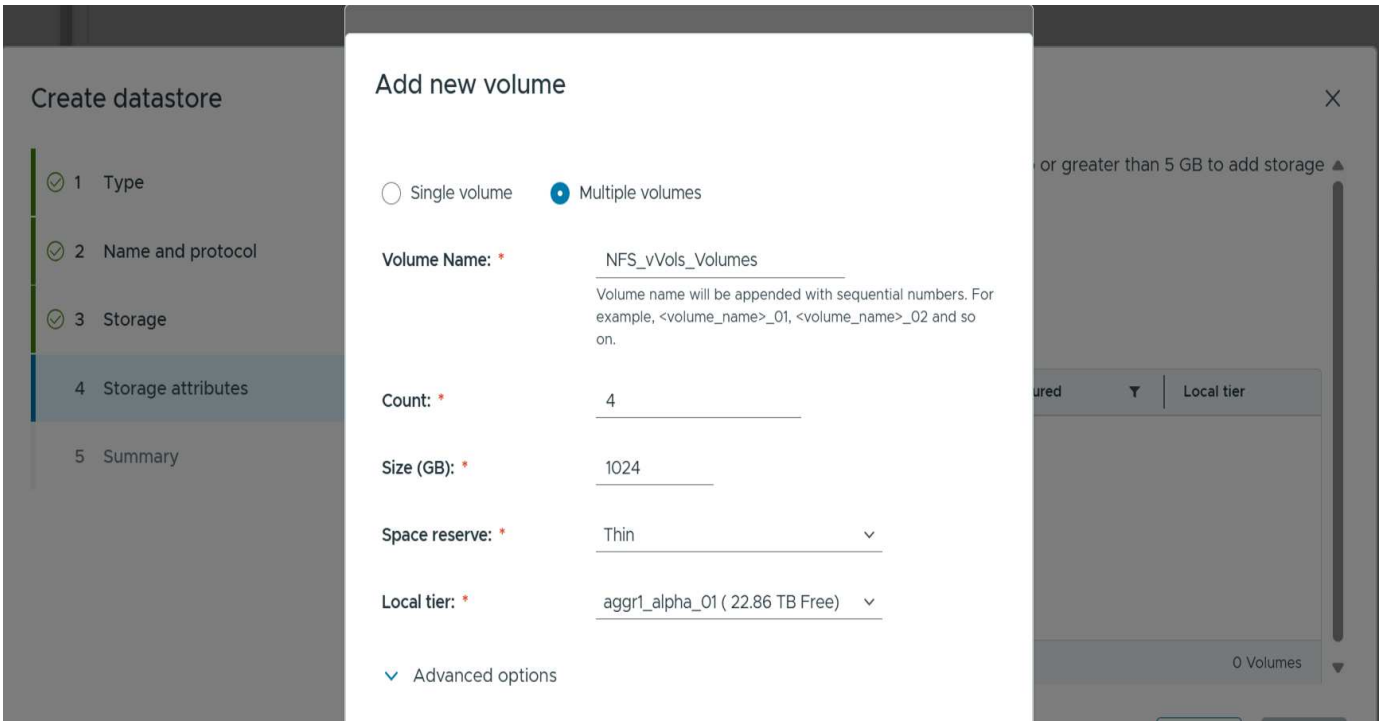
- それは簡単です!
  - ONTAPツール 10.3 とONTAP FAS、 AFF 、およびASA r2 より前のASA 。
- プロトコルを選択してください

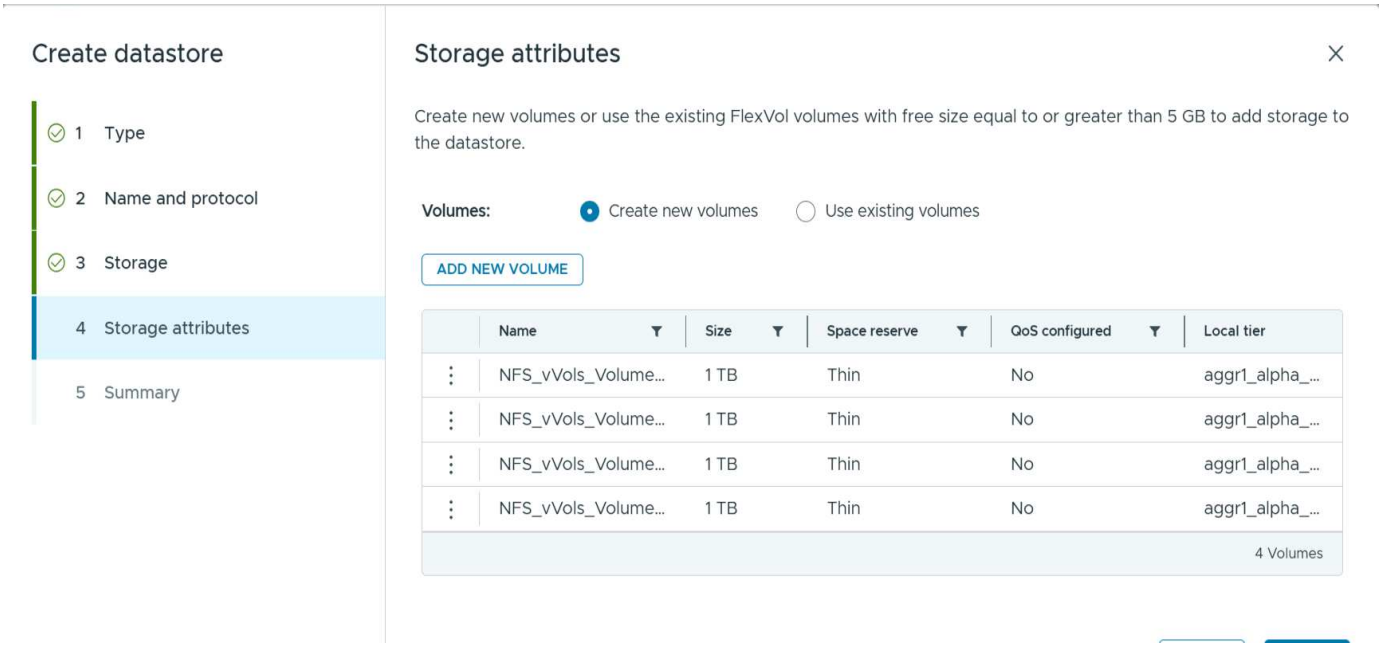


- SVMを選択し、_next_をクリックします。

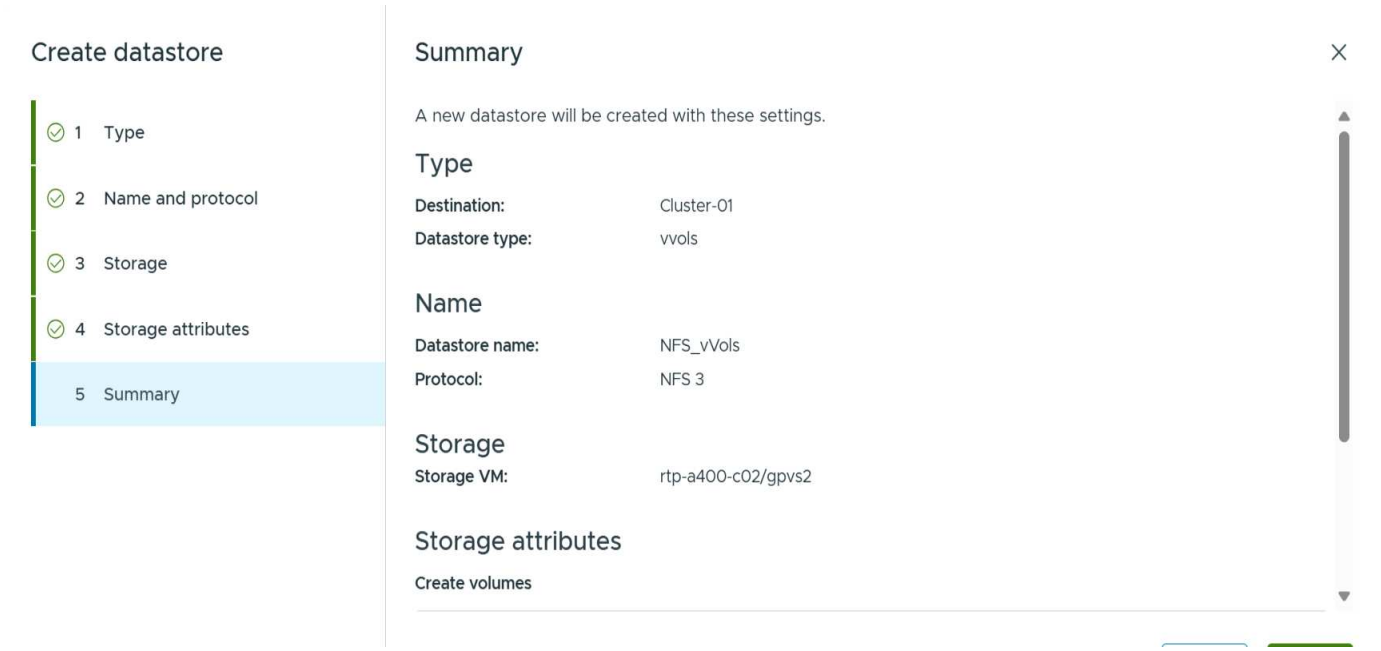


- [新しいボリュームを追加] または [既存のボリュームを使用] をクリックして、属性を指定します。ONTAPツール 10.3 では、複数のボリュームを同時に作成するように要求できることに注意してください。また、複数のボリュームを手動で追加して、 ONTAPクラスタ全体でバランスをとることもできます。「次へ」をクリック

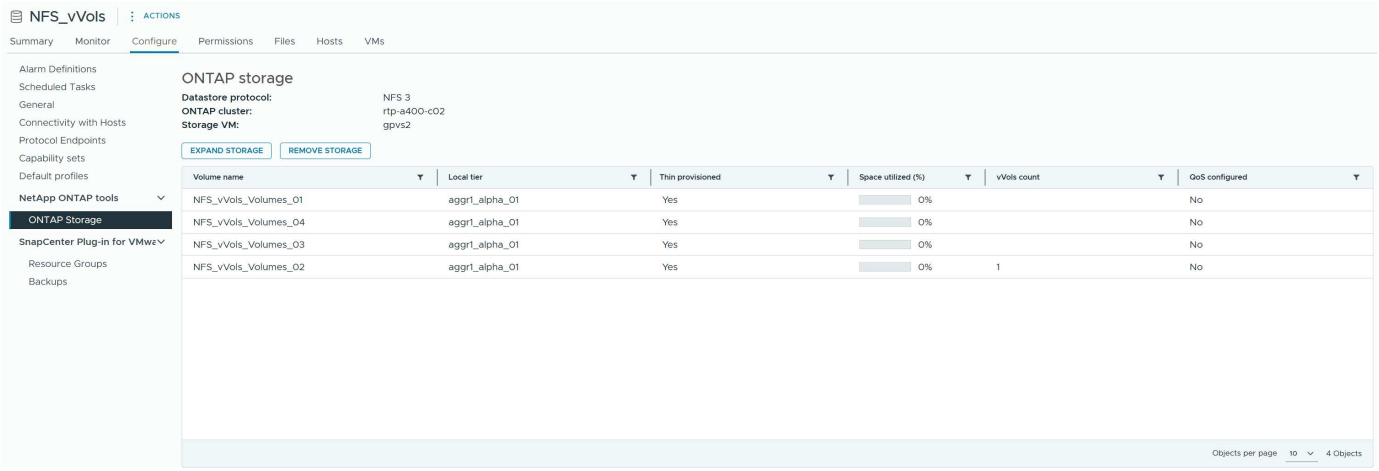




- [終了]をクリックします。



- 割り当てられているボリュームは、データストアの[Configure]タブのONTAP tools]メニューで確認できます。



- vCenter UIの_PoliciesとProfiles_menuからVMストレージポリシーを作成できるようになりました。

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。プロンプトが表示されたら、vVolデータストアに一致するVMストレージポリシーを選択します。移行コピー処理は、vSphere 6.0以降でSAN VMFSをvVolに移行する場合はオフロードできますが、NAS VMDKからvVolにはオフロードできません。

ポリシーによる**VM**の管理

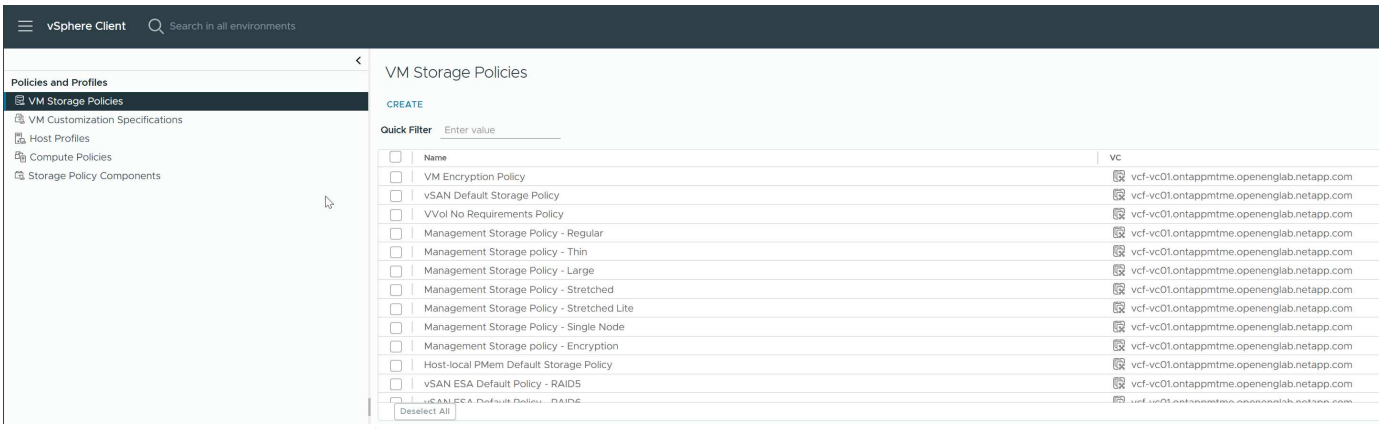
ポリシーベースの管理を使用してストレージ プロビジョニングを自動化するには、必要なストレージ機能にマップする VM ストレージ ポリシーを作成する必要があります。

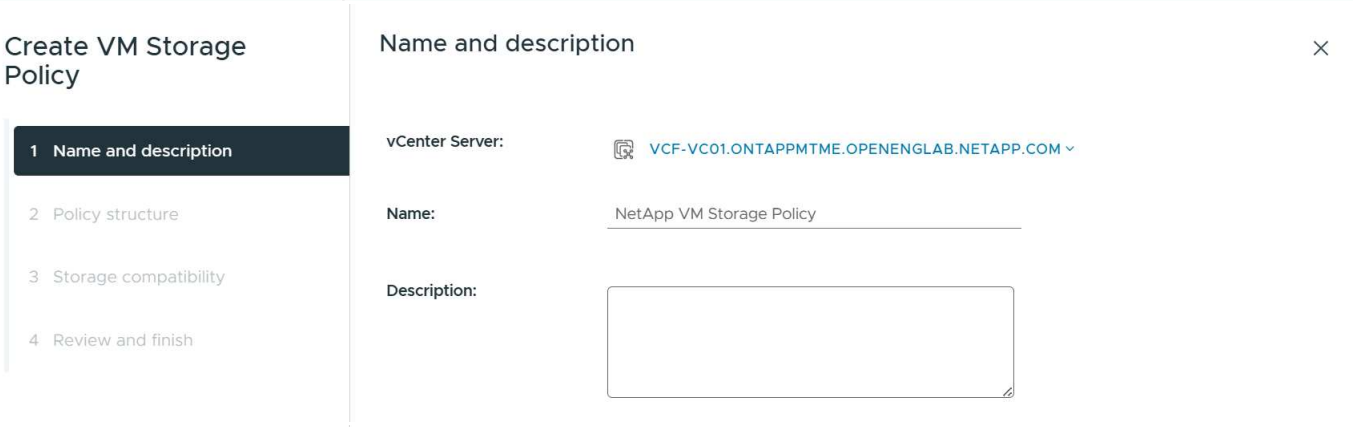
ONTAP tools 10.0以降では、以前のバージョンのようなストレージ機能プロファイルは使用されなくなりました。代わりに、ストレージ機能はVMストレージポリシー自体で直接定義されます。

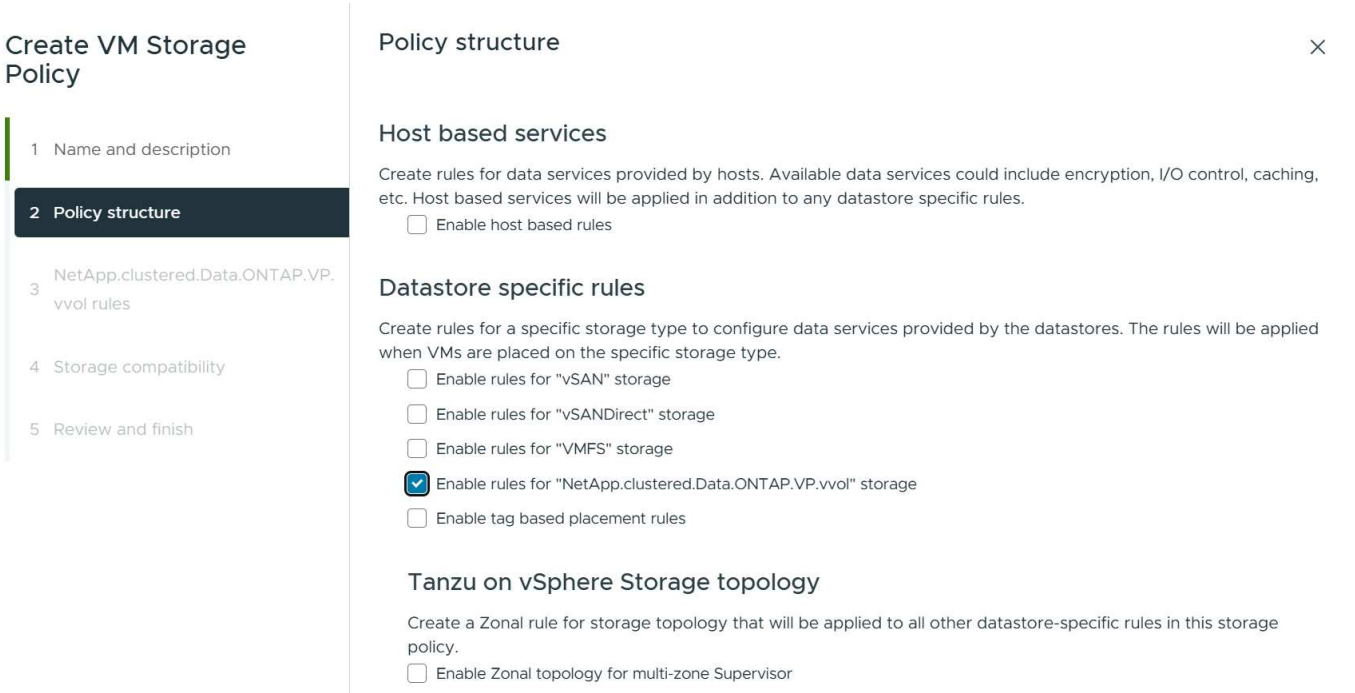
仮想マシンストレージポリシーを作成しています

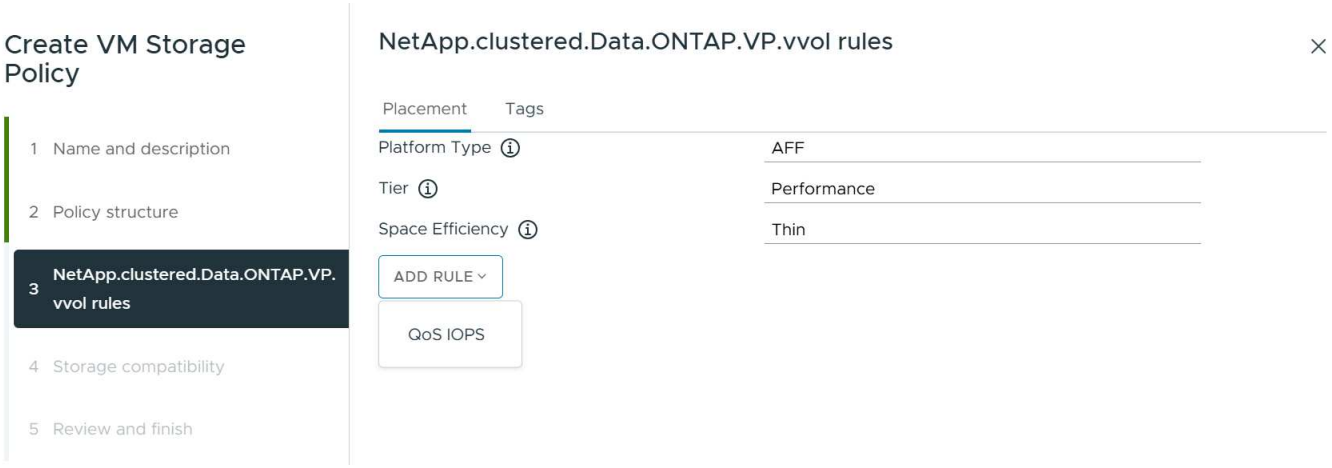
VM ストレージ ポリシーは、vSphere でストレージ I/O コントロールや vSphere 暗号化などのオプション機能を管理するために使用されます。また、 vVolsと組み合わせて使用して、VM に特定のストレージ機能を適用することもできます。「NetApp.clustered.Data. ONTAP .VP.vvol」ストレージ タイプを使用します。ONTAPツール VASA Provider を使用した例については、link:vmware-vvols-ontap.html#Best Practices[NFS v3 経由のvVolsを使用したネットワーク構成の例] を参照してください。「NetApp.clustered.Data. ONTAP.VP.VASA10」ストレージのルールは、非 vVols ベースのデータストアで使用されます。

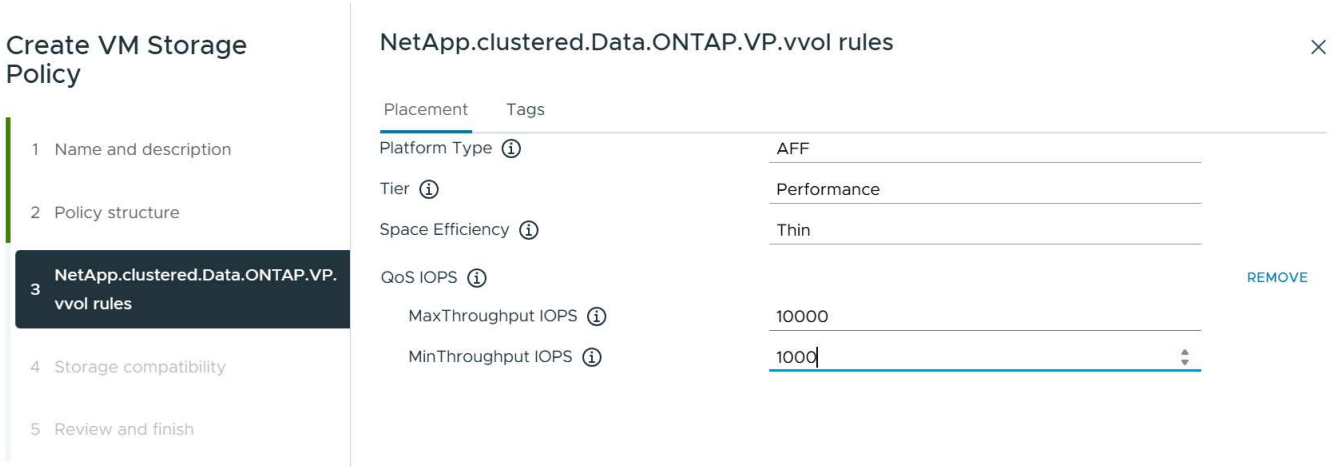
作成したストレージポリシーは、新しいVMのプロビジョニングに使用できます。

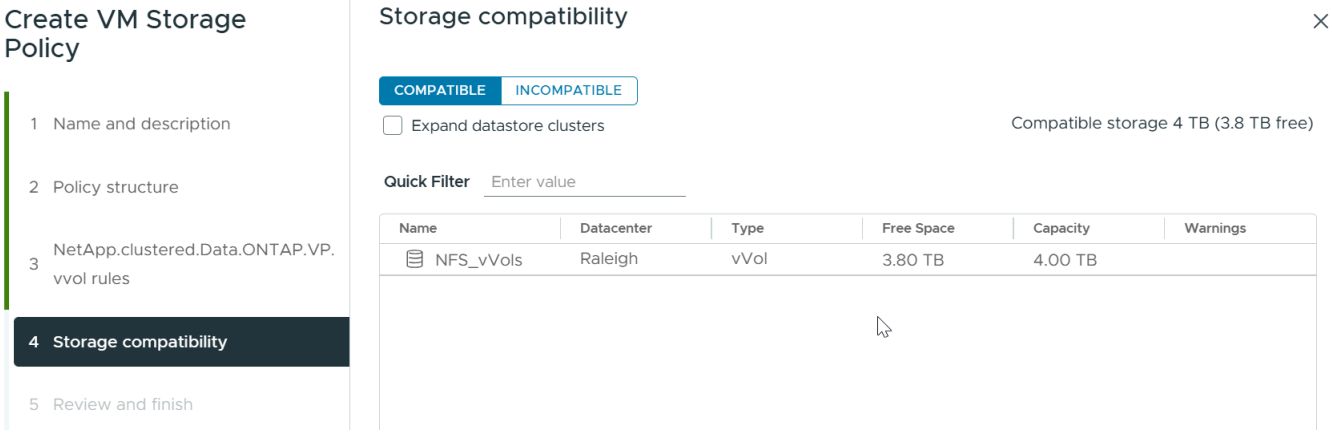

vSphere Client
Search in all environments
Policies and Profiles
VM Storage Policies
VM Customization Specifications
Host Profiles
Compute Policies
Storage Policy Components
VM Storage Policies
CREATE
Quick Filter
Enter value
Name
VC
VM Encryption Policy
vSAN Default Storage Policy
VVol No Requirements Policy
Management Storage Policy - Regular
Management Storage policy - Thin
Management Storage Policy - Large
Management Storage Policy - Stretched
Management Storage Policy - Stretched Lite
Management Storage Policy - Single Node
Management Storage policy - Encryption
Host-local PMem Default Storage Policy
vSAN ESA Default Policy - RAID5
vcf-vc01.ontappmtme.openenglab.netapp.com
Deselect All

