ネットアップの SnapMirror によるビジネス継続性機能と ONTAP 9.10 を使用した FlexPod データセンター

FlexPod

NetApp
March 25, 2024

目次

ネットアップの SnapMirror によるビジネス継続性機能と ONTAP 9.10 を使用した FlexPod データセンター

TR-4920 ：『 FlexPod Datacenter with NetApp SnapMirror Business Continuity and ONTAP 9.10 』

Jyh - ネットアップの陳氏をたたきます

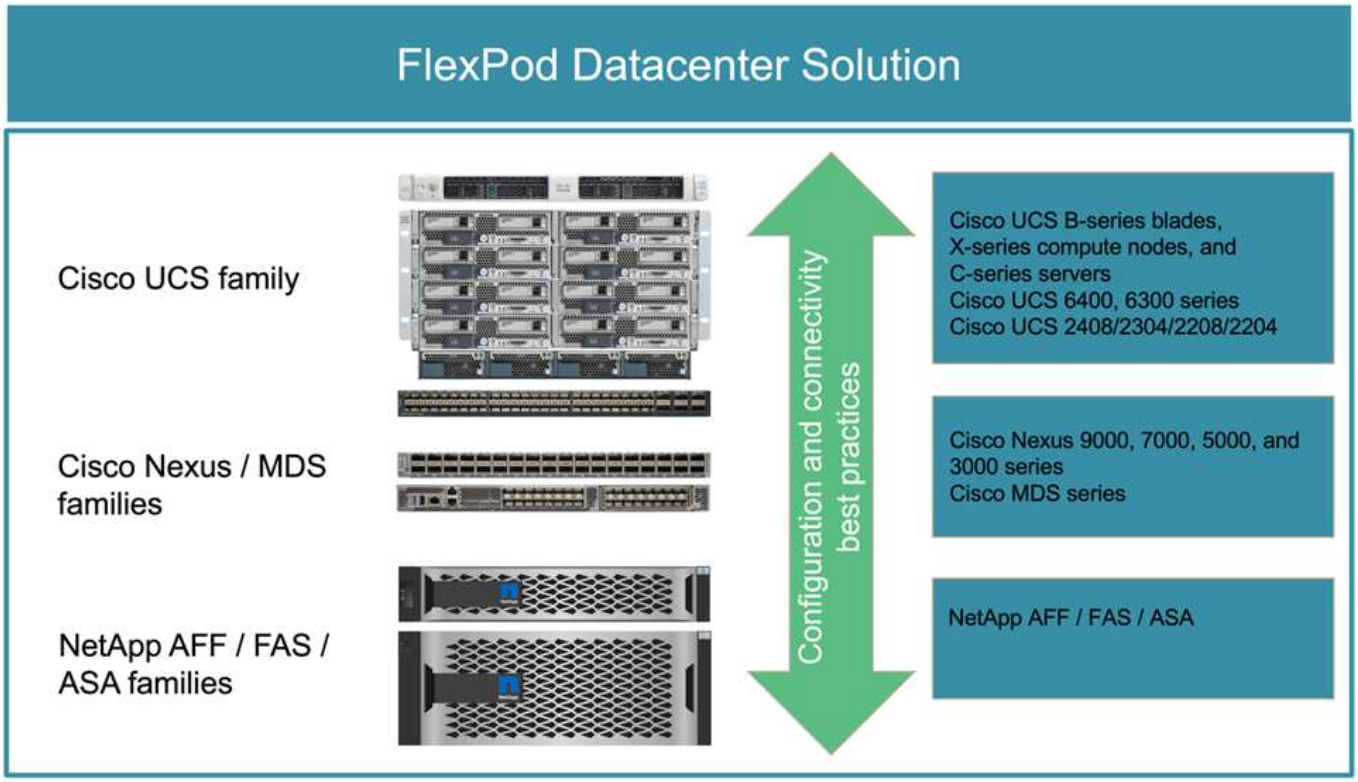
はじめに

FlexPod 解決策

FlexPod は、 Cisco とネットアップが提供する次のコンポーネントで構成される、統合インフラのベストプラクティスデータセンターアーキテクチャです。

- Cisco Unified Computing System （ Cisco UCS ）
- Cisco Nexus および MDS ファミリーのスイッチ
- NetApp FAS 、 NetApp AFF 、ネットアップオール SAN アレイ（ ASA ）システム