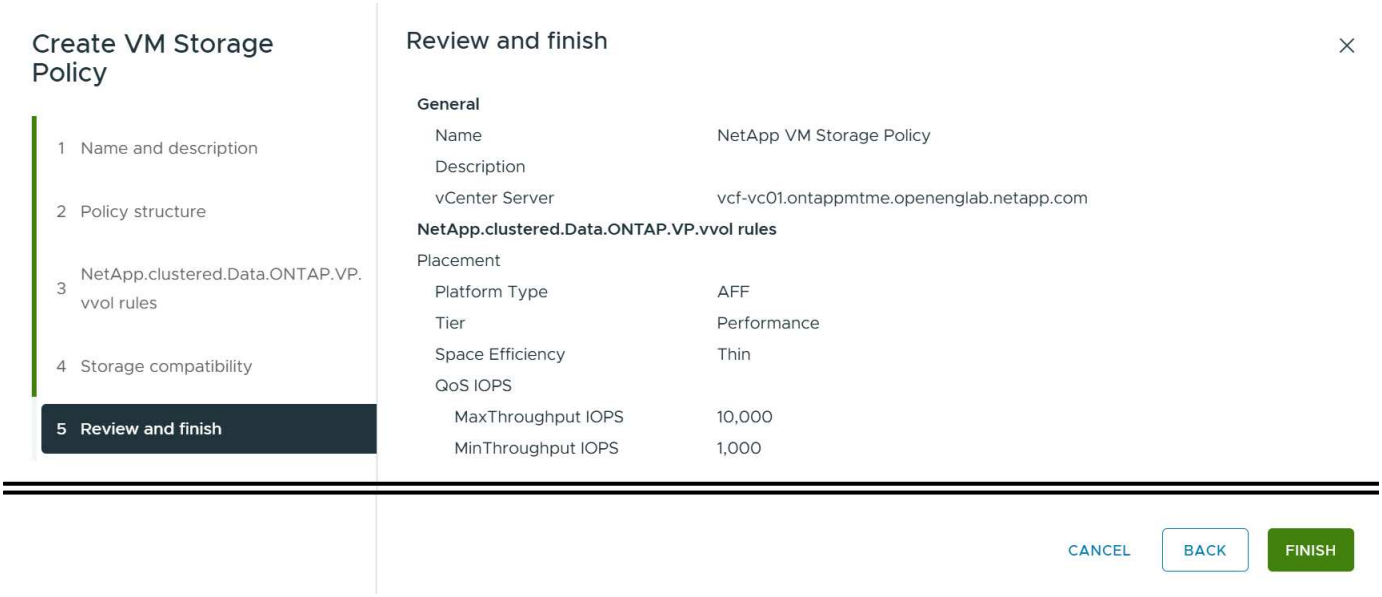

Create VM Storage Policy
1 Name and description
2 Policy structure
3 Storage compatibility
4 Review and finish
Name and description
vCenter Server:
VCF-VC01.ONTAPPMTME.OPENENGLAB.NETAPP.COM
Name:
NetApp VM Storage Policy
Description:


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Policy structure
Host based services
Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.
Enable host based rules
Datastore specific rules
Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.
Enable rules for "vSAN" storage
Enable rules for "vSANDirect" storage
Enable rules for "VMFS" storage
Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
Enable tag based placement rules
Tanzu on vSphere Storage topology
Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.
Enable Zonal topology for multi-zone Supervisor


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
ADD RULE
QoS IOPS


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
QoS IOPS
REMOVE
MaxThroughput IOPS
10000
MinThroughput IOPS
1000


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Storage compatibility
COMPATIBLE
INCOMPATIBLE
Expand datastore clusters
Compatible storage 4 TB (3.8 TB free)
Quick Filter
Enter value
Name
Datacenter
Type
Free Space
Capacity
Warnings
NFS_vVols
Raleigh
vVol
3.80 TB
4.00 TB



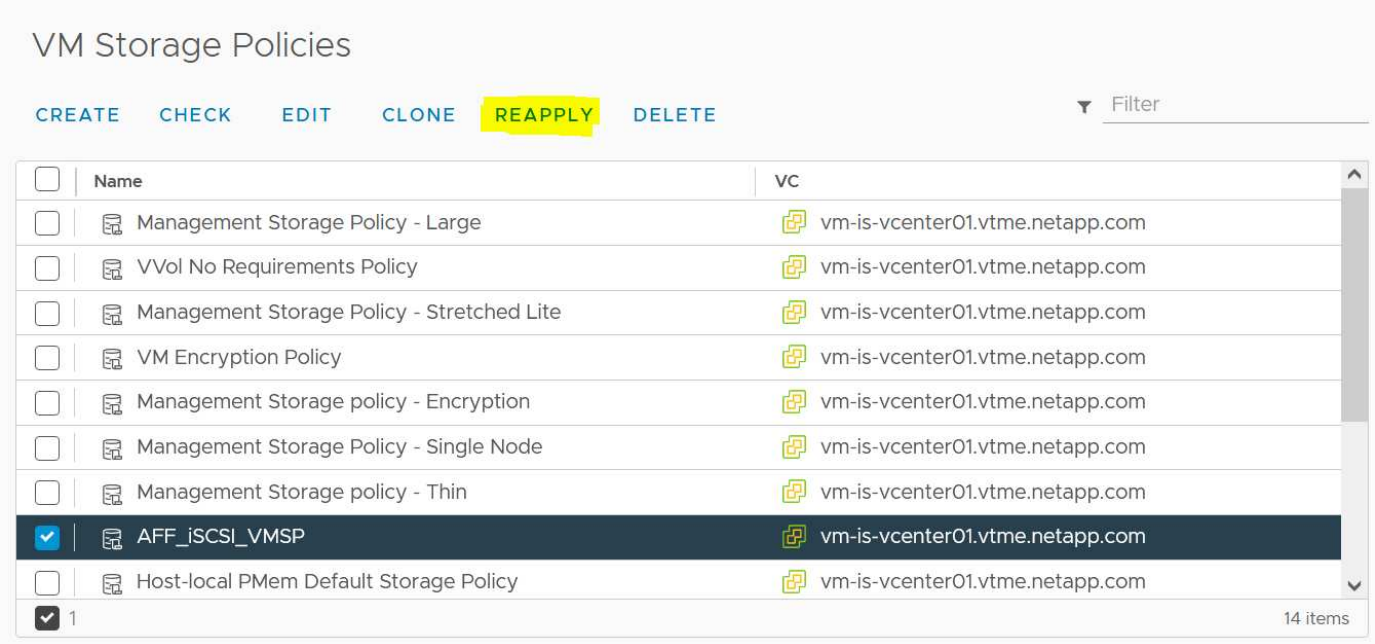
ONTAPツールによるパフォーマンス管理

ONTAP toolsは、独自の分散配置アルゴリズムを使用して、統合または従来のASAシステムを使用する最適なFlexVol volume、またはASA R2システムを使用するストレージアベイラビリティゾーン（SAZ）をvVolデータストア内に配置します。配置は、元のストレージとVMストレージポリシーの照合に基づいて行われます。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VMポリシーで指定できます。
  - ポリシー内の IOPS を変更しても、それを使用する VM に VM ポリシーが再適用されるまで、 vVols の QoS は変更されません。または、必要な IOPS で新しいポリシーを作成し、それをターゲット VM に適用することもできます。一般的には、異なるサービス層ごとに個別の VM ストレージ ポリシーを定義し、VM 上の VM ストレージ ポリシーを変更することが推奨されます。
  - ASA、 ASA r2、 AFF、およびFASパーソナリティには異なる IOP 設定があります。すべてのフラッシュ システムでは Min と Max の両方が使用できますが、 AFF以外のシステムでは Max IOP 設定のみを使用できます。
- 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。

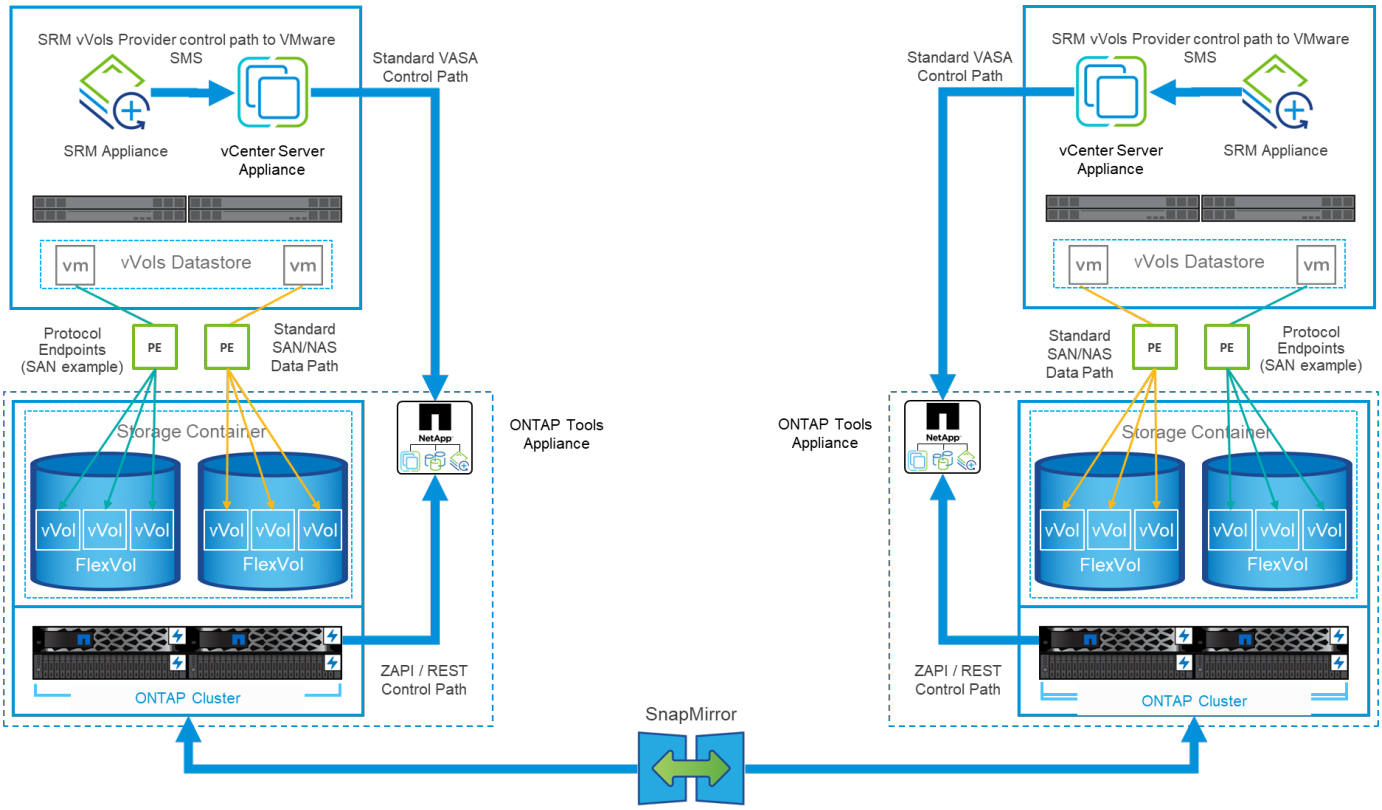
このソフトウェアツールの要件は、vVolレプリケーションの管理においてさらに重要になります。一部の機能はネイティブの機能で管理できます（たとえば、VMwareが管理するvVolのSnapshotは、高速で効率的なファイルクローンまたはLUNクローンを使用するONTAP にオフロードされます）が、一般的には、レプリケーションとリカバリを管理するためにオーケストレーションが必要です。VVOLに関するメタデータは、ONTAP とVASA Providerによって保護されますが、セカンダリサイトでメタデータを使用するには追加の処理が必要です。

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ボリュームを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、事前に作成して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。

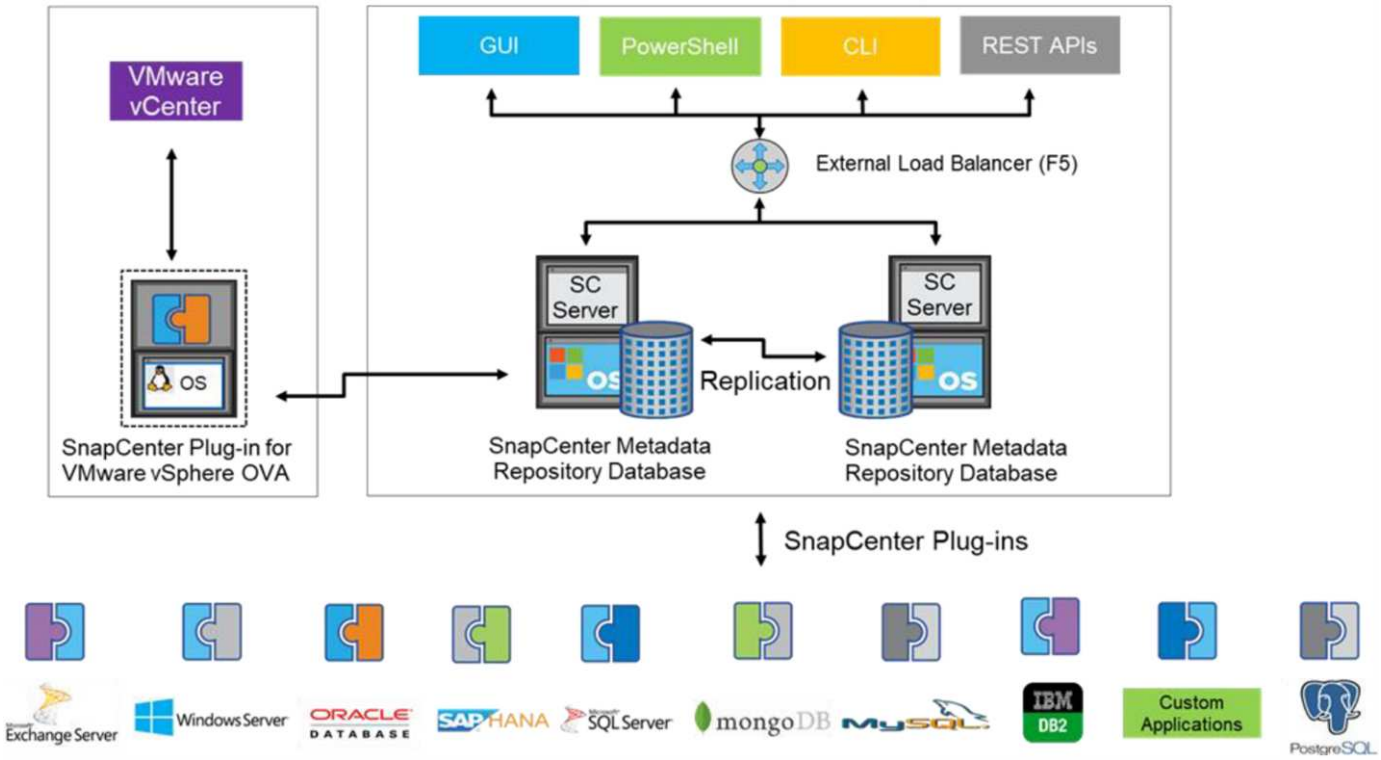
vSphere 8.0のサポートは、分離されたローカルプラグインアーキテクチャを使用するSCV 4.7で導入されました。vSphere 8.0U1のサポートがSCV 4.8に追加され、新しいリモートプラグインアーキテクチャに完全に移行しました。

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"

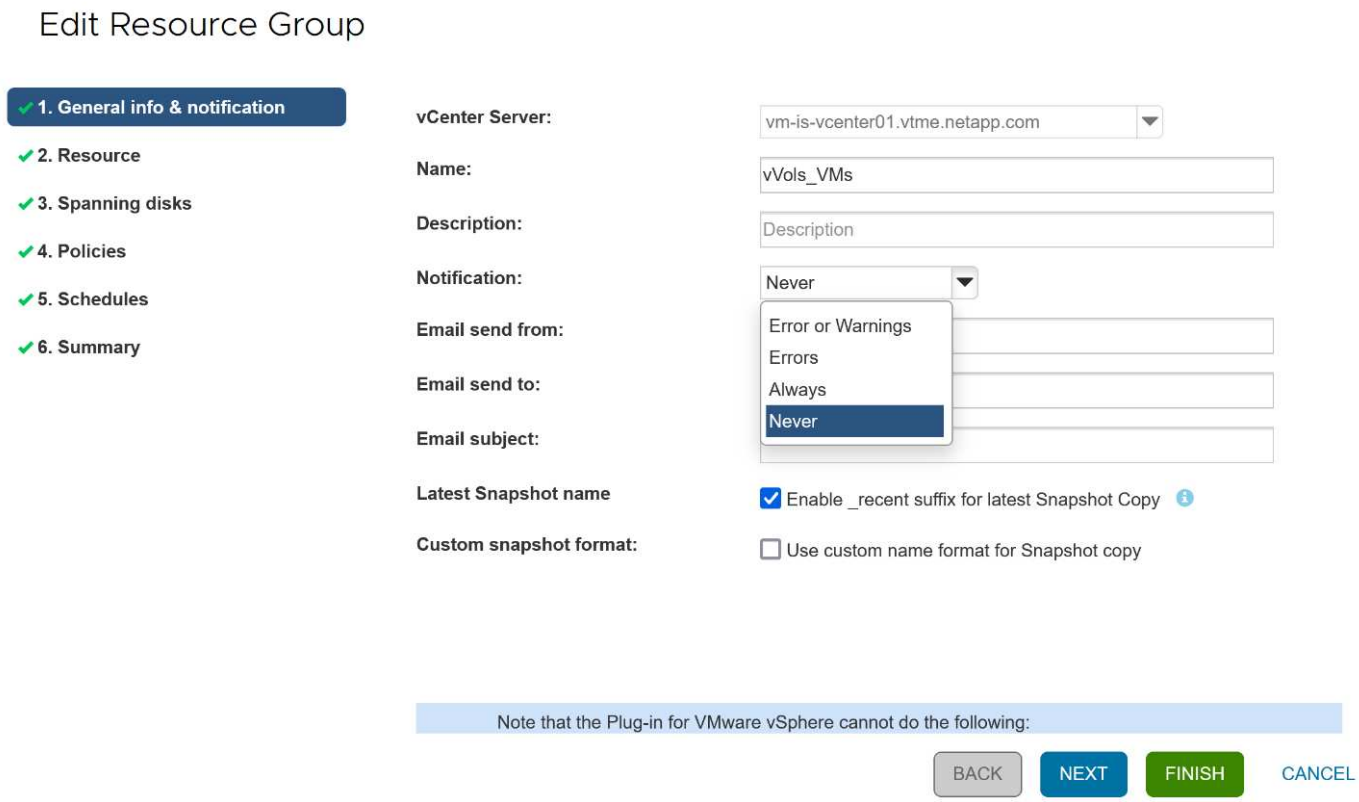
SnapCenter Plug-in for VMware vSphere REST API については、を参照してください "SnapCenter Plug-in for VMware vSphere REST API"

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サポートサイトでは、NetApp仮想化製品に関するさまざまなナレッジベース記事に加えて、製品の便利なランディングページも提供して "VMware vSphere 用の ONTAP ツール"います。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。

"*BroadcomによるVMwareによる仮想化向けNetApp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

ONTAPを使用したVMwareライブサイトリカバリ

20 年以上前に ESX が最新のデータセンターに導入されて以来、 ONTAP はVMware vSphere、そして最近では Cloud Foundation の主要なストレージ ソリューションとなっています。 NetApp は、 SnapMirrorアクティブ シンクなどの機能とともに、最新世代のASA A シリーズなどの革新的なシステムを継続的に導入しています。これらの進歩により、管理が簡素化され、回復力が強化され、IT インフラストラクチャの総所有コスト (TCO) が削減されます。

このドキュメントでは、VMware の業界をリードする災害復旧 (DR) ソフトウェアである VMware Live Site Recovery (VLSR) (旧称 Site Recovery Manager (SRM)) のONTAPソリューションについて紹介します。これには、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するための最新の製品情報とベスト プラクティスが含まれます。

> このドキュメントは、以前に公開された技術レポート_TR-4900: VMware Site Recovery Manager with ONTAP_に代わるものです。

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 10.4（NetApp Storage Replication Adapter[SRA]およびVASA Provider[VP]を含む）およびVMware Live Site Recovery 9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について説明します。

VLSRまたはSRMでONTAPを使用する理由

ONTAPを搭載したNetAppデータ管理プラットフォームは、VLSR で最も広く採用されているストレージ ソリューションの 1 つです。理由はたくさんあります。業界をリードするストレージ効率、マルチテナント、サービス品質の制御、スペース効率の高いスナップショットによるデータ保護、 SnapMirrorによるレプリケーションを提供する、安全で高性能な統合プロトコル (NAS と SAN の組み合わせ) のデータ管理プラットフォームです。これらすべては、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て VMware ワークロードを保護し、豊富な自動化およびオーケストレーション ツールを簡単に利用できるようにします。

アレイベースのレプリケーションにSnapMirror を使用すると、ONTAP の最も実績があり成熟したテクノロジの 1 つを活用できます。 SnapMirror を使用すると、VM 全体または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することで、安全で効率の高いデータ転送が可能になります。これらのブロックでも、重複排除、圧縮、コンパクト化などのスペース節約が活用されます。最新のONTAPシステムでは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 クラスターと宛先クラスターを柔軟に選択できるようになりました。 SnapMirror は、災害復旧に利用できる最も強力なツールの 1 つになりました。

従来の NFS、iSCSI、またはファイバ チャネル接続データストア (vVolsデータストアもサポートされるようになりました) を使用している場合でも、VLSR は、災害復旧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の機能を最大限に活用する強力なファーストパーティ製品を提供します。

VLSR での ONTAP 9 の活用方法

VLSR 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。

- ONTAP tools vCenterプラグイン（旧称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を簡易化し、可用性を高め、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、 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。NetAppでは、ONTAPを実行しているシステムでvSphereを使用する際に、これらのメリットをすべて考慮してこのプラグインを推奨しています。
- ONTAP tools VASA Providerは、VMware vStorage APIs for Storage Awareness（VASA）フレームワークをサポートします。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。これにより、VMware Virtual Volumes（vVol）のサポート、VM ストレージポリシーの管理、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した。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。
- SRA は VLSR 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。SRAサーバアプライアンスと、Windows SRMサーバおよびVLSRアプライアンス用のSRAアダプタの両方が含まれています。

非 vVols データストアを保護するために VLSR サーバーに SRA アダプタをインストールして構成したら、災害復旧用に vSphere 環境を構成するタスクを開始できます。

SRAは、VMware仮想マシン（VM）を含むONTAP FlexVolボリュームおよびそれらを保護するSnapMirrorレプリケーションを管理するためのVLSRサーバ用のコマンドおよび制御インターフェイスを提供します。

VLSR は、NetApp 独自のFlexCloneテクノロジーを使用して DR サイトの保護されたデータストアのクローンをほぼ瞬時に作成し、中断なく DR プランをテストできます。 VLSR は、実際の災害発生時に組織と顧客が保護されるように安全にテストするためのサンドボックスを作成し、災害時に組織がフェールオーバーを実行できることに自信を持たせます。

実際に災害が発生した場合や、計画的な移行の場合でも、 VLSR 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。

> ONTAPシステムではSnapMirrorレプリケーション用に同じクラスタ内のSVMをペアリングできますが、このシナリオのテストおよび認定はVLSRでは行われていません。したがって、VLSRを使用する場合は、異なるクラスタのSVMのみを使用することを推奨します。

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

VLSR 展開をONTAP の高度なデータ管理機能と統合すると、ローカル ストレージ オプションと比較して、スケールとパフォーマンスが大幅に向上します。しかし、それ以上に、ハイブリッド クラウドの柔軟性がもたらされます。ハイブリッド クラウドでは、 FabricPoolを使用して、高性能アレイから使用されていないデータ ブロックを優先ハイパースケーラー (NetApp StorageGRIDなどのオンプレミスの S3 ストアなど) に階層化することでコストを節約できます。また、ソフトウェア定義のONTAP SelectまたはクラウドベースのDRを備えたエッジベースのシステムにもSnapMirrorを使用できます。 "Equinix Metal 上のNetAppストレージ"、またはその他のホストされたONTAPサービス。

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。

VLSR 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。

最新バージョンの**ONTAP tools**を使用する**10**

ONTAP tools 10では、以前のバージョンに比べて次の点が大幅に改善されています。

- テストフェイルオーバーが8倍高速*
- クリーンアップと再保護が2倍高速*
- フェイルオーバーが32%高速*
- 拡張性の向上
- 共有サイトレイアウトのネイティブサポート

*これらの改善点は内部テストに基づいており、環境によって異なる場合があります。

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。

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ユーザのロールと権限の設定"含まれているJSONファイルを使用します。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。
- 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マイクロサービスであるため、ONTAP toolsのvCenter UIで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、最初にONTAP tools Managerを使用してvCenterに関連付けないかぎり、NFSパスのチェックは実行されませ "オンホオトクラスタ"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を使用し、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。
- 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。これは今でもベストプラクティスですが、最新バージョンのONTAP 9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でSnapMirrorスナップショットが削除され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。

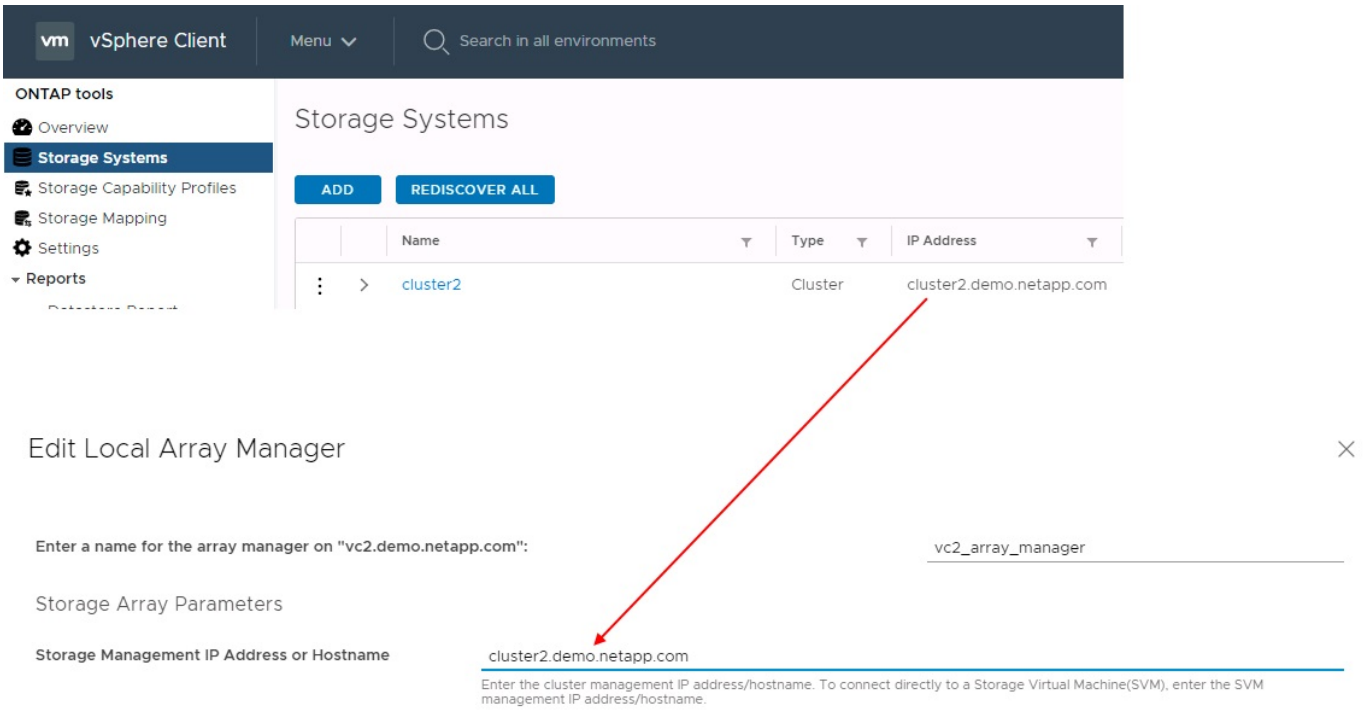
```
snap autodelete modify -volume -commitment try
```

- ボリュームのオートサイズは、SANデータストアを含むボリュームの場合は `grow_shrink`に設定し、NFSデータストアの場合はに設定する必要があります `grow`。このトピックの詳細については、を"ボリュームのサイズを自動的に拡張および縮小するように設定する"参照してください。
- 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。

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。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、SnapMirrorではアグリゲートの重複排除が考慮されていないため、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は、アプリケーションサーバの前にオンラインである必要があるMicrosoft SQL Serverよりも先に起動する必要があります。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した場合は、必ずテストフェイルオーバーを実行することを推奨します。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。

各NetApp SVM は、Site Recovery Manager では一意のアレイとして扱われます。VLSR は、特定のアレイ間 (または SVM 間) のレプリケーション レイアウトをサポートします。

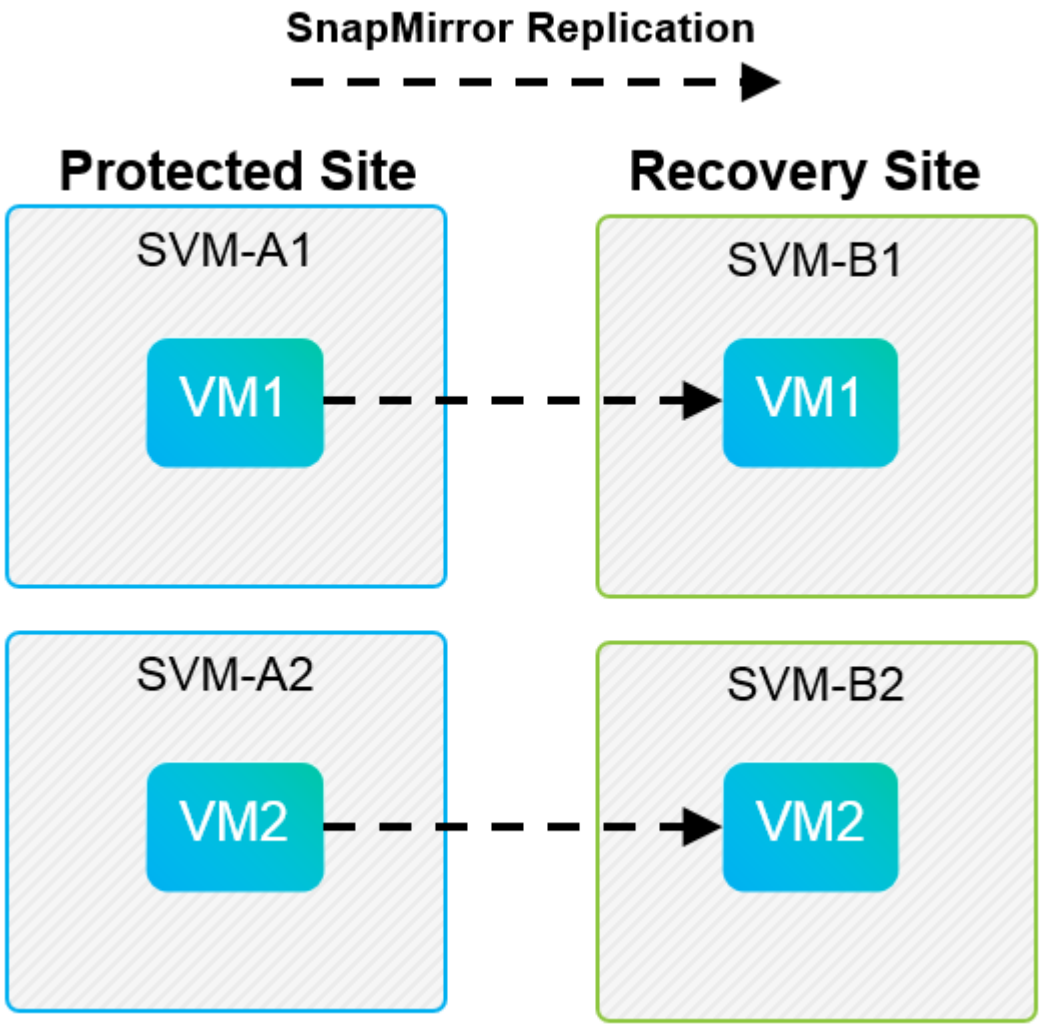
1 つの VM が、次の理由から、複数の VLSR アレイ上で仮想マシンディスク（ VMDK ）または RDM を所有することはできません。

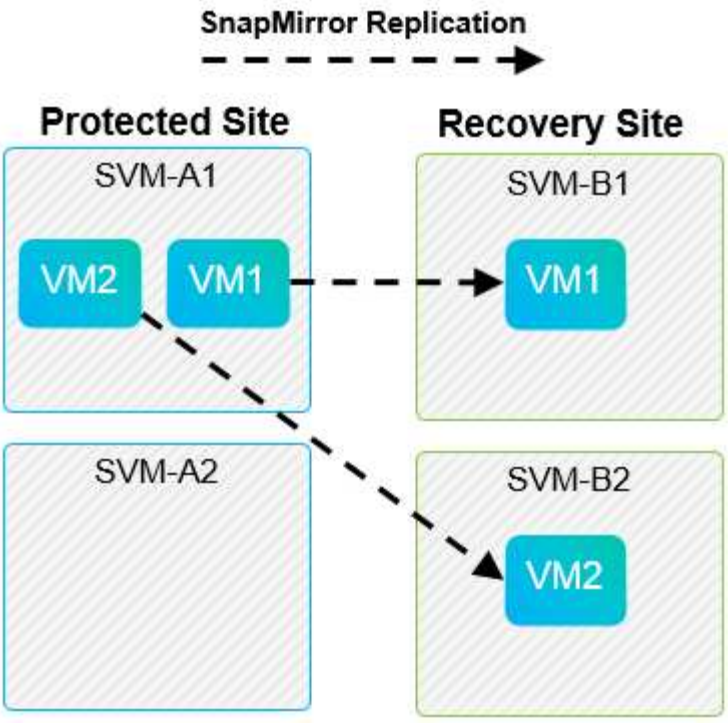
- VLSR は SVM のみを認識し、個々の物理コントローラは認識しません。
- SVM は、クラスタ内の複数のノードにまたがる LUN とボリュームを制御できます。

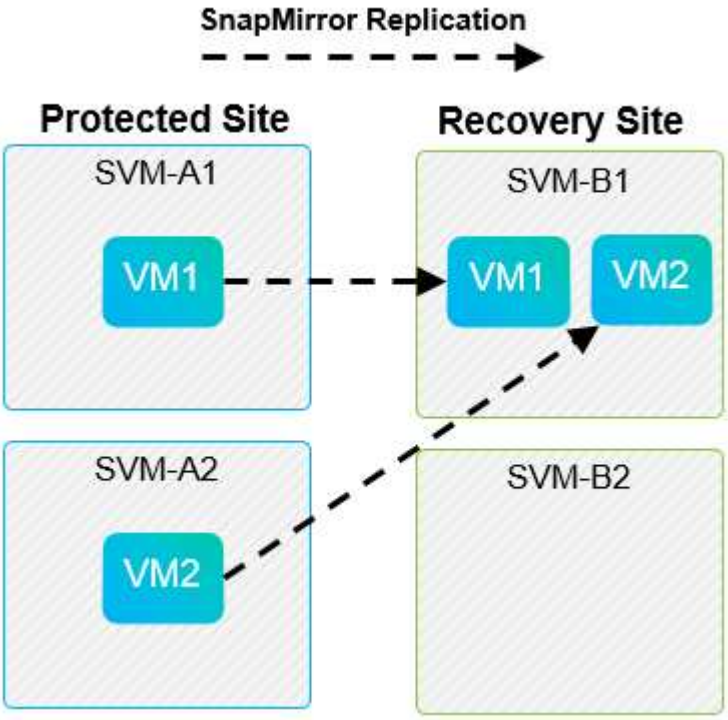
ベストプラクティス
サポートされるかどうかを判断するには、このルールに注意してください。 VLSR と NetApp SRA を使用して VM を保護するには、 VM のすべての部分が 1 つの SVM 上にのみ存在する必要があります。このルールは、保護対象サイトとリカバリサイトの両方に適用されます。

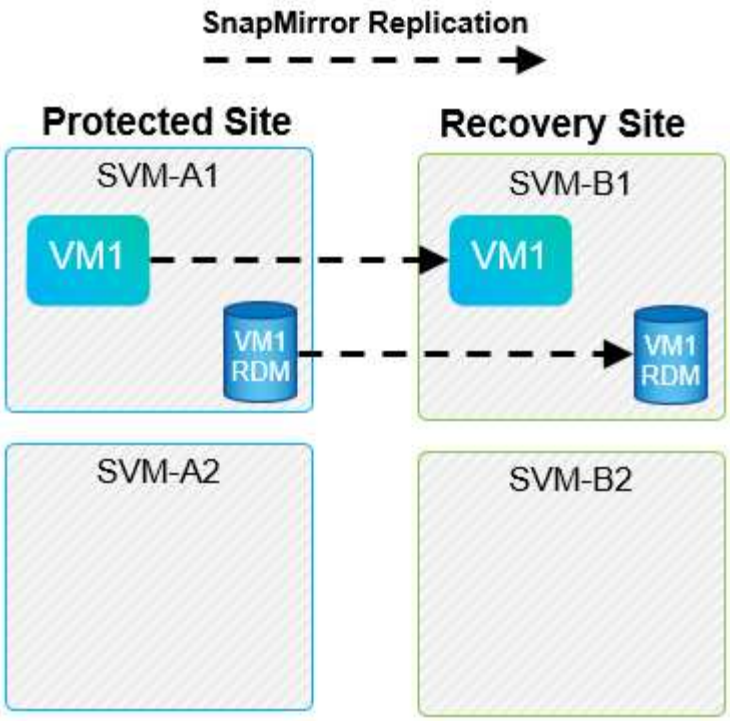
サポートされる **SnapMirror** レイアウト

次の図は、 VLSR 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 VLSR 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



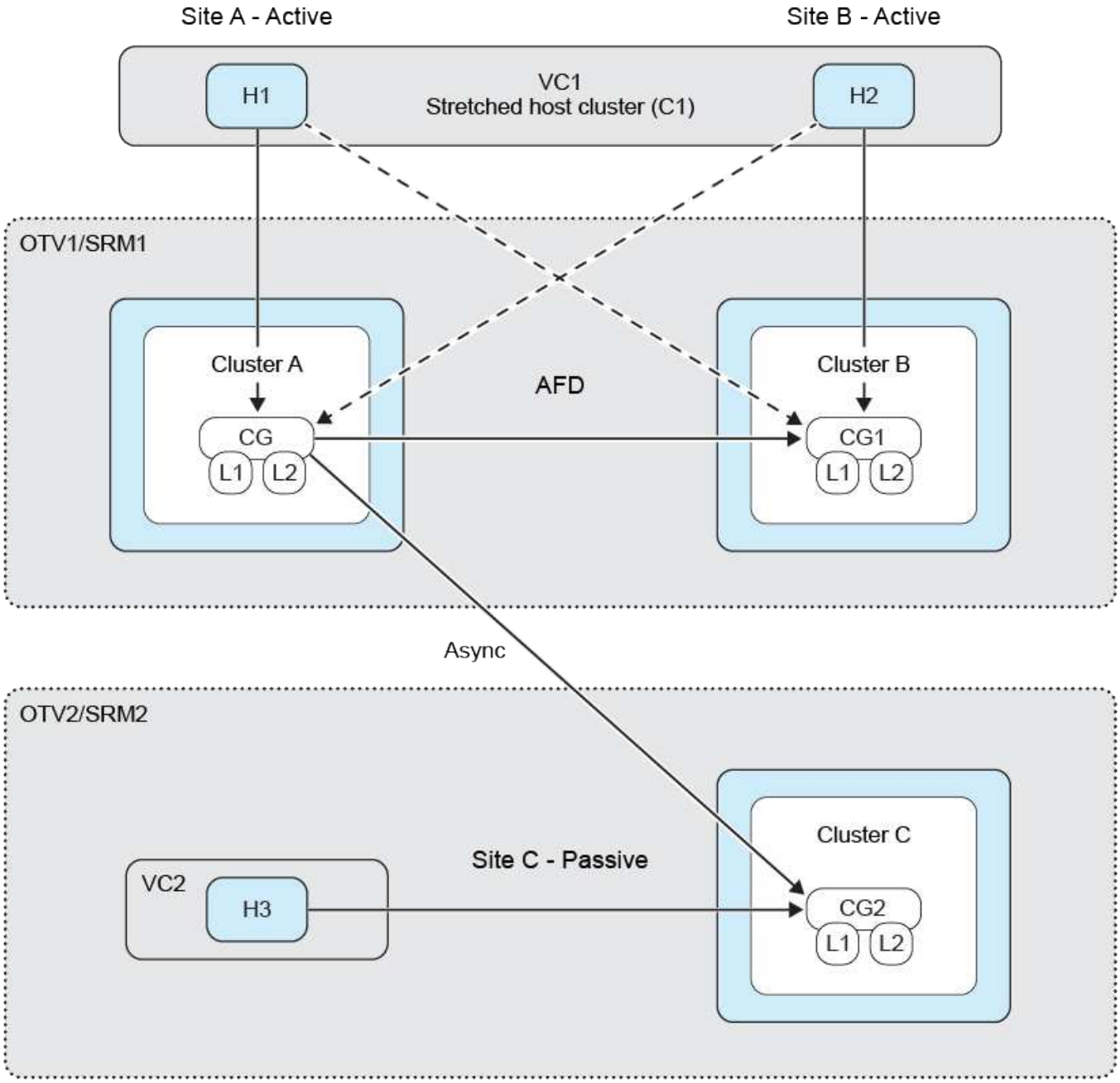
SnapMirror Active Sync による **VMFS** サポート

ONTAPツール 10.3 以降では、 SnapMirror Active Sync (SMAs) を使用した VMFS データストアの保護もサポートされています。これにより、比較的近接する 2 つのデータセンター (障害ドメインと呼ばれる) 間でのビジネス継続性のための透過的なフェイルオーバーが可能になります。その後、 ONTAPツール SRA と VLSR を介してSnapMirror非同期を使用して、長距離災害復旧を調整できます。

"ONTAP SnapMirrorアクティブ同期について学ぶ"

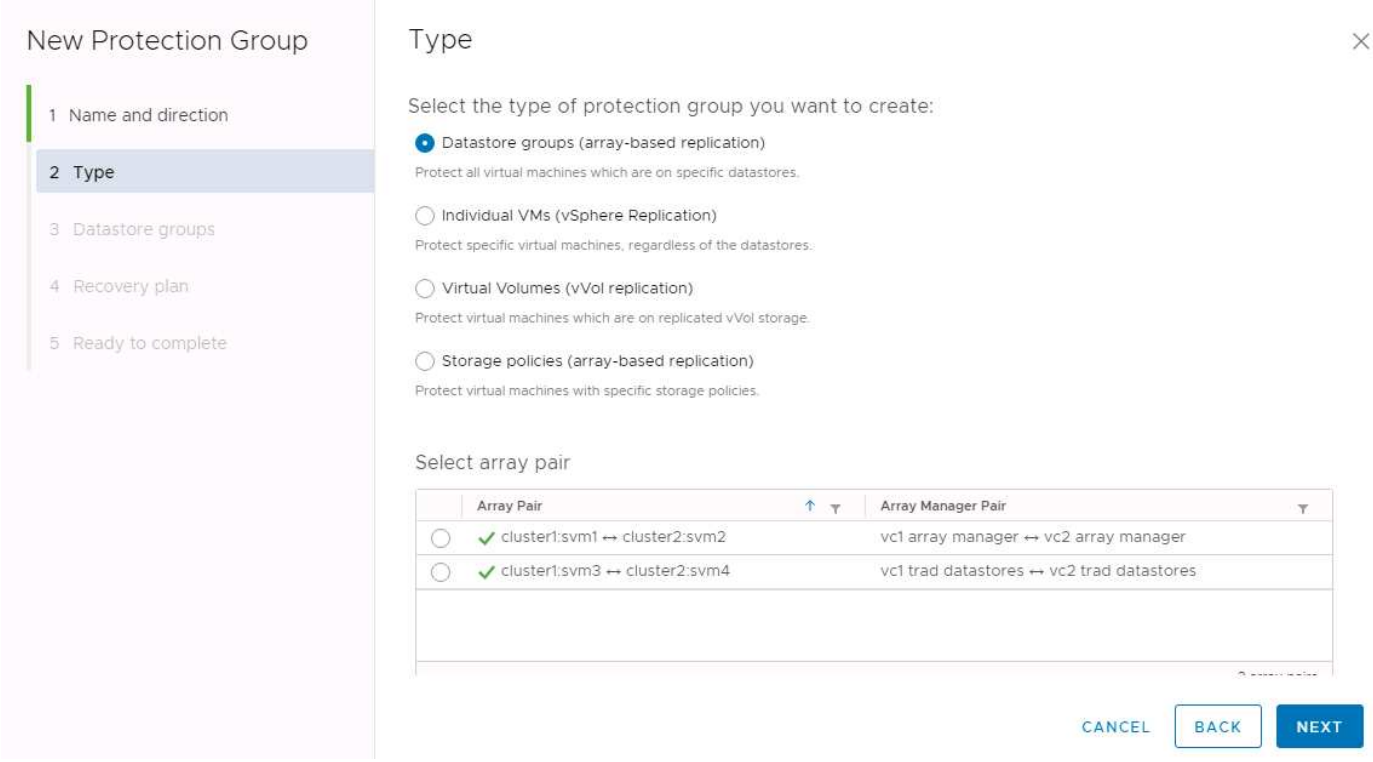
データストアは整合性グループ (CG) に集められ、すべてのデータストアにわたる VM は同じ CG のメンバーとして書き込み順序の一貫性を維持します。

たとえば、ベルリンとハンブルクのサイトを SMas で保護し、3 番目のサイトのレプリカをSnapMirror非同期を使用して VLSR で保護することが考えられます。もう 1 つの例としては、SMas を使用してニューヨークとニュージャージーのサイトを保護し、3 番目のサイトをシカゴに置くことが挙げられます。



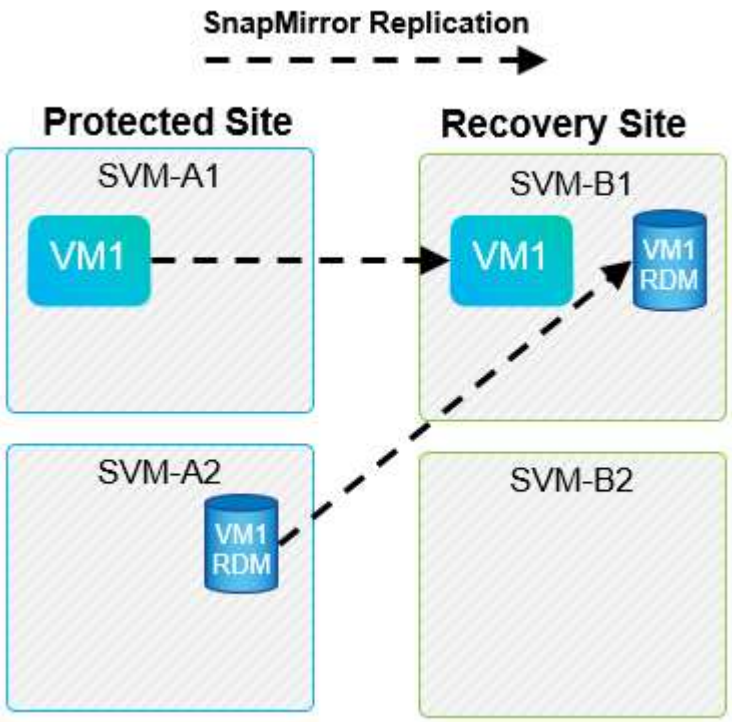
サポートされている **Array Manager** レイアウト

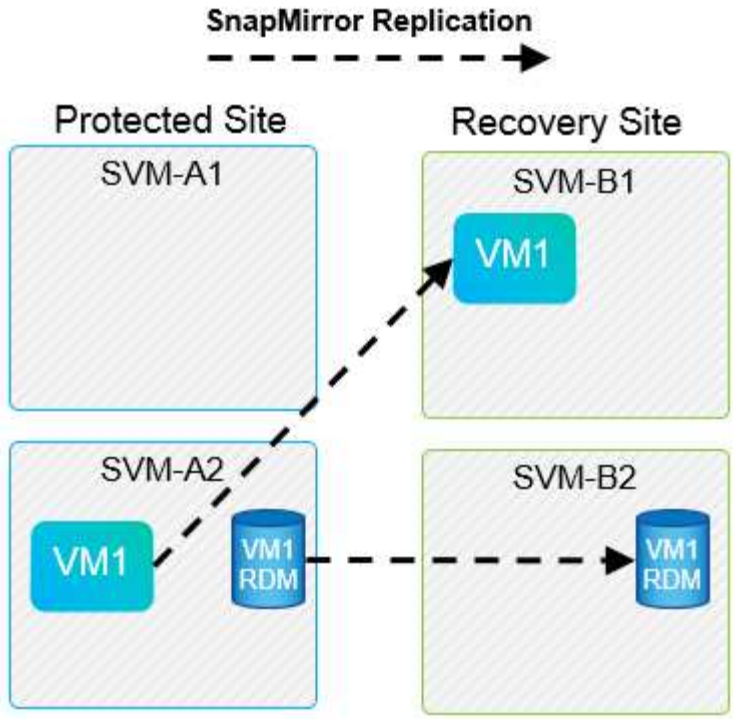
次のスクリーンショットに示すように、 VLSR でアレイベースレプリケーション（ ABR ）を使用すると、保護グループは単一のアレイペアに分離されます。このシナリオでは、 `SVM1` `SVM2`リカバリサイトでと `SVM4`のピア関係が設定されて `SVM3`います。ただし、保護グループを作成するときに選択できるアレイペアは 2 つのうちの 1 つだけです。



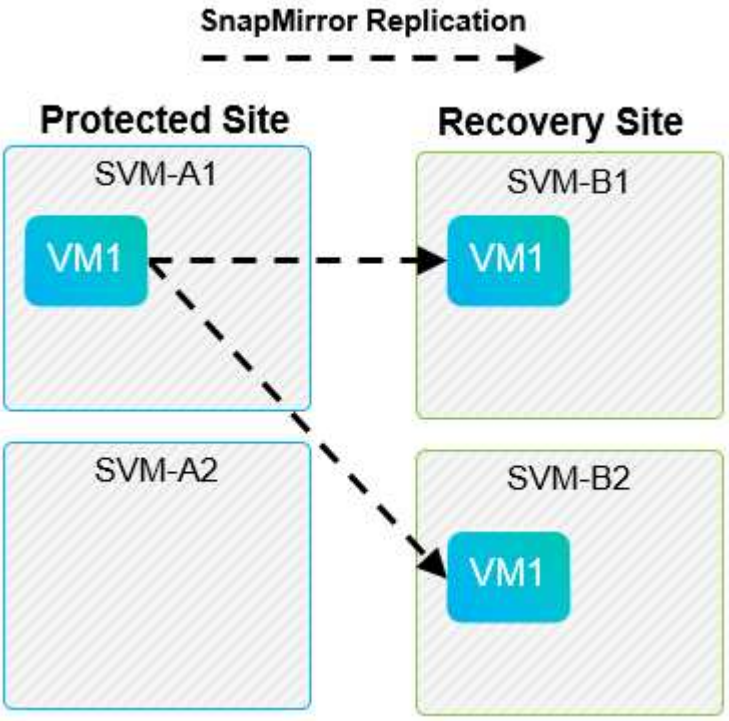
サポートされないレイアウトです

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。次の図の例では、が2つのSVM上にあるため、を `VM1`VLSR`で保護するように設定することはできません。 `VM1`





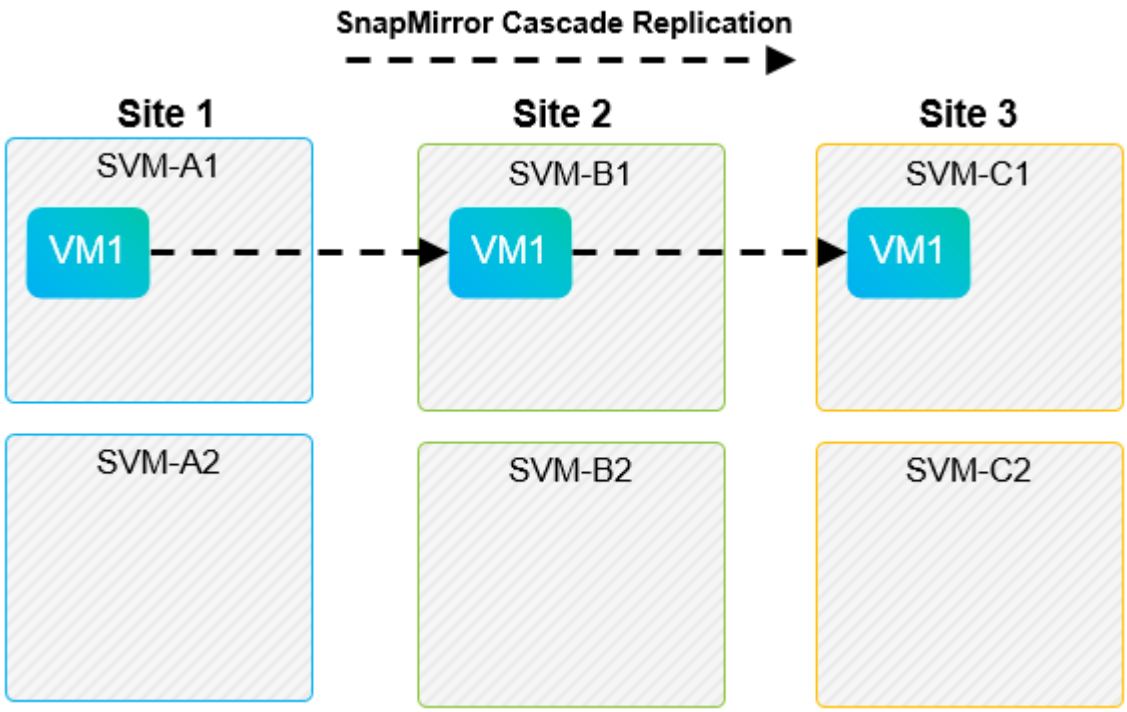
1 つのネットアップボリュームを 1 つのソース SVM から同じ SVM または異なる SVM の複数のデスティネーションにレプリケートするレプリケーション関係は、 SnapMirror ファンアウトと呼ばれます。VLSR ではファンアウトはサポートされていません。次の図の例では、は `VM1`SnapMirrorを使用して2つの異なる場所にレプリケートされるため、VLSRで保護を設定できません。



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、 VLSR ではサポートしていません。次の図に示すシナリオでは、 VLSR 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、VLSR 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、 VLSR フェイルオーバーまたはレプリケーションの反転時

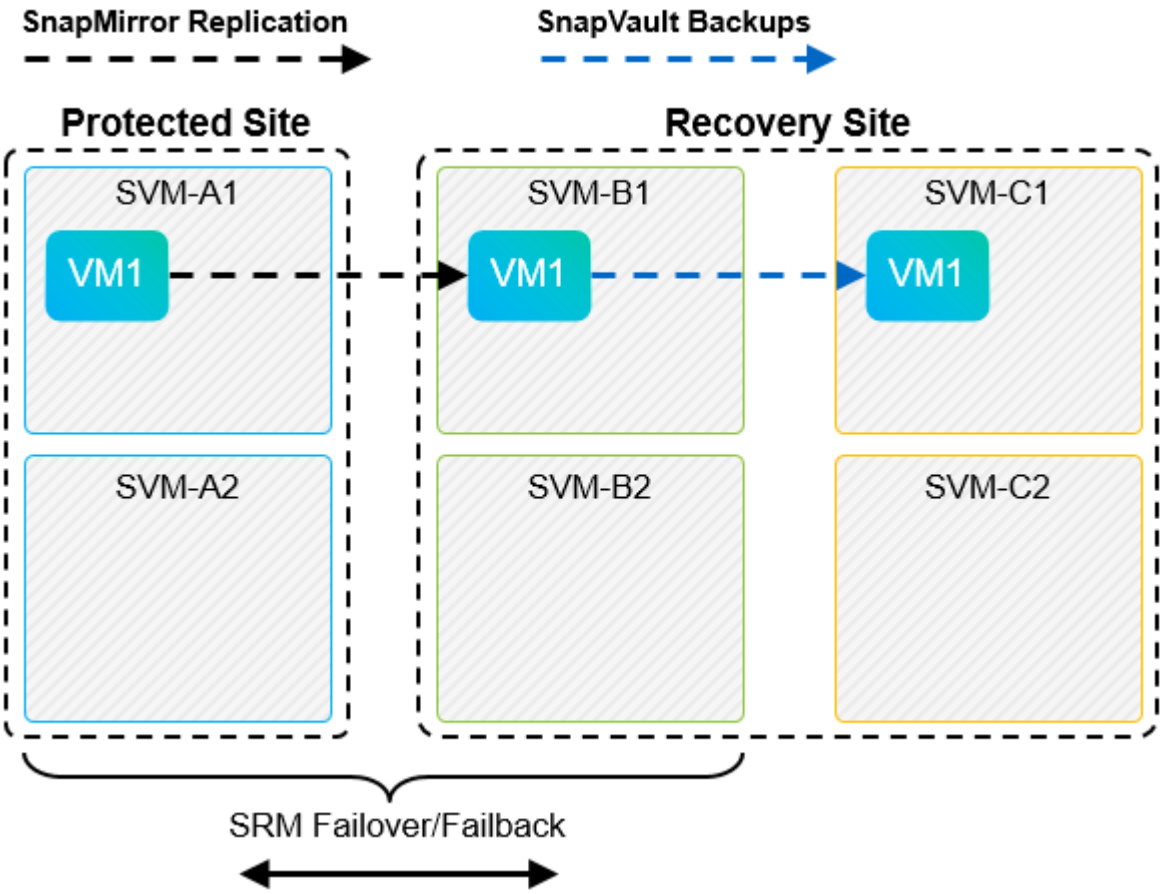
に、 SRA は、 SnapMirror デスティネーションボリュームを SnapVault のソースとして使用するように SnapVault 関係を自動では再設定しません。

ONTAP 9のSnapMirrorとSnapVaultの最新情報については、以下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 VLSR 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。

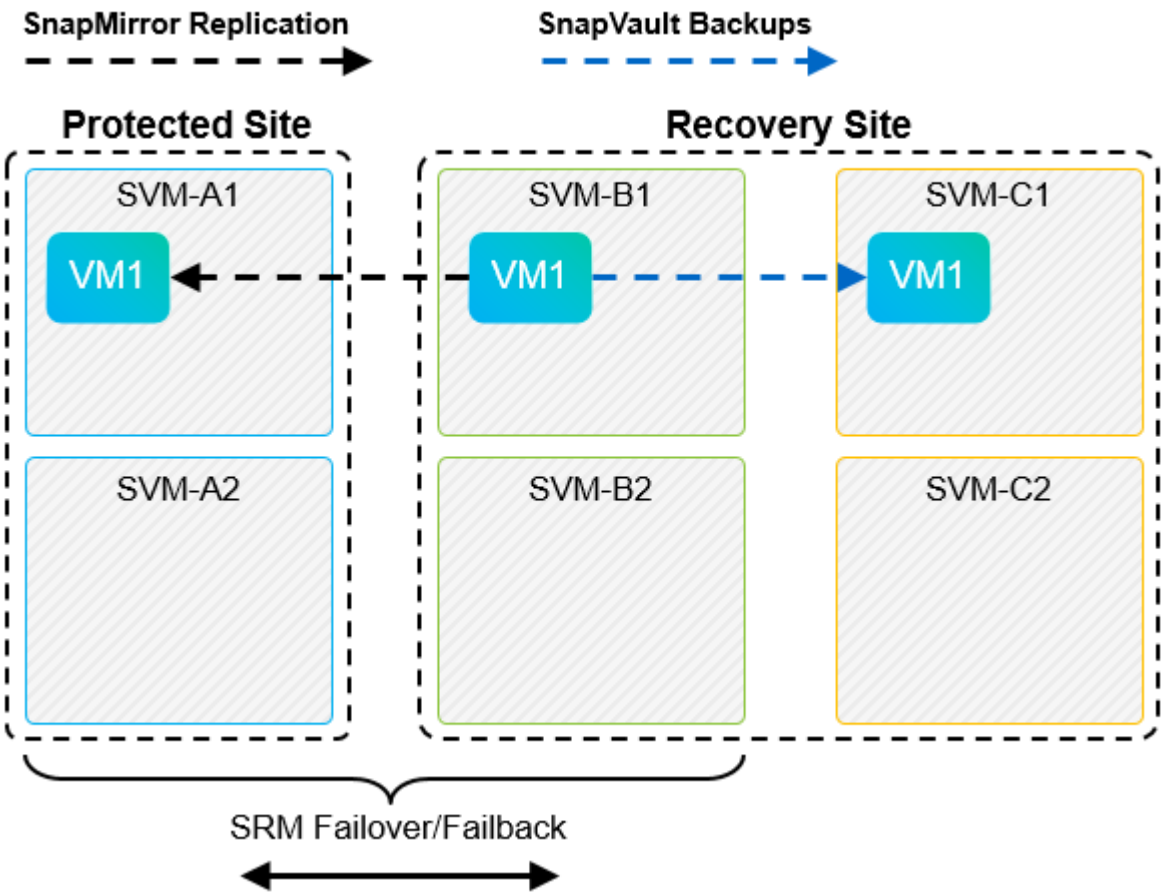
VMware 環境では、各データストアに Universal Unique Identifier （ UUID ）が割り当てられ、各 VM には一意の Managed Object ID （ MOID ）が割り当てられます。VLSR は、フェイルオーバーやフェイルバックの実行時にこれらの ID を維持しません。VLSR はフェイルオーバーでデータストア UUID と VM MOID を維持しないため、これらの ID に依存するアプリケーションは VLSR フェイルオーバーのあとに再設定する必要があります。たとえば、 SnapVault レプリケーションを vSphere 環境と調整する NetApp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



VSRMがフェイルバックおよびSnapMirror関係の2回目の反転を実行すると、本番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できる特別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、のSnapMirrorでは、個 々のqtreeのレプリケーションや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、 VLSR 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 VLSR 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 VLSR ではサポートされていません。 VLSR 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、 VLSR 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
VLSR 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、 VLSR リソースマッピングを設定することも推奨します。

vVolレプリケーション使用時のVLSRM / SRMのトラブルシューティング

ONTAP tools 9.13P2を使用している場合、vVolレプリケーションを使用している場合は、SRAおよび従来のデータストアで使用される場合とは、VLSRおよびSRMでのワークフローが大きく異なります。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`コマンドや `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。

- ONTAP Tools for VMware vSphere 10.xのリソース"https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"
- ONTAP Tools for VMware vSphere 9.xのリソース"https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- 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 ONTAP 9 向けSnapMirror構成ベストプラクティスガイド https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf
- VMware Live Site Recoveryのドキュメント"https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"

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については、NetAppサポートサイトのを参照して"Interoperability Matrix Tool （ IMT ）"ください。NetApp IMTでは、NetAppでサポートされ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と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。

> このドキュメントは、以前に公開されたテクニカルレポート（TR-4128：『vSphere on NetApp MetroCluster _』）を差し替えます。

vSphere環境向けの継続的可用性ソリューション

ONTAPアーキテクチャは、データストアに SAN (FCP、iSCSI、NVMe-oF) および NAS (NFS v3 および v4.1) サービスを提供する、柔軟でスケーラブルなストレージ プラットフォームです。NetApp AFF、 ASA、およびFAS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、S3 や SMB/CIFS などのゲスト ストレージ アクセス用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

（災害時のクラスタフェイルオーバーまたはCFOD）、ハードウェアの冗長性、および高レベルの可用性を実現する地理的な分離も含まれます。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。

非MetroClusterシステムおよびASA R2システムで使用できる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します。vMSC全体を保護することも、優先度の高いワークロードを選択的に保護することもできます。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。ONTAP 9.15.1以降ではSnapMirror、対称アクティブ/アクティブ機能がサポートされます。これにより、双方向同期レプリケーションによって、保護されたLUNの両方のコピーからの読み取りおよび書き込みI/O処理が可能になり、両方のLUNコピーがローカルでI/O処理を処理できるようになります。ONTAP 9.15.1より前のバージョンでは、SnapMirrorのアクティブ同期でサポートされるのは非対称アクティブ/アクティブ構成のみです。この構成では、セカンダリサイトのデータがLUNのプライマリコピーにプロキシされます。

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。

も参照してください "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構成です。これは、ラック、建物、キャンパス、さらには都市などのさまざまな障害ドメインに分散された ESXi ホストのクラスターとともに、ストレッチ ストレージのコンセプトを使用することで実現されます。NetApp MetroClusterおよびSnapMirrorアクティブ同期ストレージ テクノロジは、ホスト クラスタにゼロ復旧ポイント目標 (RPO=0) 保護を提供するために使用されます。vMSC 構成は、物理サイトまたは論理サイト全体に障害が発生した場合でも、データが常に利用可能となるように設計されています。vMSC 構成の一部であるストレージ デバイスは、vMSC 認定プロセスに合格した後に認定される必要があります。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"。

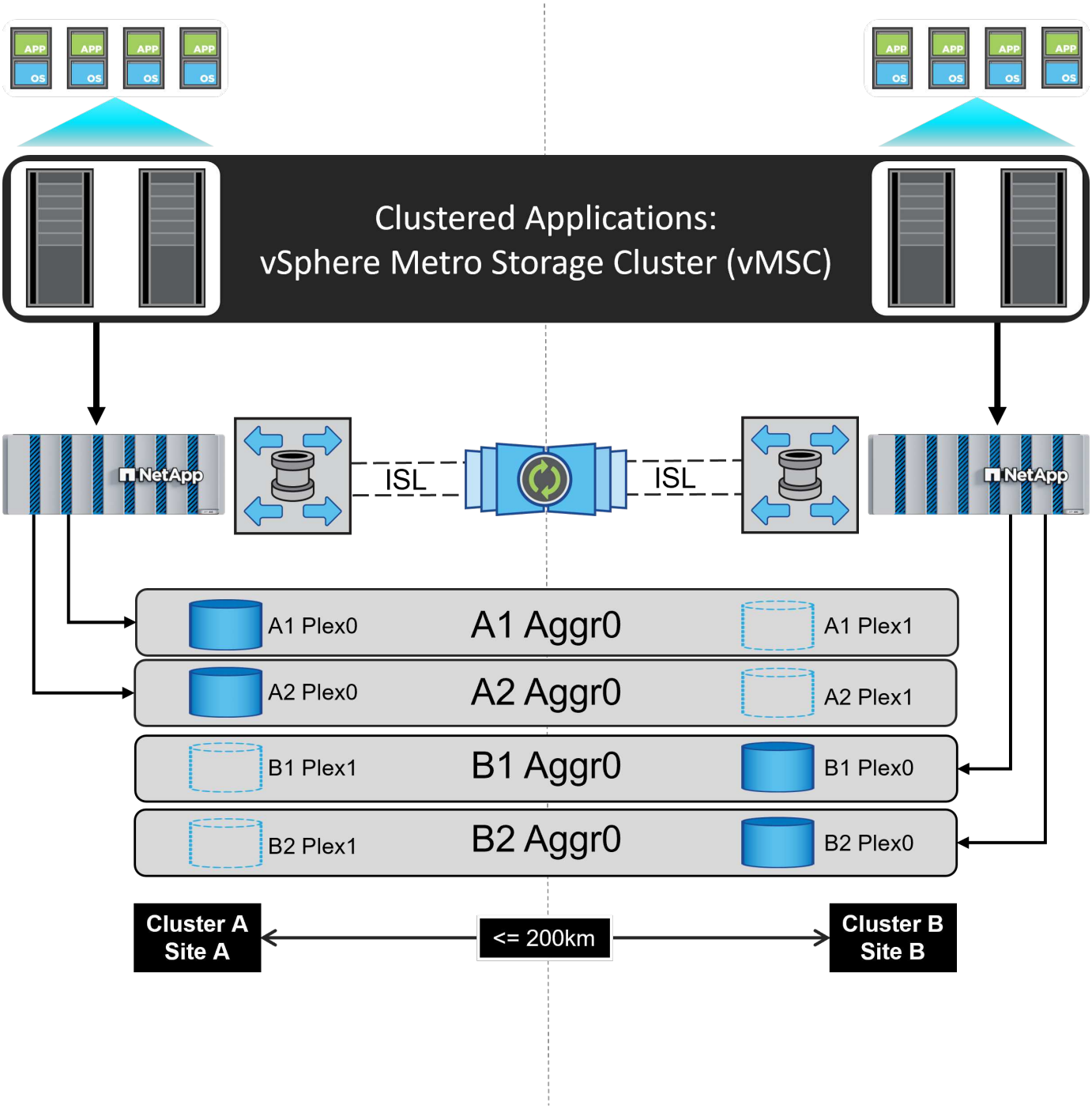
vSphere Metro Storage Clusterの設計ガイドラインの詳細については、次のドキュメントを参照してください。

- "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）

NetApp MetroClusterは、vSphereで使用する2種類の構成で導入できます。

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

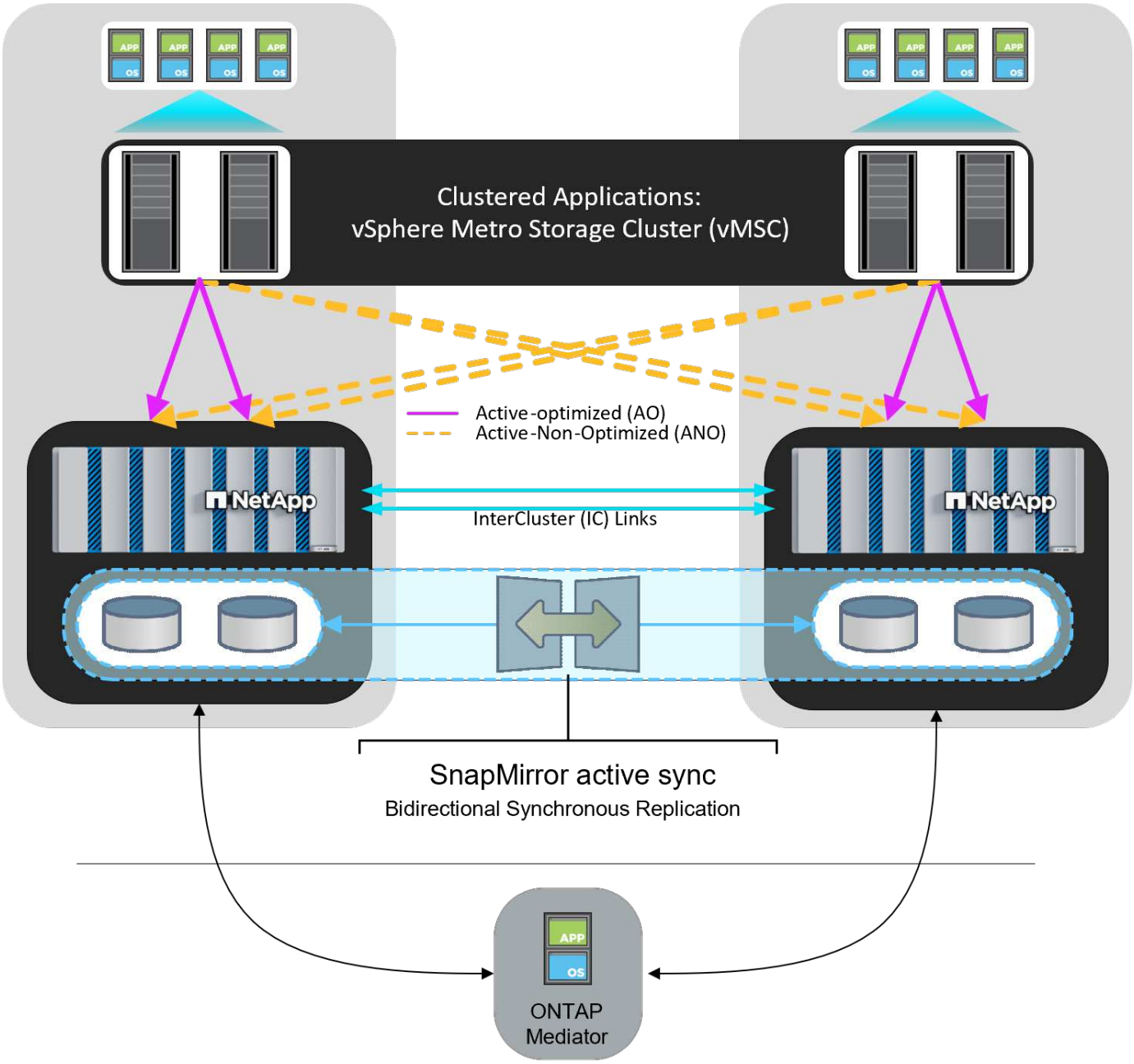
次の図は、ストレッチMetroClusterのトポロジ図の概要を示しています。



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Active Sync（ONTAP 9.15.1）



SnapMirrorアクティブ同期の特定の設計および配置情報については、を参照してください "ネットアップのドキュメント"。

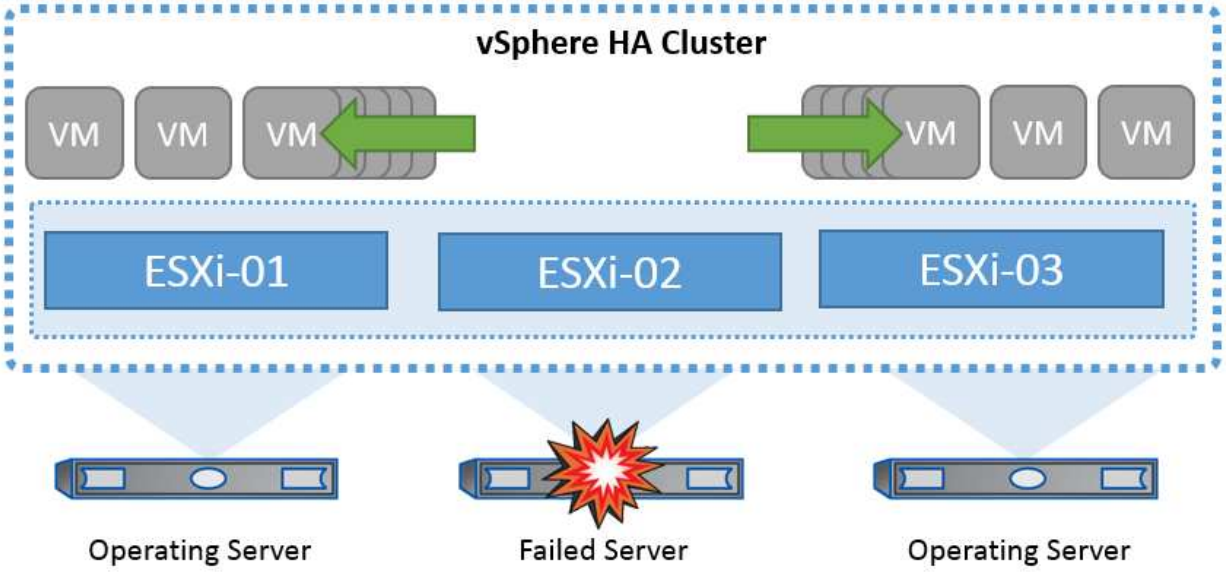
VMware vSphere解決策の概要

vCenter Server Appliance (VCSA) は、管理者が ESXi クラスターを効果的に操作できるようにする、vSphere 用の強力な集中管理システムおよび単一管理画面です。VM のプロビジョニング、vMotion 操作、高可用性 (HA)、分散リソース スケジューラ (DRS)、VMware vSphere Kubernetes Service (VKS) などの主要な機能を容易に実現します。これは VMware クラウド環境に不可欠な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用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OSに障害が発生した場合、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できます。vSphere HAを使用すると、計画的ダウンタイムの削減、計画外ダウンタイムの防止、およびシステム停止からの迅速なリカバリが可能になります。

障害が発生したサーバーから VM を復旧する vSphere HA クラスタ。



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 クラスターが作成されるとすぐに、クラスター内のすべてのホストが選出に参加し、ホストの 1 つ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担います。

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。

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

隔離対応は、vSphere HA クラスタ内のホストが管理ネットワーク接続を失ったが実行を継続している場合に仮想マシンでトリガーされるアクションを決定する vSphere HA の設定です。この設定には、「無効」、「VM をシャットダウンして再起動する」、「VM の電源をオフにして再起動する」の 3 つのオプションがあります。

「シャットダウン」は、最新の変更をディスクにフラッシュしたり、トランザクションをコミットしたりしない「電源オフ」よりも優れています。仮想マシンが 300 秒以内にシャットダウンしない場合は、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。

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 は、ストレージ デバイスが恒久的に故障した場合、または管理上削除されて復旧が期待されない場合に発生する状態です。NetAppストレージ アレイは、デバイスが永久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「障害条件と VM 応答」セクションでは、PDL 条件が検出された後の応答を設定できます。

NetApp、「PDL を含むデータストアの応答」を「**VM** の電源をオフにして再起動する」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上で 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 デバイスがホストにアクセスできなくなり、アレイへのパスが利用できなくなるとき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見なし、デバイスが再び利用可能になると予想しています。

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。

- 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指します。「保守的」に設定すると、HA は、別のホストが再起動できることがわかっている場合にのみ、APD の影響を受ける VM を再起動します。アグレッシブの場合、HA は他のホストの状態がわからない場合でも VM の再起動を試みます。これにより、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場合、VM が再起動されなくなる可能性があります。
- タイムアウトが経過する前に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。
- 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 SnapMirror Active Syncのための**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。

NetApp MetroCluster向け**VMware DRS**の実装

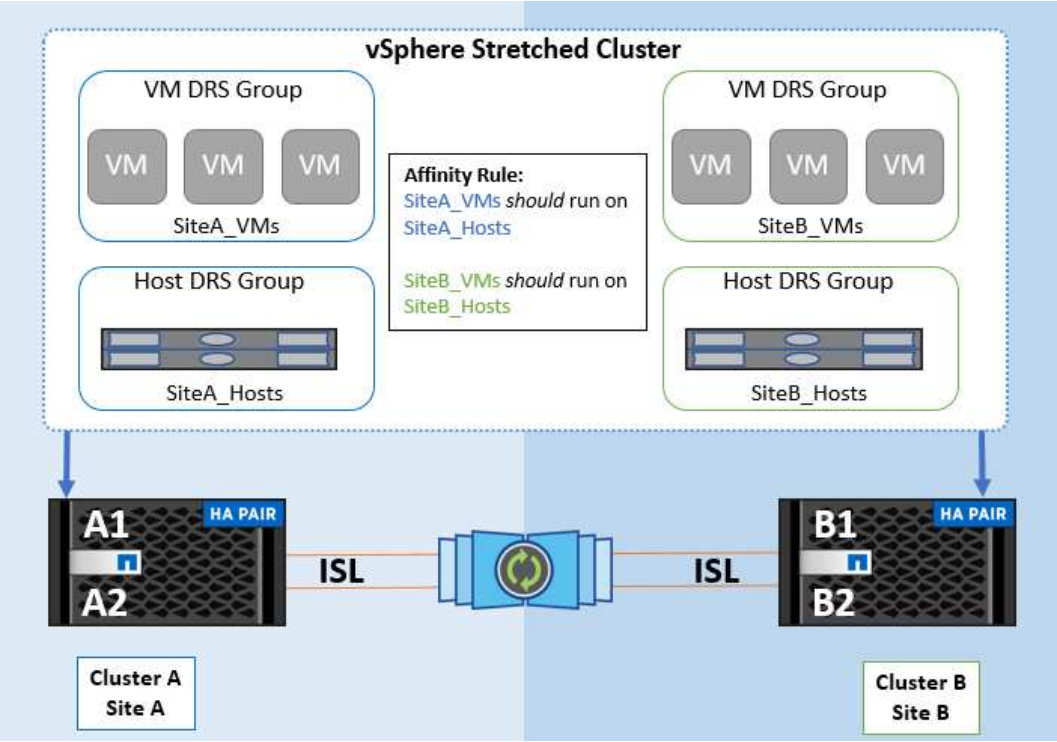
```
 To avoid cross-site traffic, NetApp recommends configuring DRS affinity
rules to manage a logical separation of VMs. This will ensure that, unless
there is a complete site failure, HA and DRS will only use local hosts.
```
クラスタ用のDRSアフィニティルールを作成する場合は、仮想マシンのフェイルオーバー時にvSphereがそのルールを適用する方法を指定できます。

vSphere HA フェイルオーバー動作に指定できるルールには 2 つの種類があります。

- 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も優先される必要があります。データセンター全体に障害が発生するシナリオでは、「必須」ルールによって 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い場合は仮想マシンは再起動しません。

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（SIOC）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。

- ONTAPストレージを使用する場合は、Storage DRSを無効にすることを推奨します。
- Storage DRSは通常、ONTAPストレージシステムでの使用には必要ありません。推奨もされません。
- ONTAPには、重複排除、圧縮、コンパクションなど、Storage DRSの影響を受ける独自のStorage Efficiency機能が用意されています。
- ONTAPスナップショットを使用している場合、Storage vMotion はスナップショット内に VM のコピーを残すため、ストレージ使用率が上昇し、VM とそのONTAPスナップショットを追跡するNetApp SnapCenterなどのバックアップ アプリケーションに影響を及ぼす可能性があります。

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のセットアップ手順については、を参照してください "MetroCluster のドキュメント" 。SnapMirror Active Sync（SMA）の手順については、を参照してください "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や、MetroClusterでサポートされていないONTAPシステム（ASA R2システムなど）を使用している場合は、SnapMirrorアクティブ同期を使用して、異なる障害ドメイン内の複数のONTAPクラスタ間でデータストアのきめ細かな保護とアクティブ/アクティブアクセスを提供できます。SMAでは、整合グループ（CG）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CG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。たとえば、データストア間でゲストLVMを分散した場合などです。SMAは、Raw Device Mapping（RDM；rawデバイスマッピング）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しています。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、SMA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。次に、SnapMirrorのアクティブな同期で保護するデータストアの整合グループを1つ以上作成する必要があります。最後に、作成した整合グループのSnapMirrorポリシーを作成する必要があります。これらはすべて、ONTAP tools vCenterプラグインの「クラスタの保護」ウィザードを使用して簡単に実行できます。また、ONTAP CLIまたはSystem Managerを使用して手動で実行することもできます。

SnapMirror Active Sync用ONTAPツールvCenterプラグインの使用

ONTAP tools vCenterプラグインを使用すると、vMSCのSnapMirrorアクティブ同期をシンプルかつ直感的に設定できます。ONTAP tools vCenterプラグインを使用して、2つのONTAPクラスタ間にSnapMirrorのアクティブな同期関係を作成および管理できます。このプラグインは、これらの関係を効率的に確立および管理するための使いやすいインターフェイスを提供します。ONTAP tools vCenterプラグインの詳細については、を参照 "VMware vSphere 用の ONTAP ツール"するか、にジャンプし "ホストクラスタの保護を使用した保護"ます。

VMware vSphereの設定

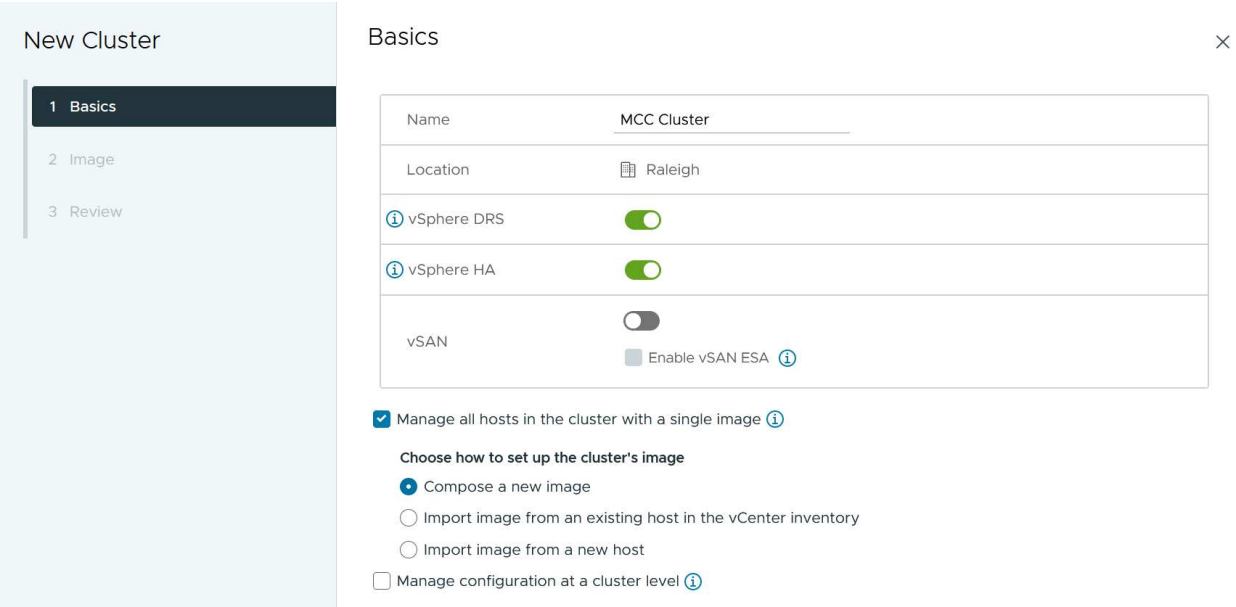
vSphere HAクラスタの作成

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。

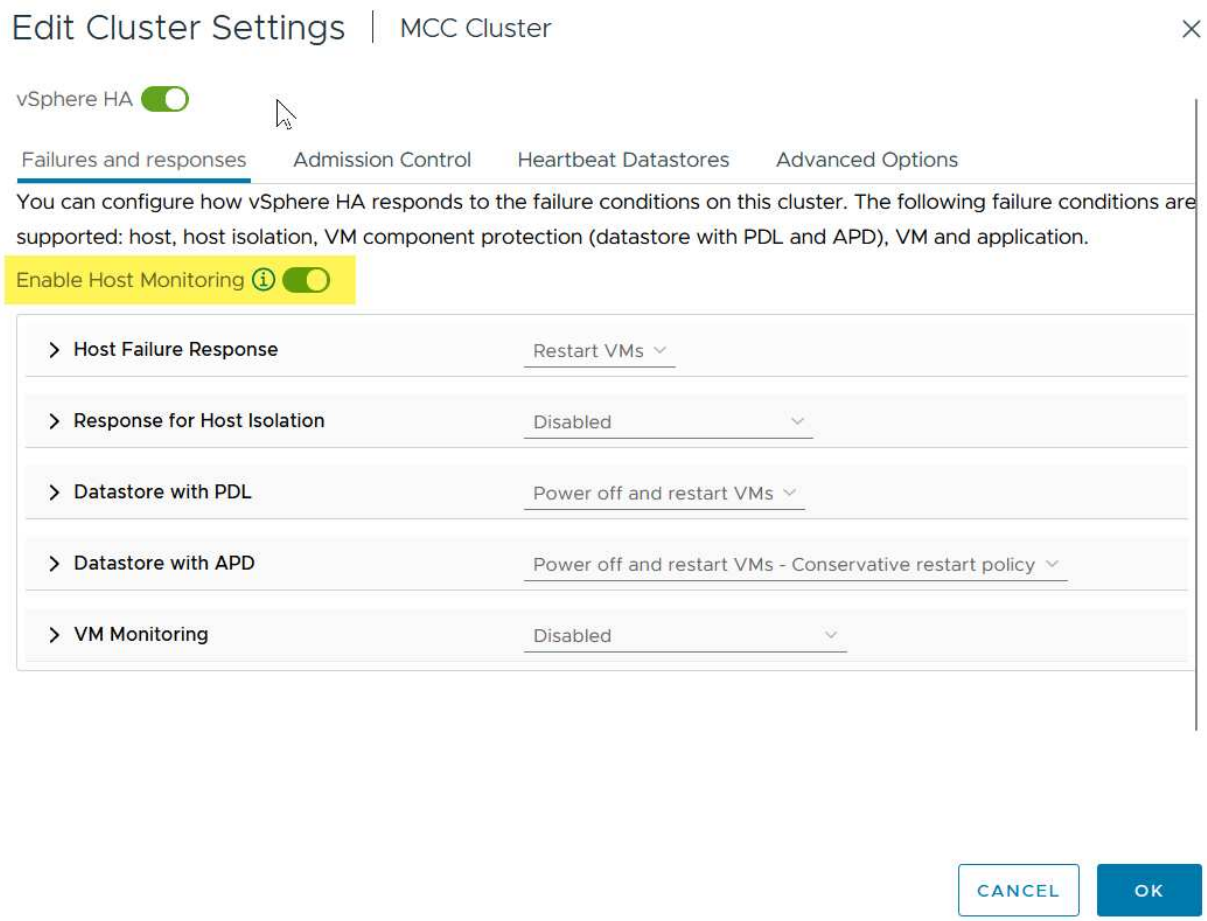
> このドキュメントに記載されている内容は優先され "VMware vSphere Metro Storage Cluster Recommended Practices"ません。このコンテンツは参照しやすいように提供されており、VMwareの公式ドキュメントに代わるものではありません。

HAクラスタを設定するには、次の手順を実行します。

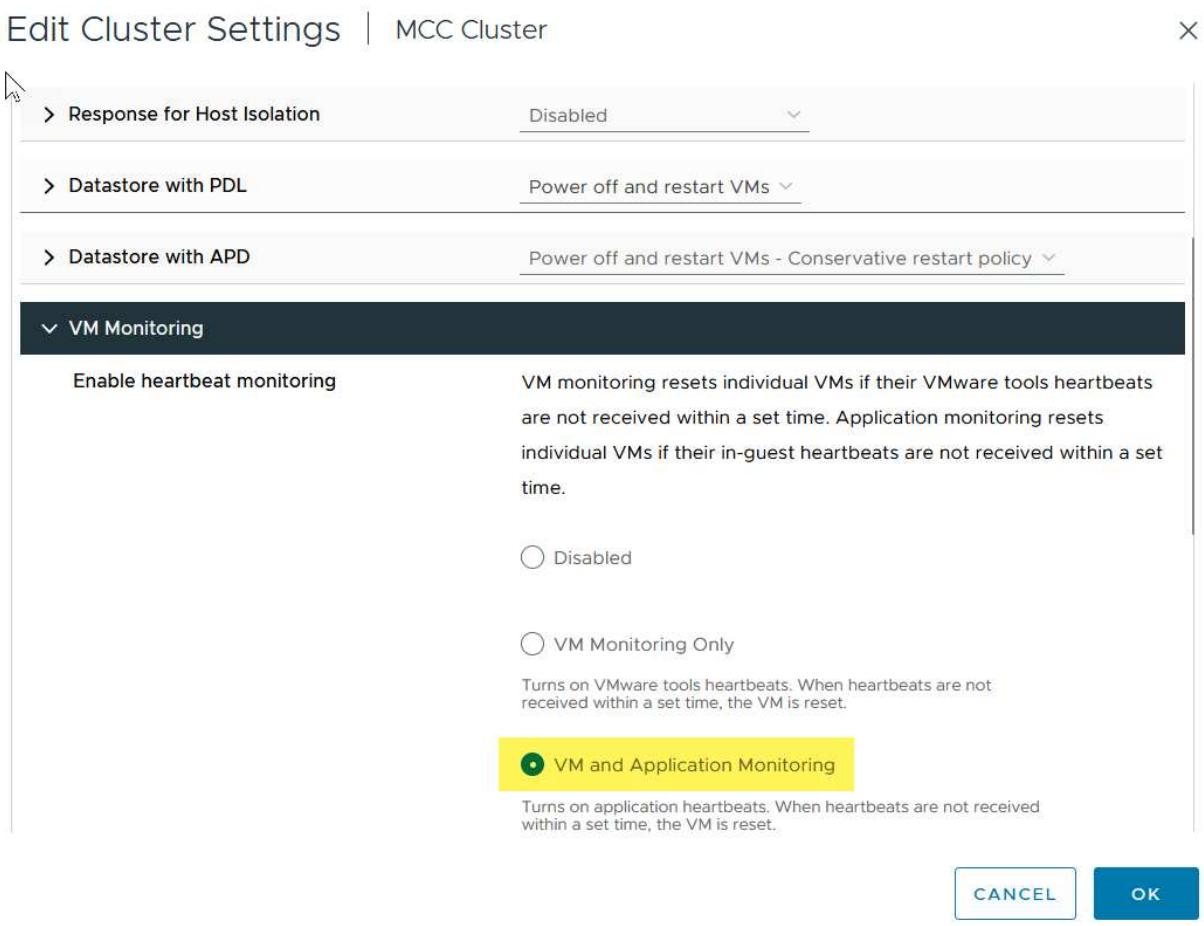
1. vCenter UIに接続します。
2. [Hosts and Clusters]で、HAクラスタを作成するデータセンターを選択します。
3. データセンターオブジェクトを右クリックし、[New Cluster]を選択します。[Basics]で、vSphere DRSとvSphere HAが有効になっていることを確認します。ウィザードの手順を実行します。



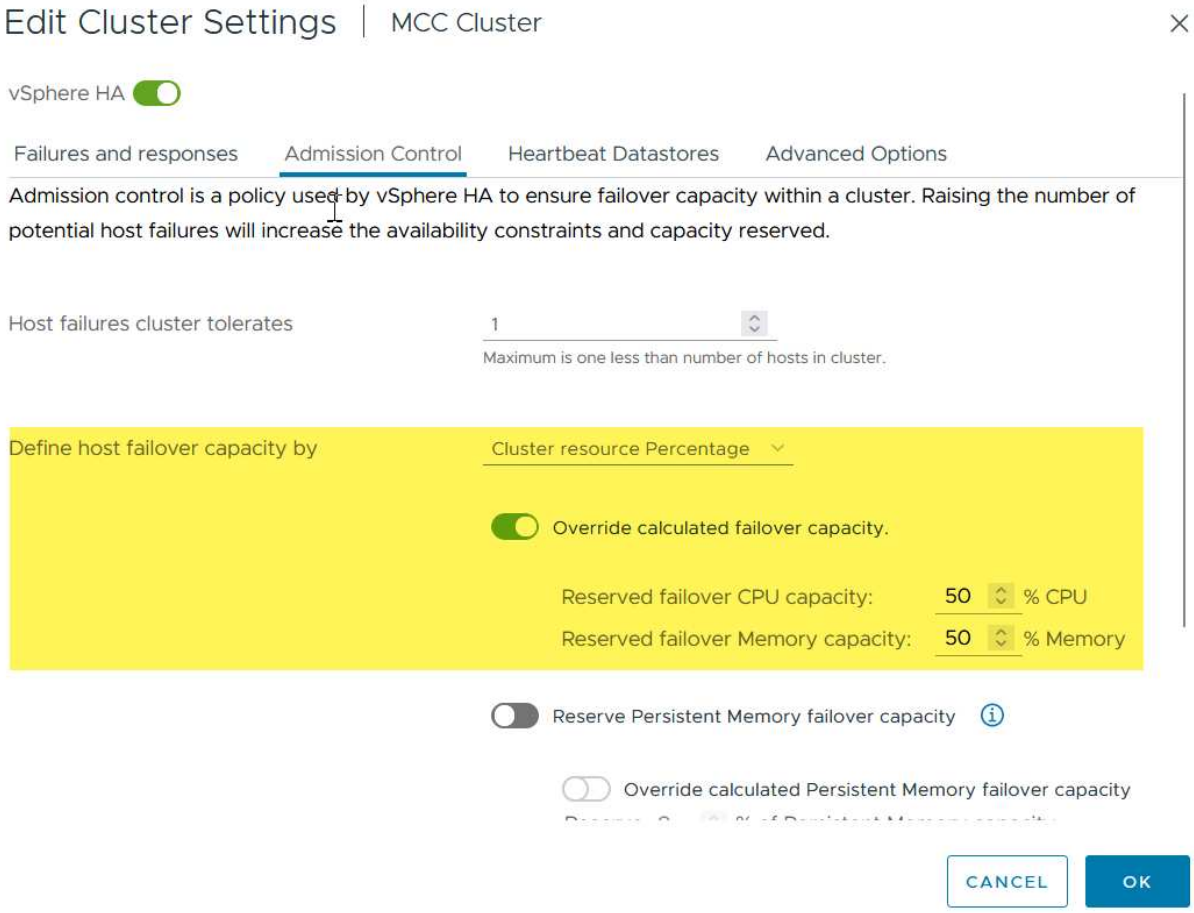
1. クラスタを選択し、[Configure]タブに移動します。[vSphere HA]を選択し、[edit]をクリック
2. [Host Monitoring]で、[Enable Host Monitoring]オプションを選択します。



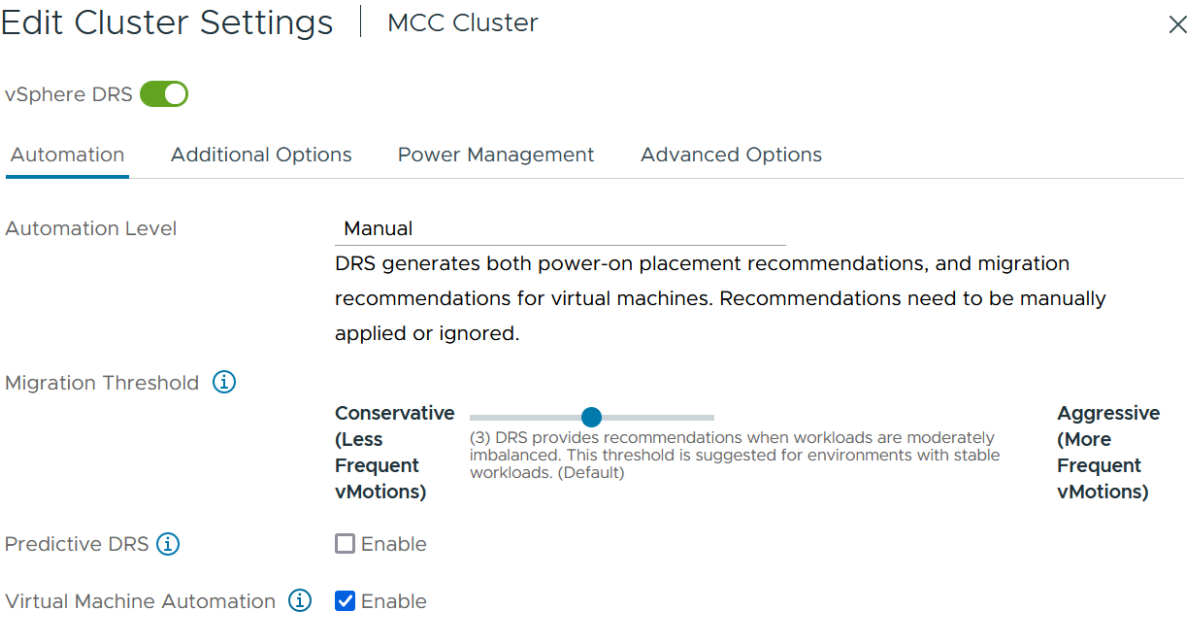
1. [Failures and Responses]タブの[VM Monitoring]で、[VM Monitoring Only]オプションまたは[VM and Application Monitoring]オプションを選択します。



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。



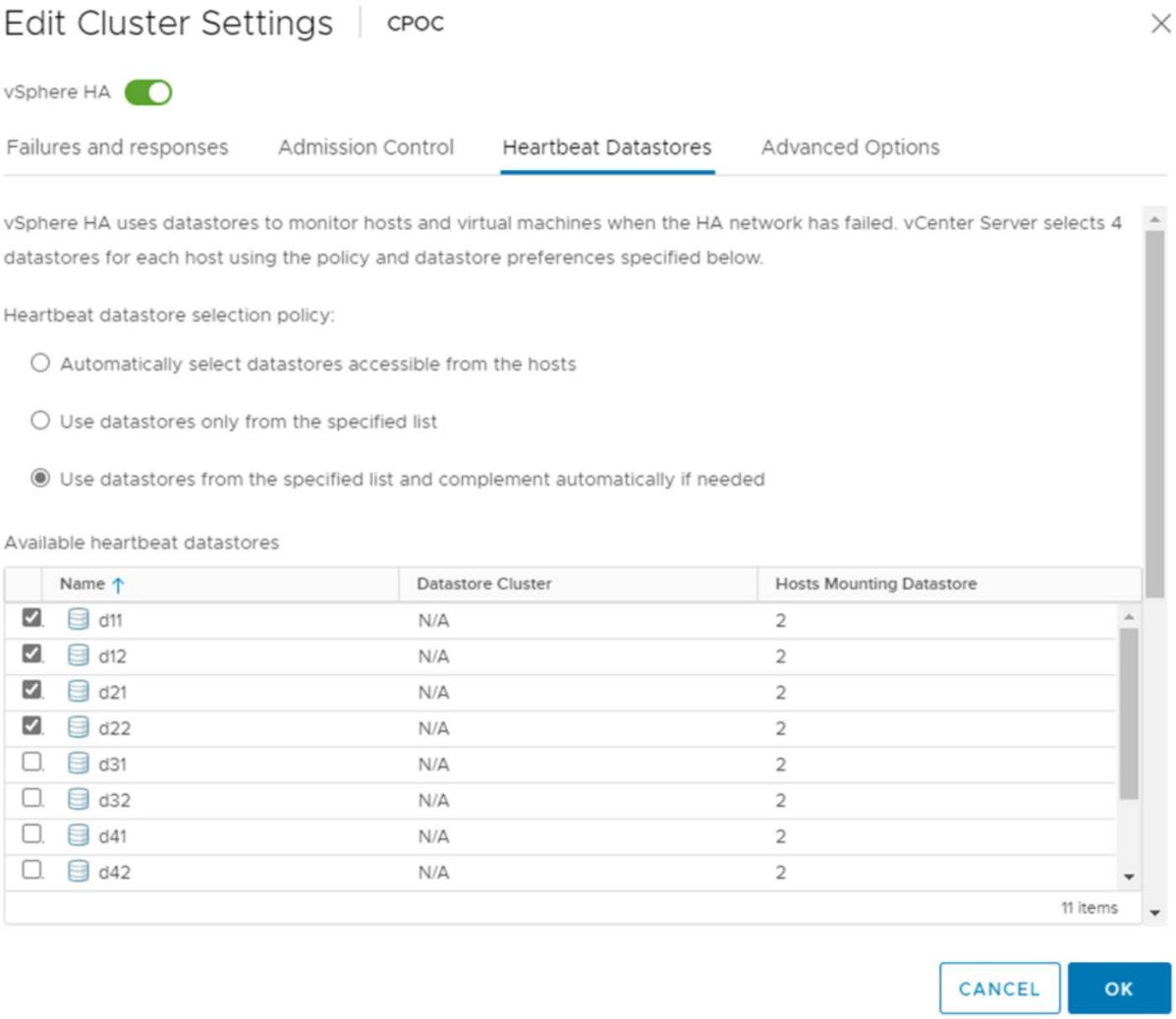
1. VMコンポーネント保護を有効にします。を参照してください。 "docs.vmware.com"。
2. MetroClusterを備えたvMSCでは、次のvSphere HAの追加設定が推奨されます。

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。

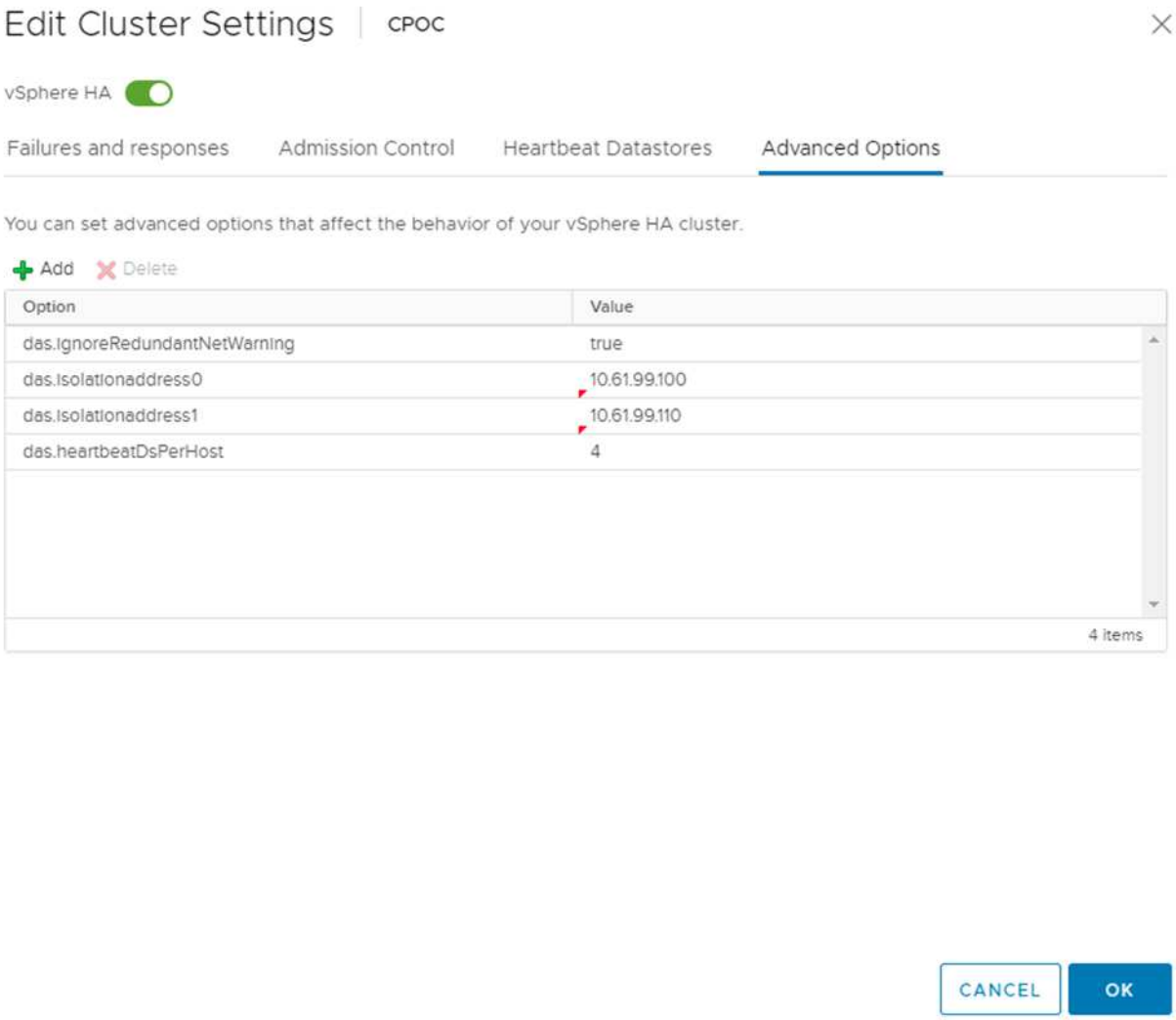
1. [Datastore Heartbeating]セクションで、[Use Datastores from the Specified List and Complement Automatically if Needed]を選択します。
2. vCenterで使用するデータストアを両方のサイトから選択し、[OK]を押します。



詳細オプションの設定

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。

詳細については、を参照してください "VMware vSphere Metro Storage Cluster Recommended Practices"。



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、これらは、MetroClusterやSnapMirrorのアクティブな同期で保護する必要はありません。

詳細については、を参照してください "VMware vSphere Metro Storage Cluster Recommended Practices"。

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。

- 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。
- 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、のドキュメントを参照して"vSphereの監視とパフォーマンス"ください。

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。

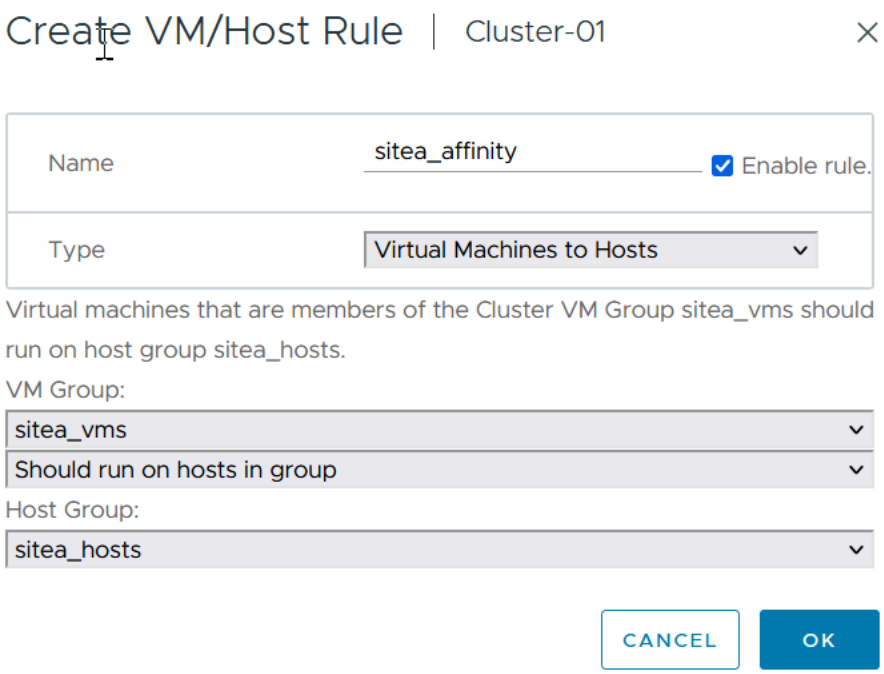
1. vSphere Web Clientで、インベントリ内のクラスタを右クリックし、[Settings]を選択します。
2. [VM\Host Groups]をクリックします。
3. 追加をクリックします。
4. グループの名前を入力します（例：sitea_vms）。
5. [Type]メニューから[VM Group]を選択します。
6. [Add]をクリックし、サイトAから目的のVMを選択して[OK]をクリックします。
7. 同じ手順を繰り返して、サイトBのホストグループをもう1つ追加します。
8. [OK] をクリックします。

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。



必要に応じてデータストアクラスタを作成

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。

- ONTAPストレージを使用する場合は、Storage DRSを無効にすることを推奨します。
- Storage DRSは通常、ONTAPストレージシステムでの使用には必要ありません。推奨もされません。
- ONTAPには、重複排除、圧縮、コンパクションなど、Storage DRSの影響を受ける独自のStorage Efficiency機能が用意されています。
- ONTAPスナップショットを使用している場合、Storage vMotionによってスナップショットにVMのコピーが残されるため、ストレージ利用率が向上し、VMとそのONTAPスナップショットを追跡するNetApp SnapCenterなどのバックアップアプリケーションに影響が及ぶ可能性があります。

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、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、冷却装置の喪失、ネットワーク接続の喪失、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。

テイクオーバー中は、MetroCluster構成のNAS LIFが自動的にフェイルオーバーされます。ただし、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、を参照して "HAペアの管理の概要"ください。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、ONTAPメディエーターが必要です。

vMSCとMetroCluster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。

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。

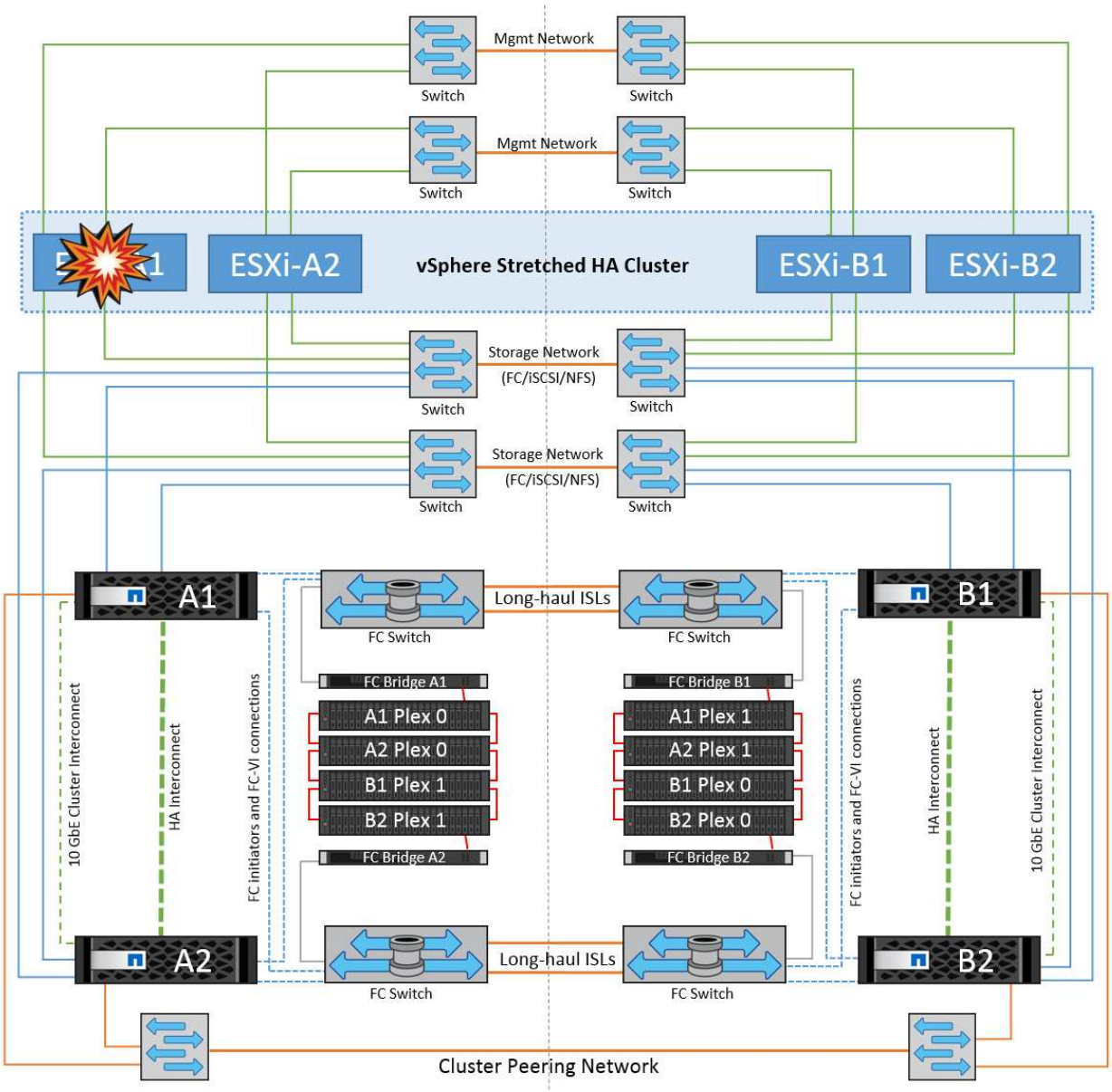
また、iSCSI LUNの場合は、vmkernelインターフェイスをiSCSIネットワークアダプタにバインドしてマルチパスを設定する必要があります。詳細については、vSphereストレージのドキュメントを参照してください。

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。

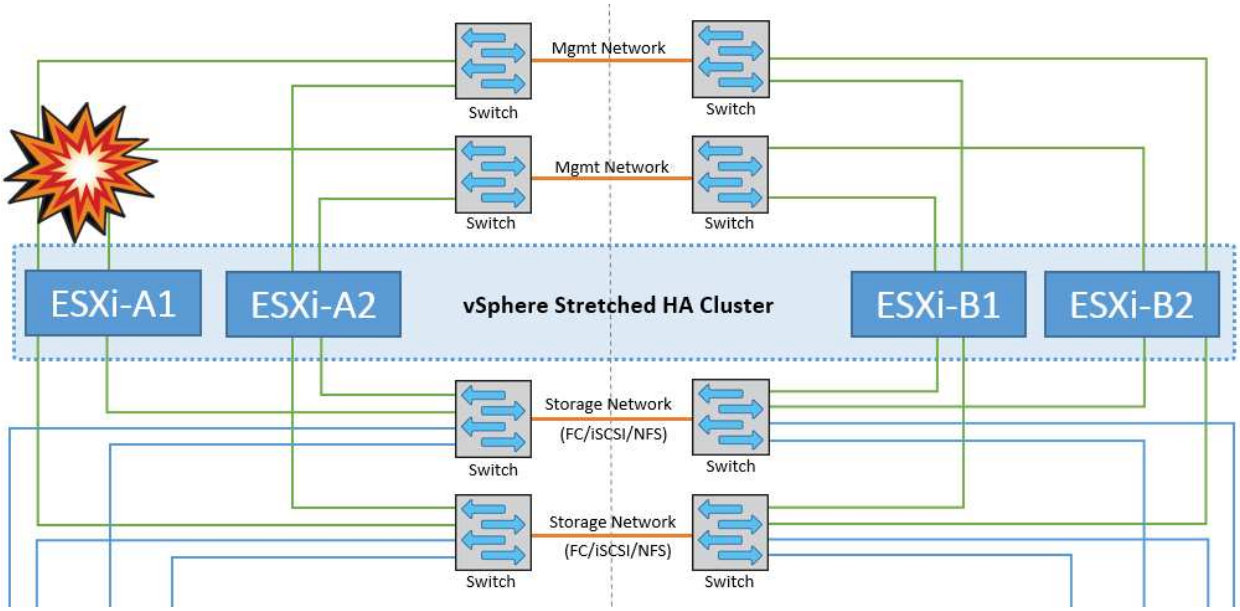
DRSのVMとホストのアフィニティルールが設定されている場合（VMグループsitea_vmsのVMはホストグループsitea_hostsのホストを実行する必要があります）、HAマスターは最初にサイトAで使用可能なリソースを確認します。サイトAに使用可能なホストがない場合、マスターはサイトBのホストでVMの再起動を試みます。

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

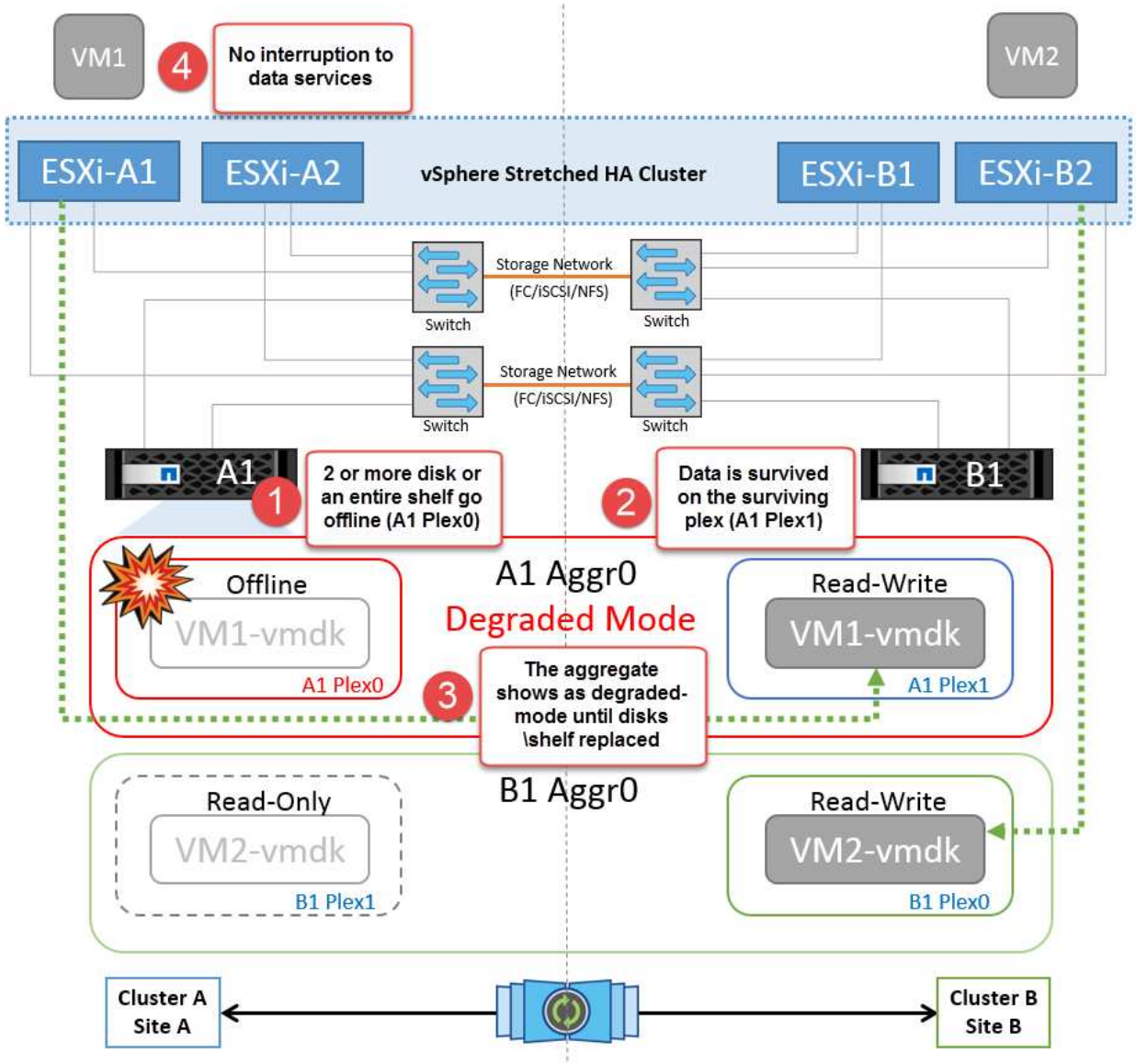


このシナリオでは、ESXiホストの管理ネットワークが停止すると、HAクラスタ内のマスターノードがハートビートを受信しなくなり、このホストがネットワークから分離された状態になります。障害が発生したか、隔離されているだけかを判別するために、マスターノードはデータストアハートビートの監視を開始します。ホストが存在する場合、ホストはマスターノードによって分離されていると宣言されます。構成されている隔離時の対応に応じて、ホストは仮想マシンの電源をオフにするか、シャットダウンするか、仮想マシンの電源をオンにしたままにするかを選択できます。分離応答のデフォルトの間隔は30秒です。

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、プレックスを再構築する必要があります。

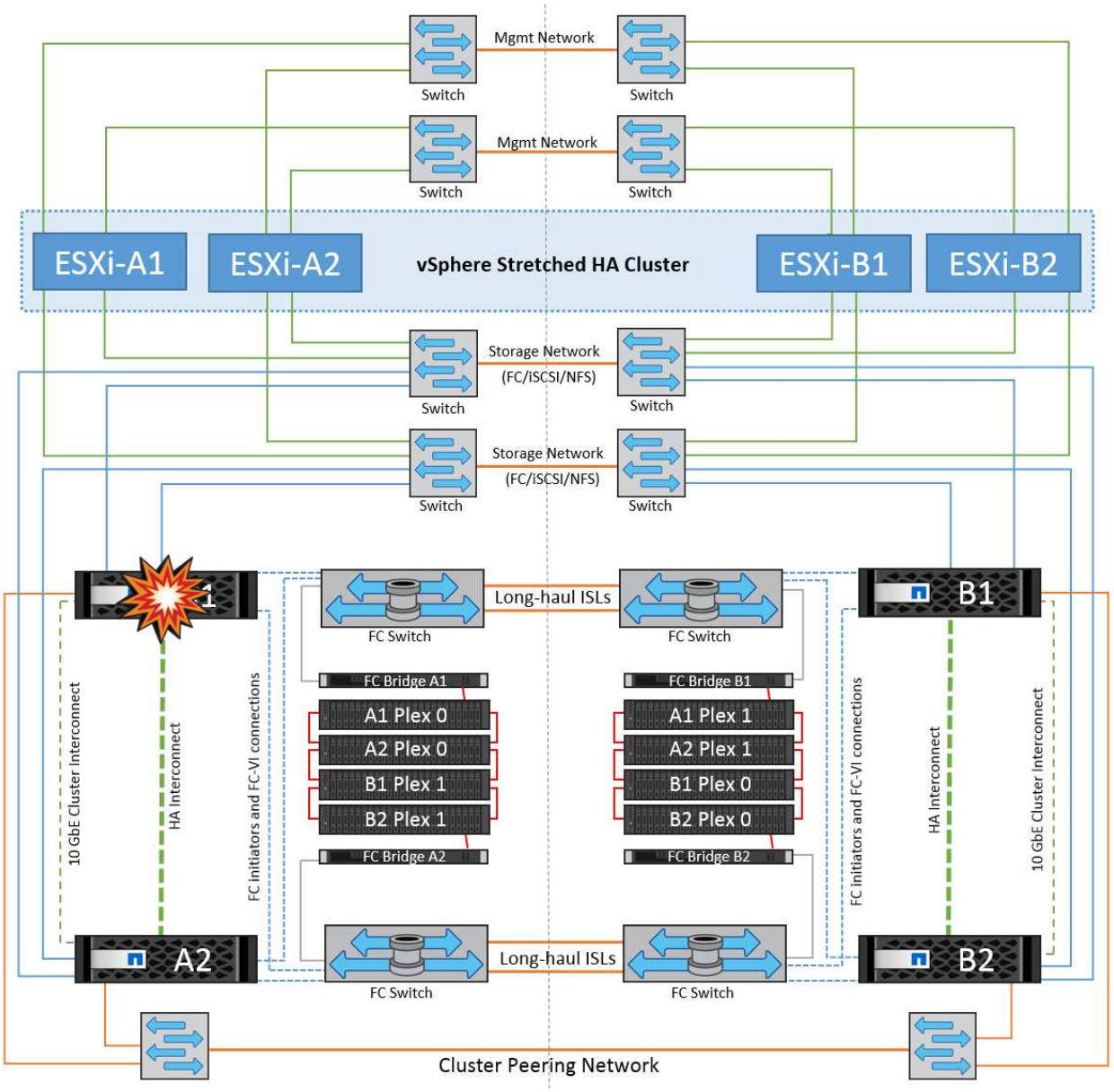


*[メモ]

- この間、仮想マシンのI/O処理には影響はありませんが、データには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

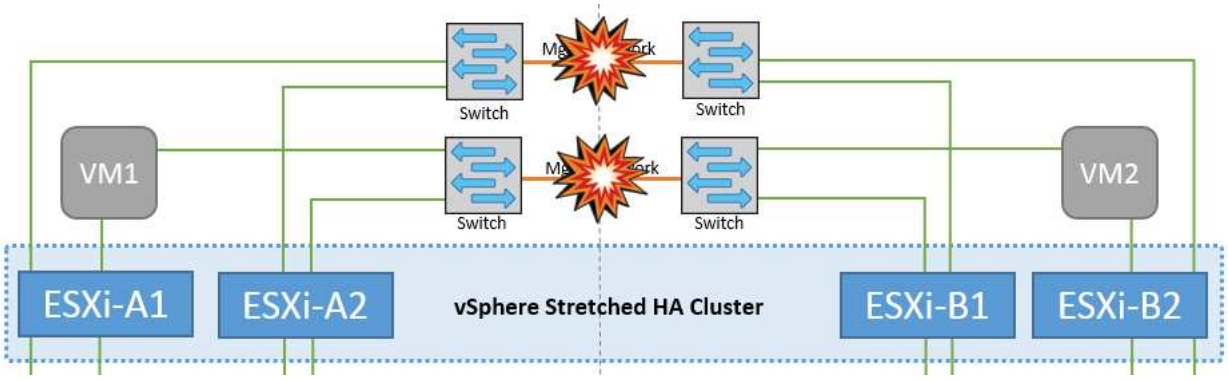
このシナリオでは、一方のサイトの2台のストレージコントローラのどちらかで障害が発生します。各サイトにHAペアがあるため、一方のノードで障害が発生すると、もう一方のノードへのフェイルオーバーが透過的かつ自動的にトリガーされます。たとえば、ノードA1に障害が発生した場合、そのストレージとワークロードは自動的にノードA2に転送されます。すべてのプレックスが引き続き使用可能なため、仮想マシンに影響はありません。2つ目のサイトのノード（B1とB2）は影響を受けません。また、クラスタ内のマスターノードは引き続きネットワークハートビートを受信するため、vSphere HAによる処理は行われません。



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

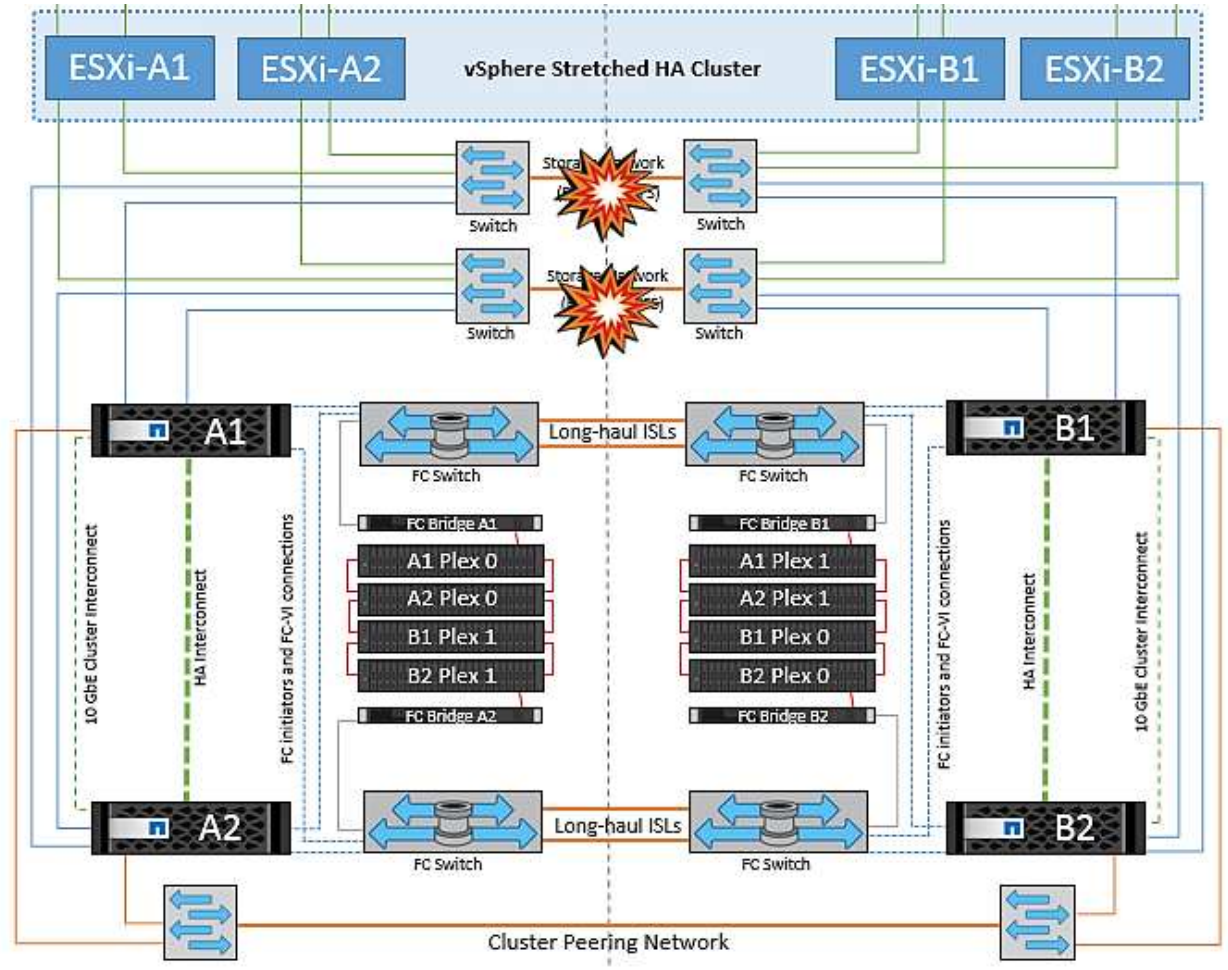
管理ネットワークでのスイッチ間リンク障害



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。

この間、仮想マシンは引き続き実行され、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

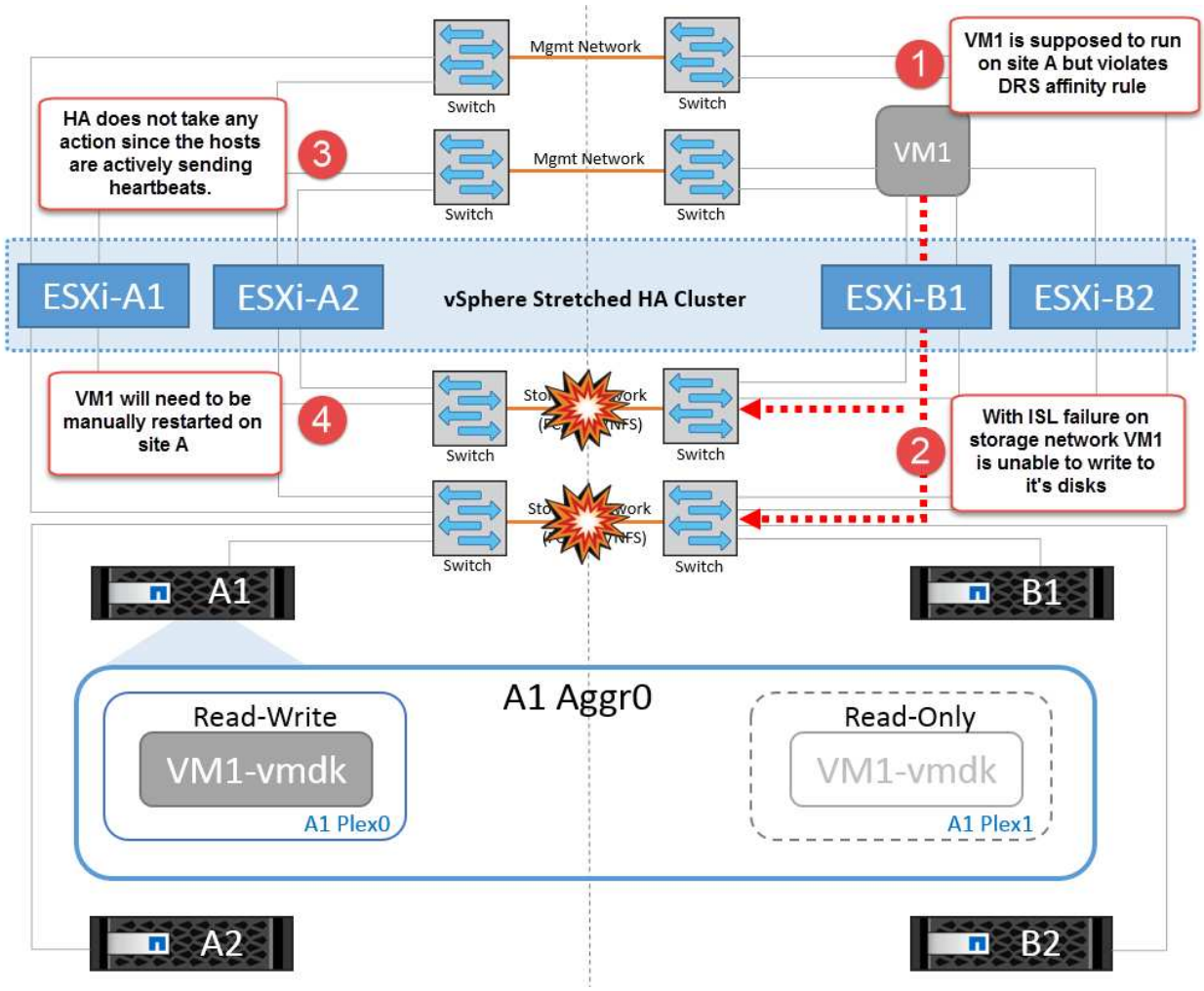


このシナリオでは、バックエンドストレージネットワークのISLリンクで障害が発生すると、サイトAのホストはサイトBのクラスタBのストレージボリュームまたはLUNにアクセスできなくなります。その逆も同様で

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。

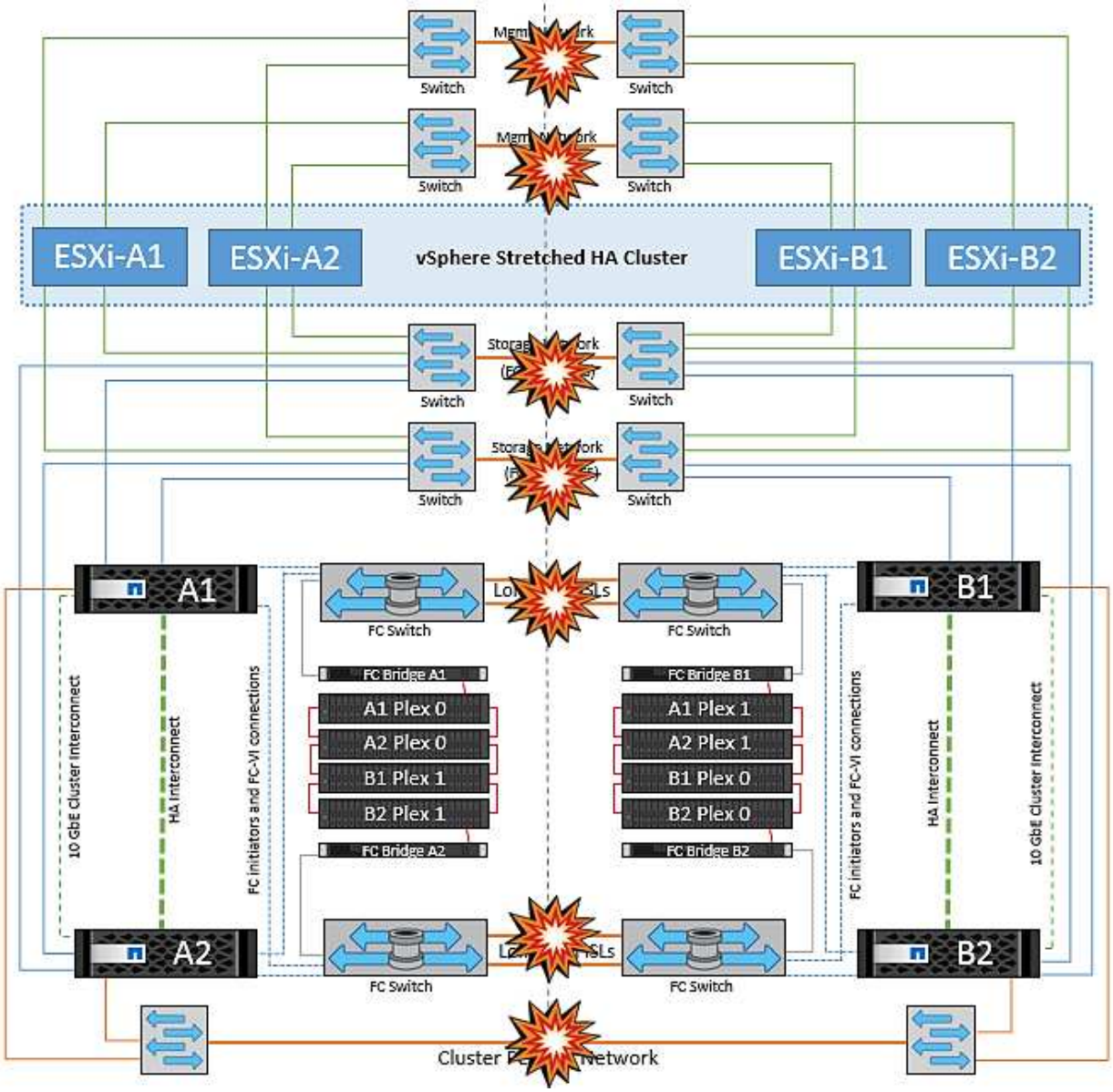


すべてのスイッチ間障害またはデータセンターの完全なパーティション

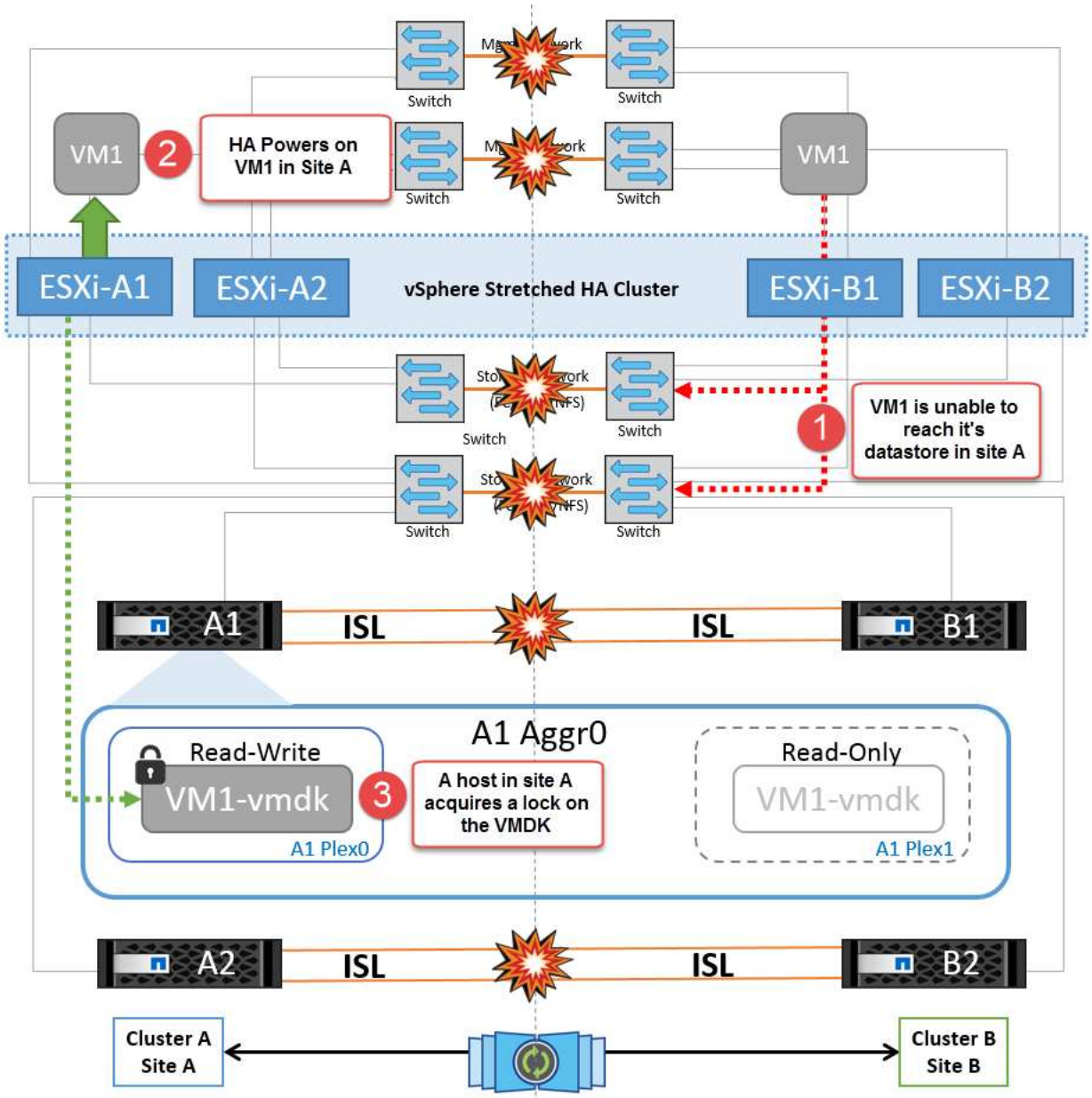
このシナリオでは、サイト間のすべてのISLリンクが停止し、両方のサイトが相互に分離されます。管理ネットワークやストレージネットワークでのISL障害などのシナリオで説明したように、ISL全体で障害が発生しても仮想マシンは影響を受けません。

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それぞれの読み取り/書き込みボリューム/ 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みなします。サイトAのvSphere HAはサイ

トBの仮想マシンを再起動しようとしますが、ストレージISLの障害によってサイト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。



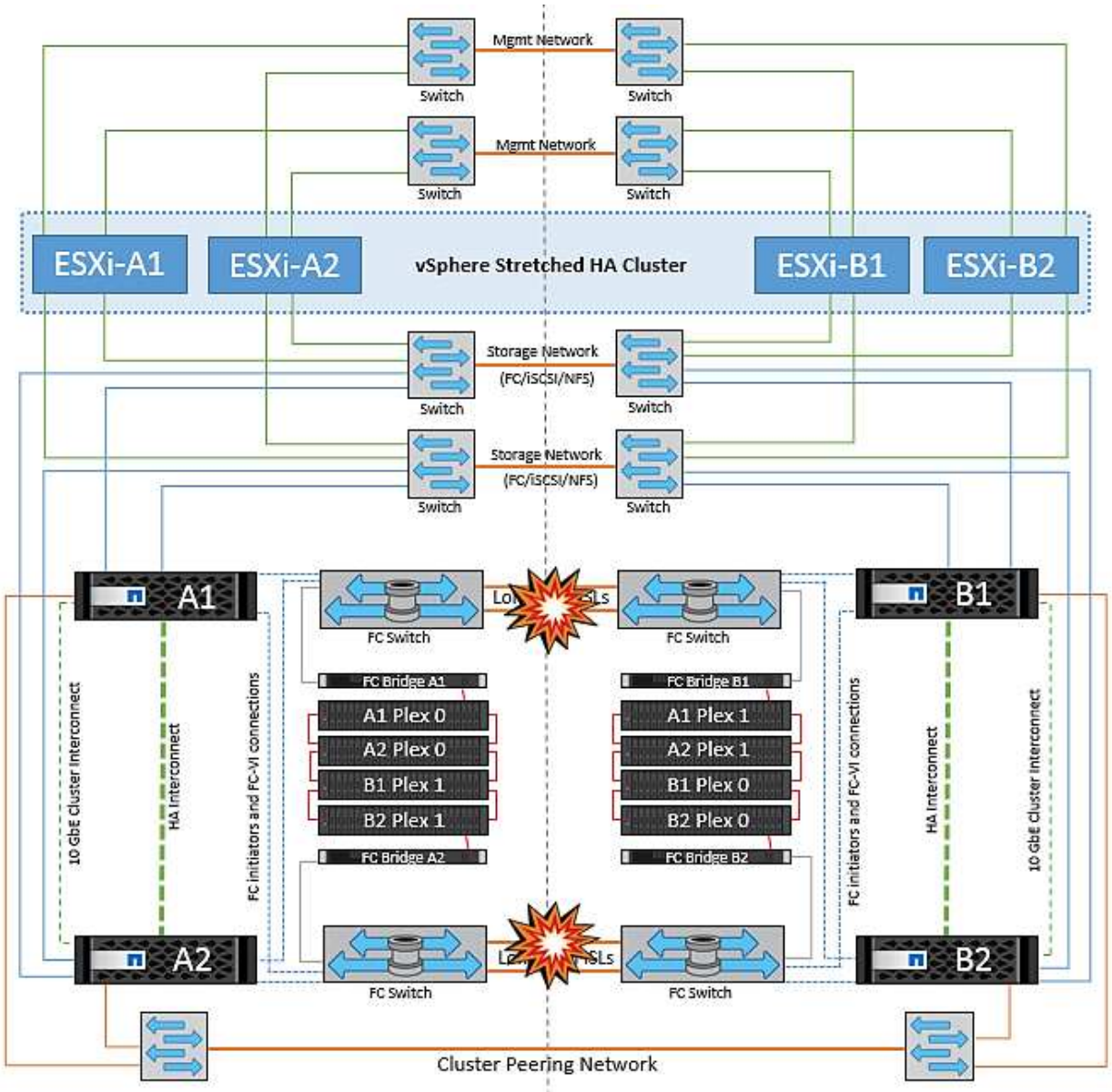
NetAppでは、DRSルールに違反した仮想マシンがないかどうかを確認することを推奨しています。リモートサイトから実行されている仮想マシンはデータストアにアクセスできないため停止し、vSphere HAはその仮想マシンをローカルサイトで再起動します。ISLリンクがオンラインに戻ると、同じMACアドレスで仮想マシンのインスタンスが2つ実行されることはないため、リモートサイトで実行されていた仮想マシンが強制終了されます。



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

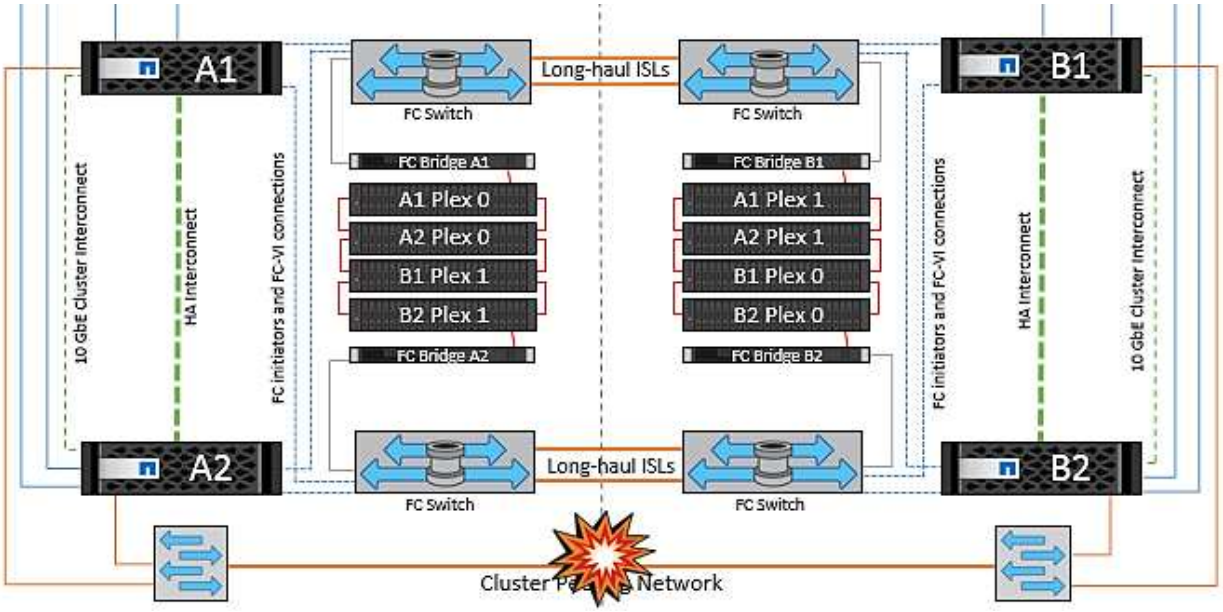
1つ以上のISLで障害が発生した場合、トラフィックは残りのリンクを経由して続行されます。両方のファブリックのすべてのISLで障害が発生し、ストレージとNVRAMのレプリケーション用のサイト間のリンクがなくなった場合、各コントローラはローカルデータの提供を継続します。少なくとも1つのISLがリストアされると、すべてのプレックスの再同期が自動的に実行されます。

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カバリ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。



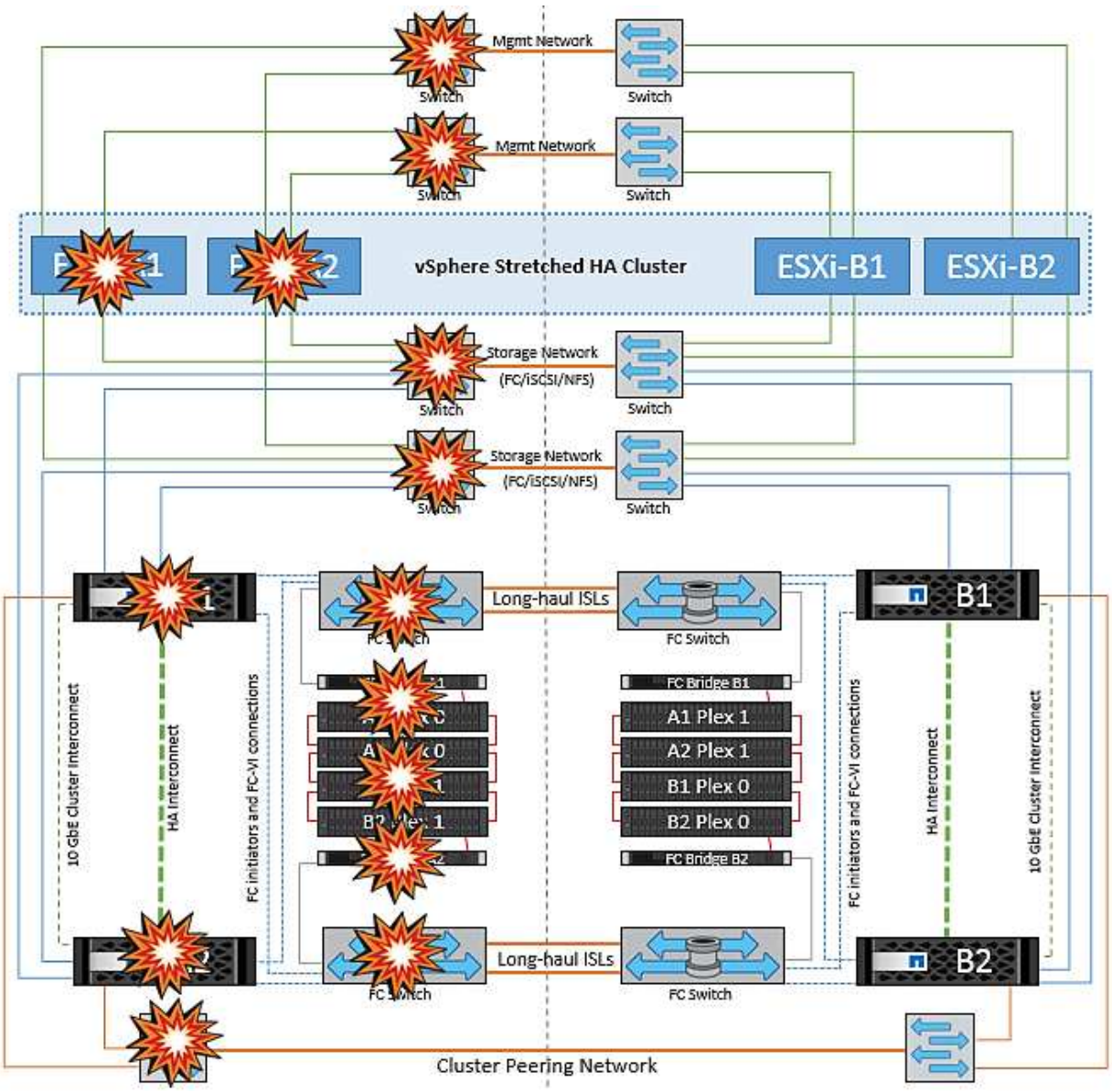
サイト全体の障害

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。

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。そのため、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 SOAP over https 接続に使用されます 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 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 9.13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 9.13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

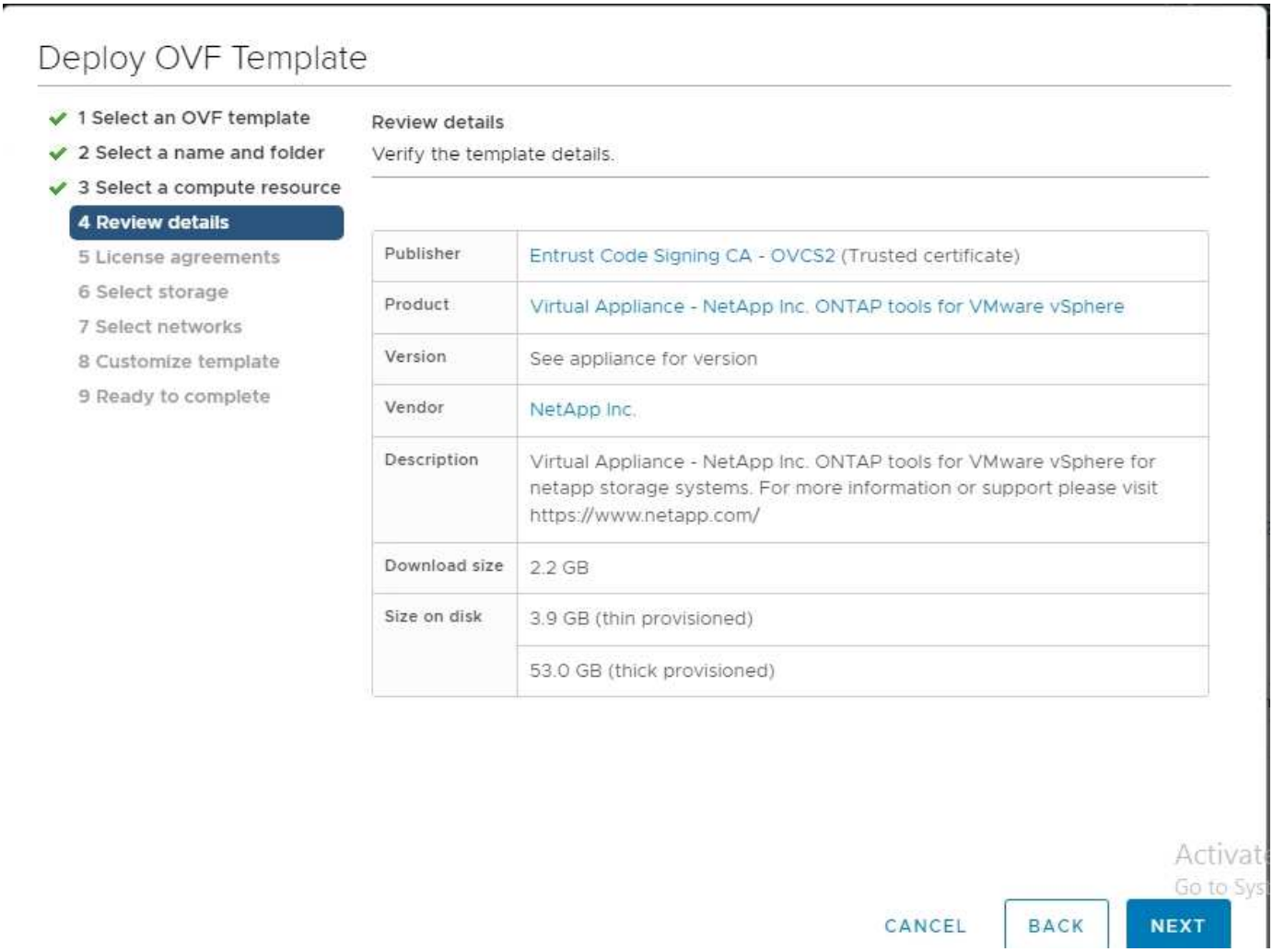
vAppインストールパッケージはtarball形式で提供されます。このtarballには、仮想アプライアンスの中間証明書とルート証明書、READMEファイル、OVAパッケージが含まれています。READMEファイルには、vApp OVAパッケージの整合性を検証する方法が記載されています。

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UI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
```

ONTAP tools 9.13の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+ SOAP over HTTPS接続に使用+ 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+ 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 9.13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。

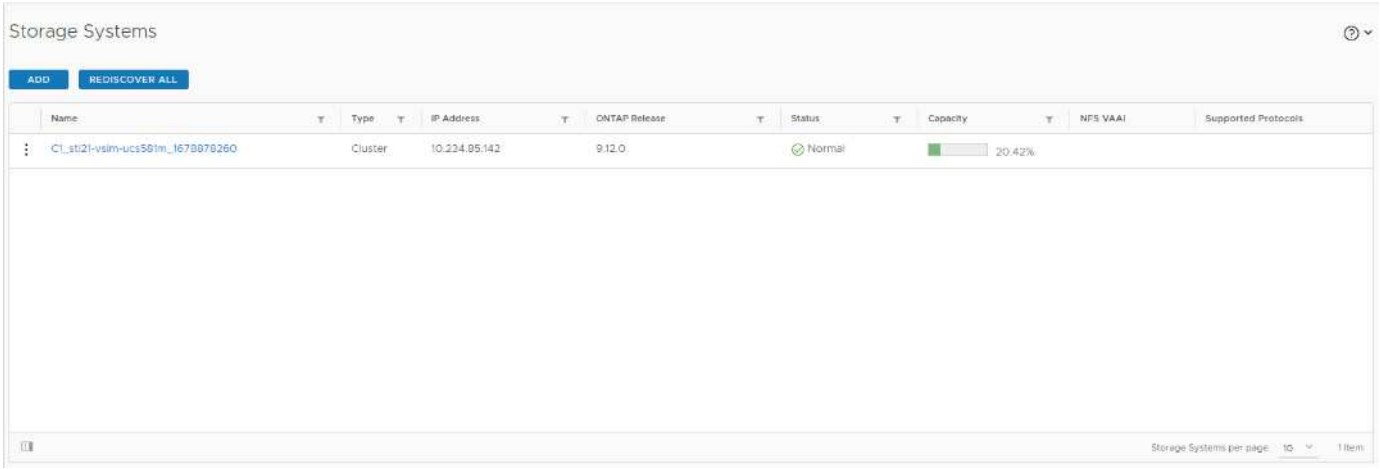
ONTAP tools 9.13相互TLS（証明書ベースの認証）

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

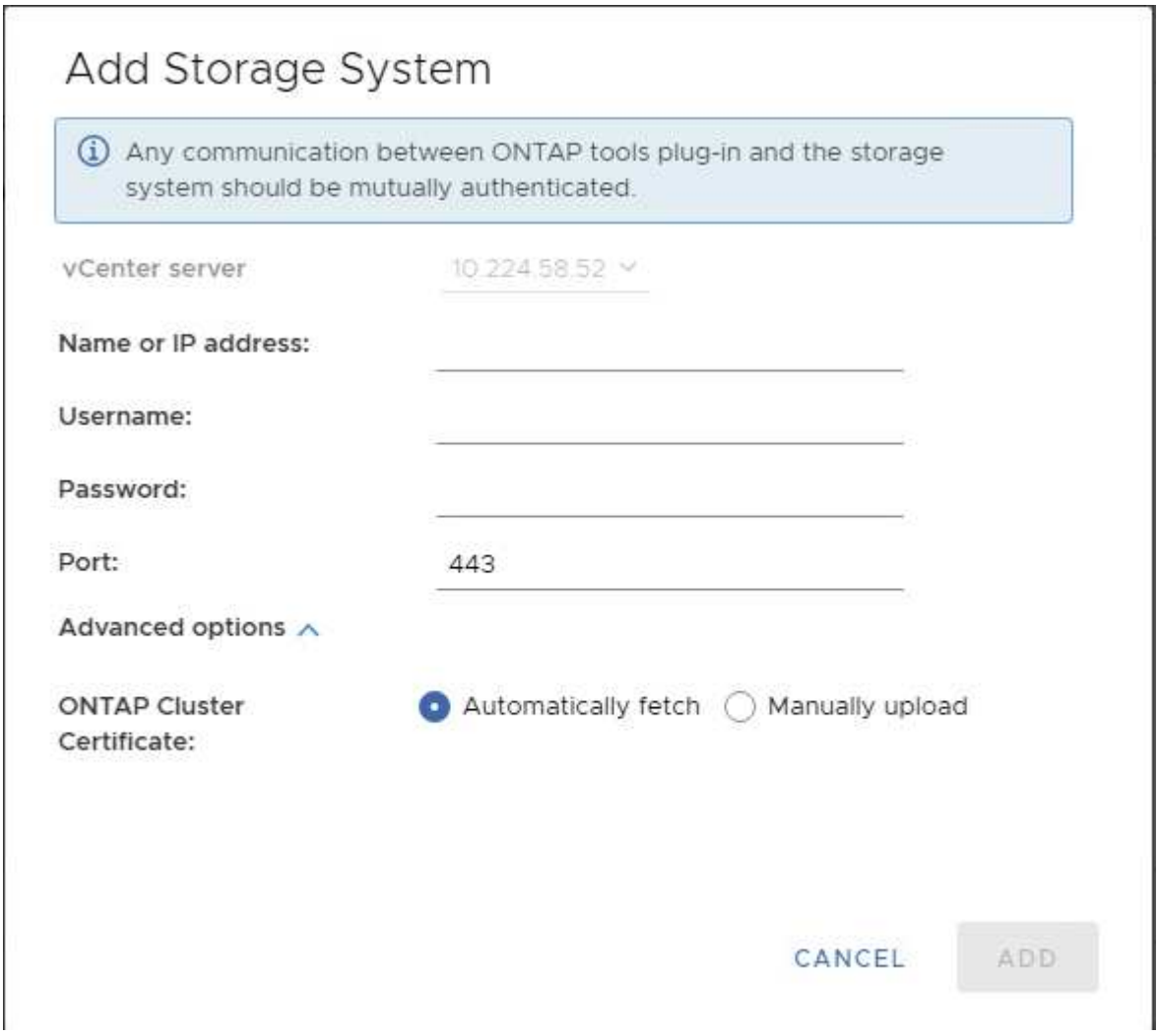
以前に追加されたすべてのストレージシステム：アップグレード中に、追加されたすべてのストレージシステムが自動信頼され、証明書ベースの認証メカニズムが設定されます。

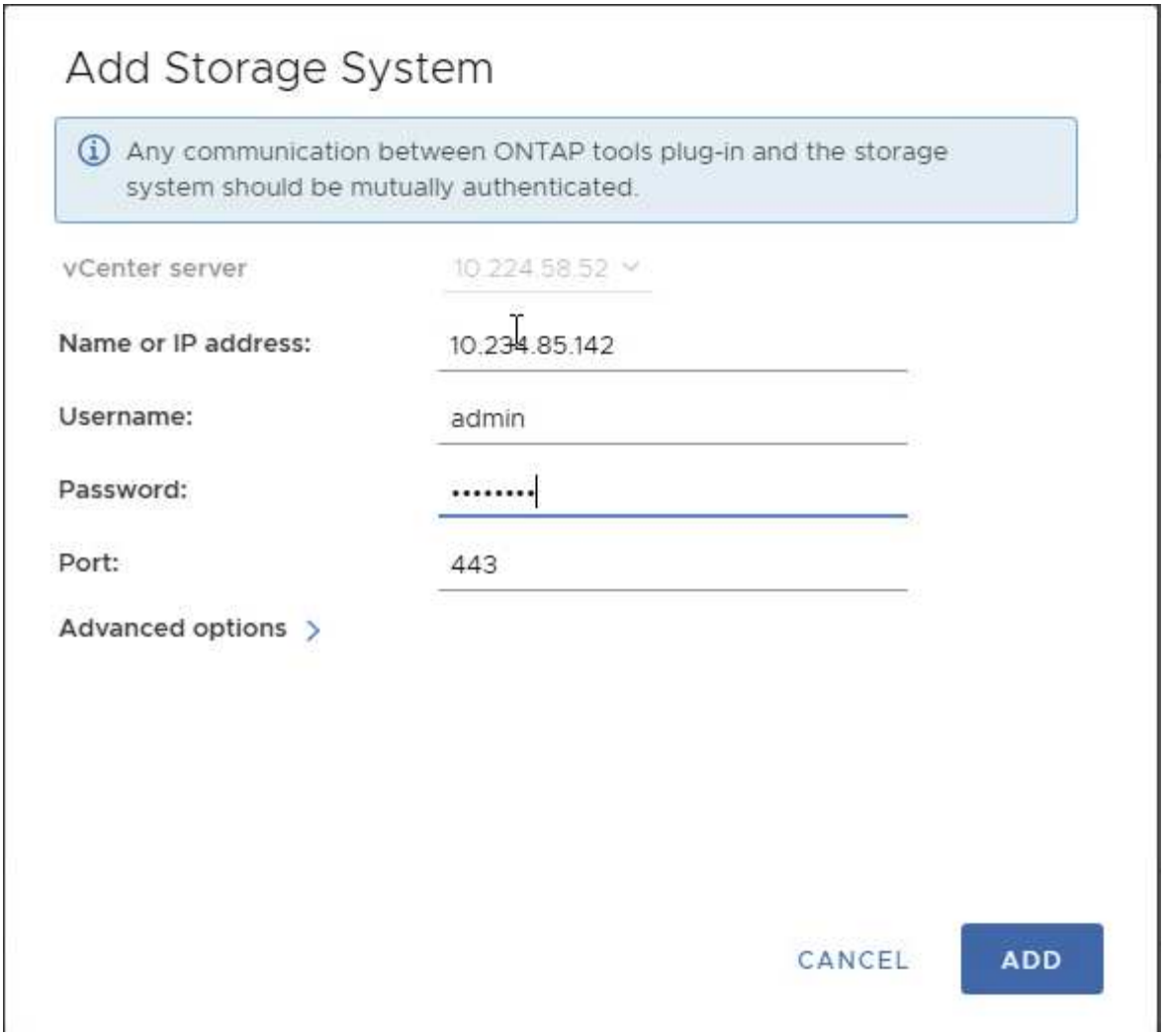
下のスクリーンショットのように、[クラスタセットアップ]ページには、各クラスタに対して設定されたMutual TLS（証明書ベースの認証）のステータスが表示されます。

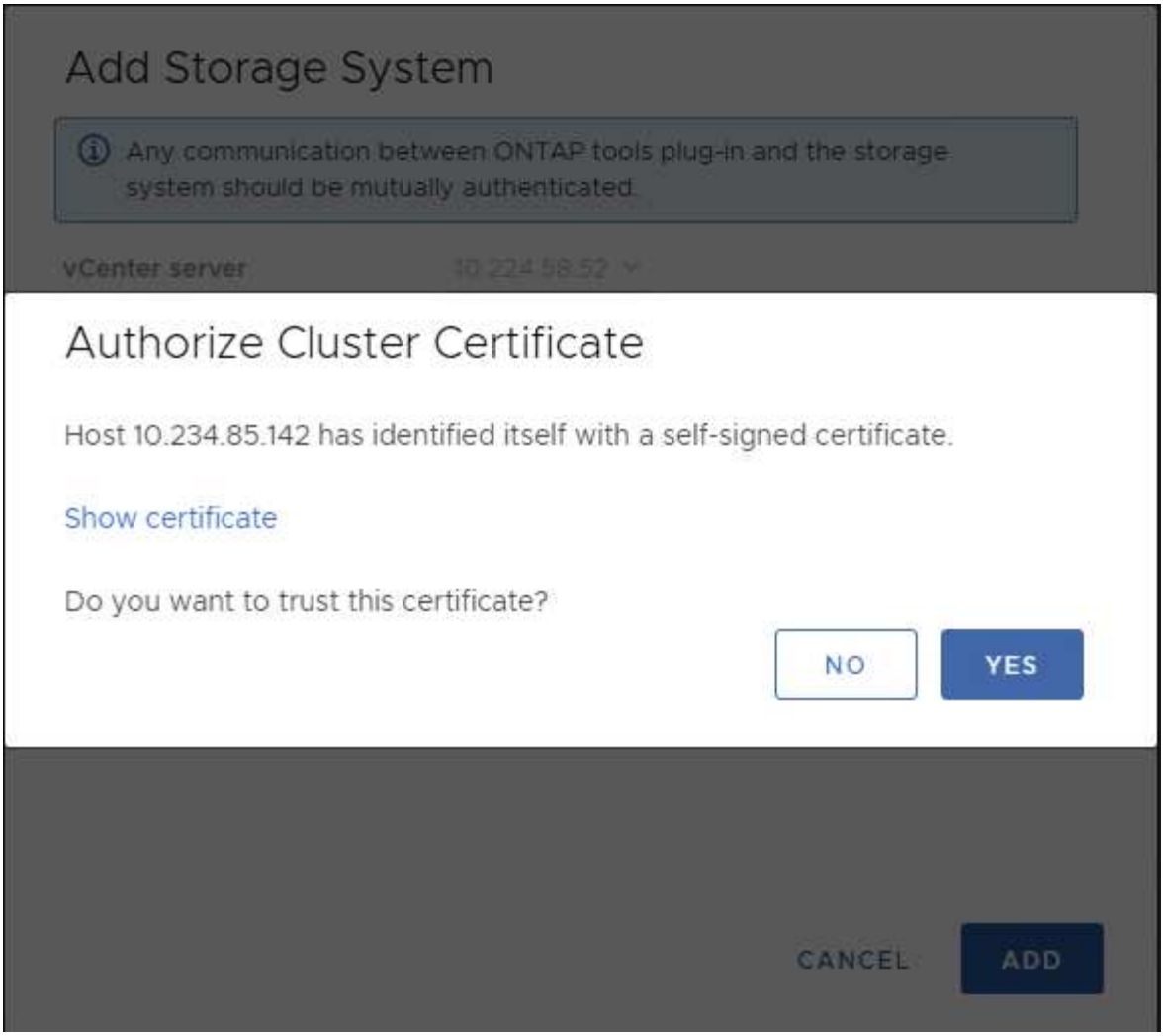


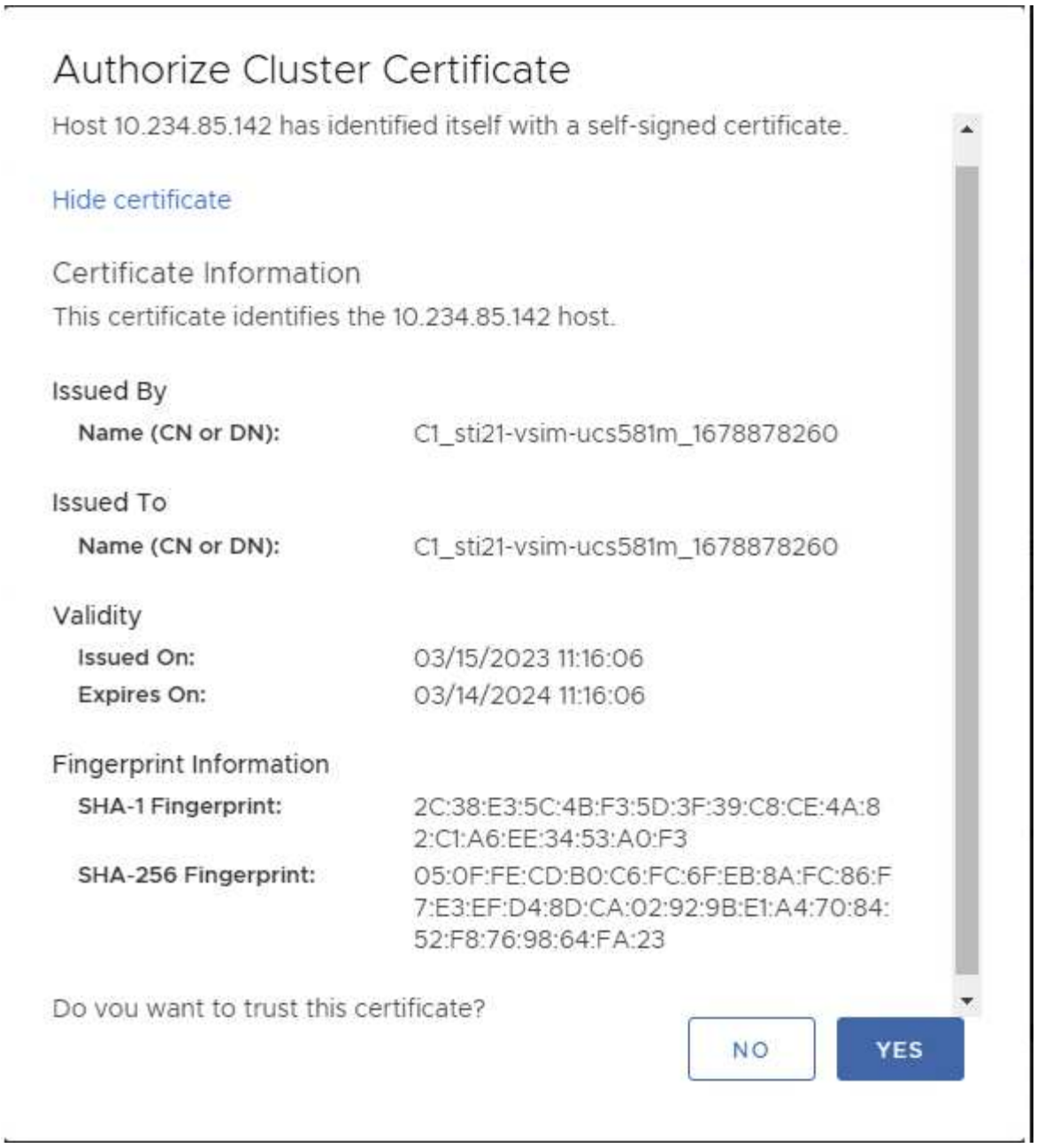
クラスタの追加

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

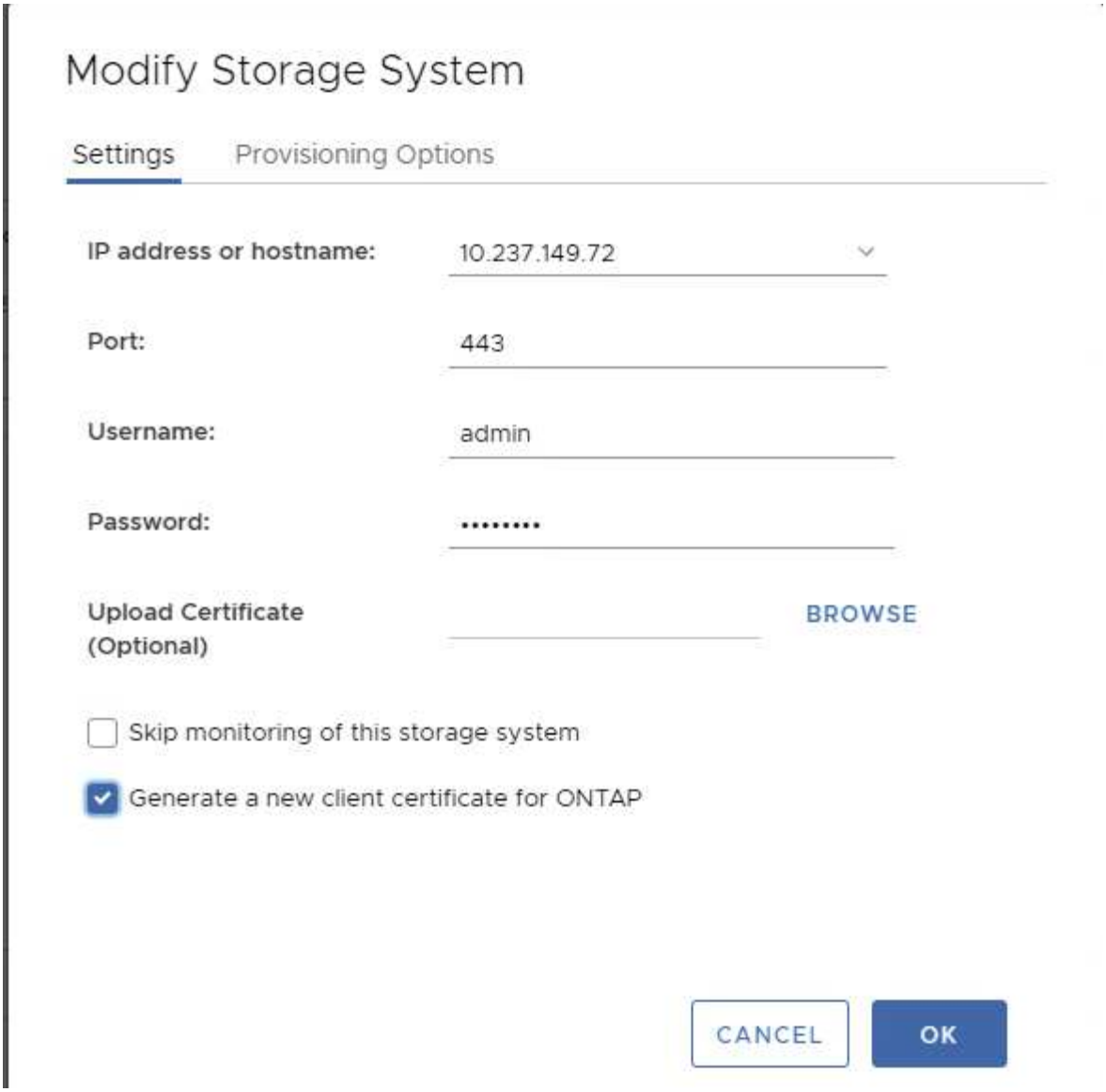

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES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

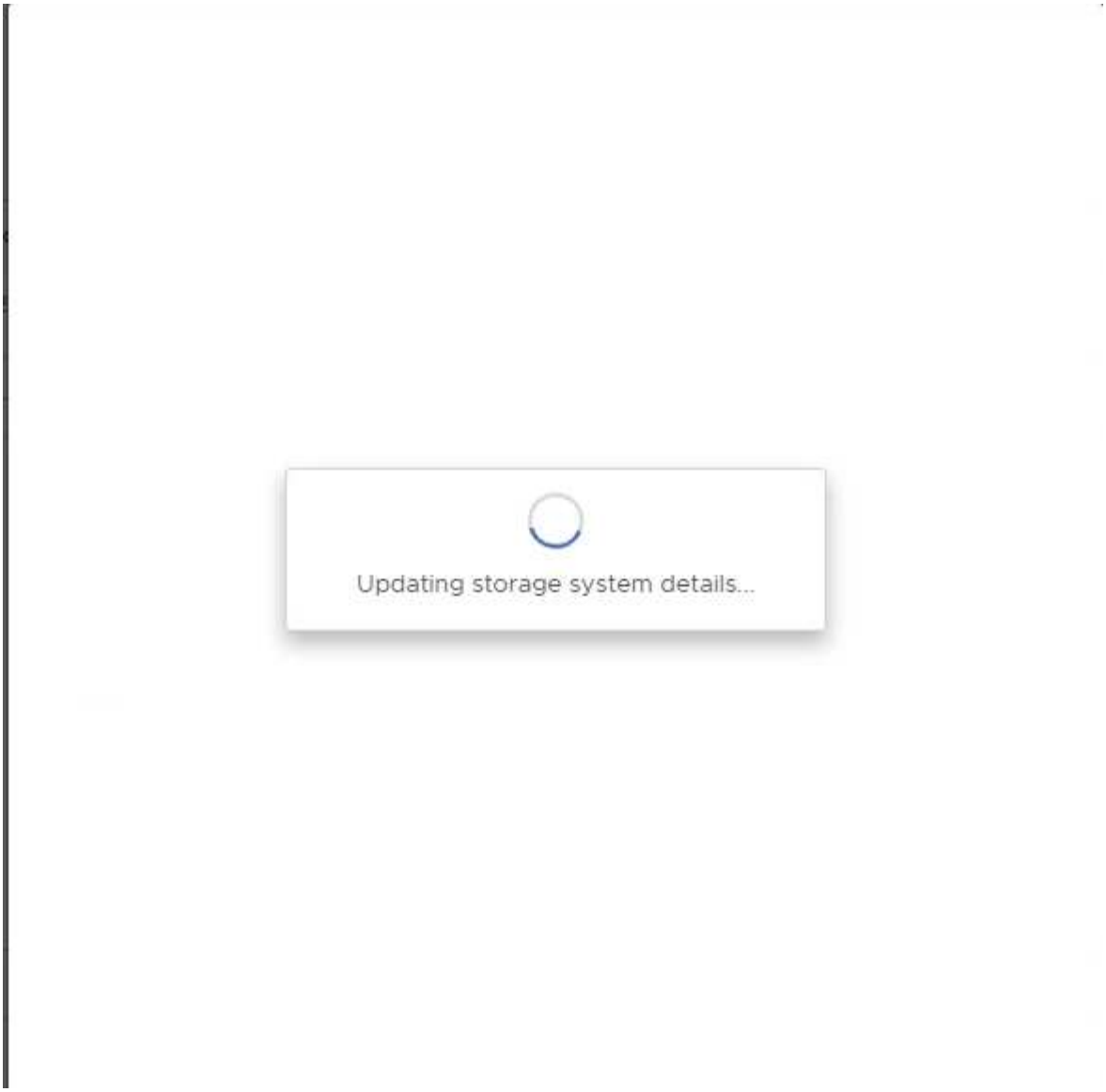


クラスタの編集

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 9.13 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。

ONTAP tools 9.13のログインバナー

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はデフォルトでは無効になっており、VMコンソールから有効にした場合は1回限りのログインが許可されます。

```
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.
```

ONTAP tools 9.13での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。

ユーザー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）VMware vSphere 9.13向けONTAPツール

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"}
```

ONTAP tools 9.13の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。

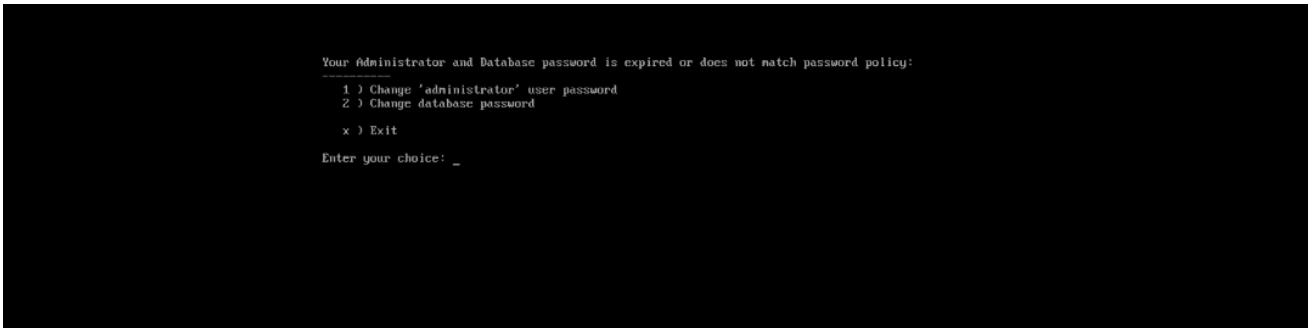
ONTAP tools 9.13のパスワードポリシー

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