次の図は、 FlexPod ソリューションの作成に使用するコンポーネントの一部を示しています。これらのコンポーネントは、 Cisco とネットアップの両方のベストプラクティスに従って接続および構成されており、さまざまなエンタープライズワークロードを確実に実行するための理想的なプラットフォームを提供します。



Cisco Validated Design （ CVD ）や NetApp Verified Architectures （ NVA ）が幅広く用意されています。これらの CVD と NVA は、主要なデータセンターワークロードをすべてカバーしており、ネットアップと Cisco on FlexPod ソリューションとの間で継続的なコラボレーションやイノベーションの成果です。

作成プロセスに広範なテストと検証を組み込むことで、 FlexPod CVD と NVA は、解決策 アーキテクチャのリファレンス設計と段階的な導入ガイドを提供し、パートナー様やお客様が FlexPod ソリューションを導入して採用できるよう支援します。これらの CVD と NVA を設計と実装のガイドとして使用することで、リスクを軽減し、解決策 のダウンタイムを短縮し、導入する FlexPod ソリューションの可用性、拡張性、柔軟性、セキュリティを向上させることができます。

ここに示す FlexPod コンポーネントファミリー（ Cisco UCS 、 Cisco Nexus / MDS スイッチ、ネットアップストレージ）には、インフラをスケールアップまたはスケールダウンするためのプラットフォームオプションとリソースオプションが用意されており、 FlexPod の設定と接続のベストプラクティスに基づいて必要な機能がサポートされています。FlexPod は、複数の一貫した導入が必要な環境でも、追加の FlexPod スタックをロールアウトしてスケールアウトすることができます。

ディザスタリカバリとビジネス継続性

企業がアプリケーションとデータサービスを災害から迅速にリカバリできるようにするためには、さまざまな方法を採用できます。ディザスタリカバリ（ DR ）とビジネス継続性（ BC ）を計画し、ビジネス目標を達成する解決策 を実装し、災害シナリオを定期的にテストすることで、企業は災害からのリカバリが可能となり、災害発生後も重要なビジネスサービスを継続できます。

アプリケーションやデータサービスの種類によって、 DR や BC の要件が異なる場合があります。緊急時や災害時には必要としないアプリケーションやデータもあれば、ビジネス要件に対応するために継続的な可用性が必要となるアプリケーションやデータもあります。

ミッションクリティカルなアプリケーションやデータサービスを利用できない場合は、ビジネスで考慮すべきメンテナンスや災害のシナリオなど、回答 の質問に対して慎重な評価が必要です。 災害発生時にどの程度のデータ損失を許容できるか、リカバリをどのくらいの時間で実施できるか。

収益創出のためにデータサービスに依存解決策 している企業では、さまざまな単一点障害のシナリオに耐えられるだけでなく、継続的なビジネス運用を可能にするためにサイト障害のシナリオによってデータサービスを保護する必要があります。

目標復旧時点と目標復旧時間

Recovery Point Objective （ RPO ；目標復旧時点）は、損失やデータのリカバリ先となるデータの量を、時間の観点から測定します。日々のバックアップ計画では、企業が 1 日分のデータを失うことがあります。これは、前回のバックアップ以降に行われたデータの変更が災害で失われる可能性があるためです。ビジネスクリティカルなデータサービスやミッションクリティカルなデータサービスの場合、 RPO ゼロ、およびデータ損失ゼロの関連計画とインフラが求められることがあります。

Recovery Time Objective （ RTO ；目標復旧時間）は、データを使用できない時間、またはデータサービスを復旧するまでにどれくらいの時間がかかるかを測定します。たとえば、バックアップとリカバリを実装しており、サイズによっては特定のデータセットに対して従来のテープを使用する場合があります。このため、バックアップテープからデータをリストアするには、数時間かかる場合もあれば、インフラに障害が発生している場合は数日かかる場合もあります。時間の考慮事項には、データのリストアに加えて、インフラをバックアップする時間も考慮する必要があります。ミッションクリティカルなデータサービスの場合、 RTO が非常に低く、ビジネスの継続性を維持するためにデータサービスを迅速にオンラインに戻すために数秒から数分のフェイルオーバー時間しか許容されないことがあります。

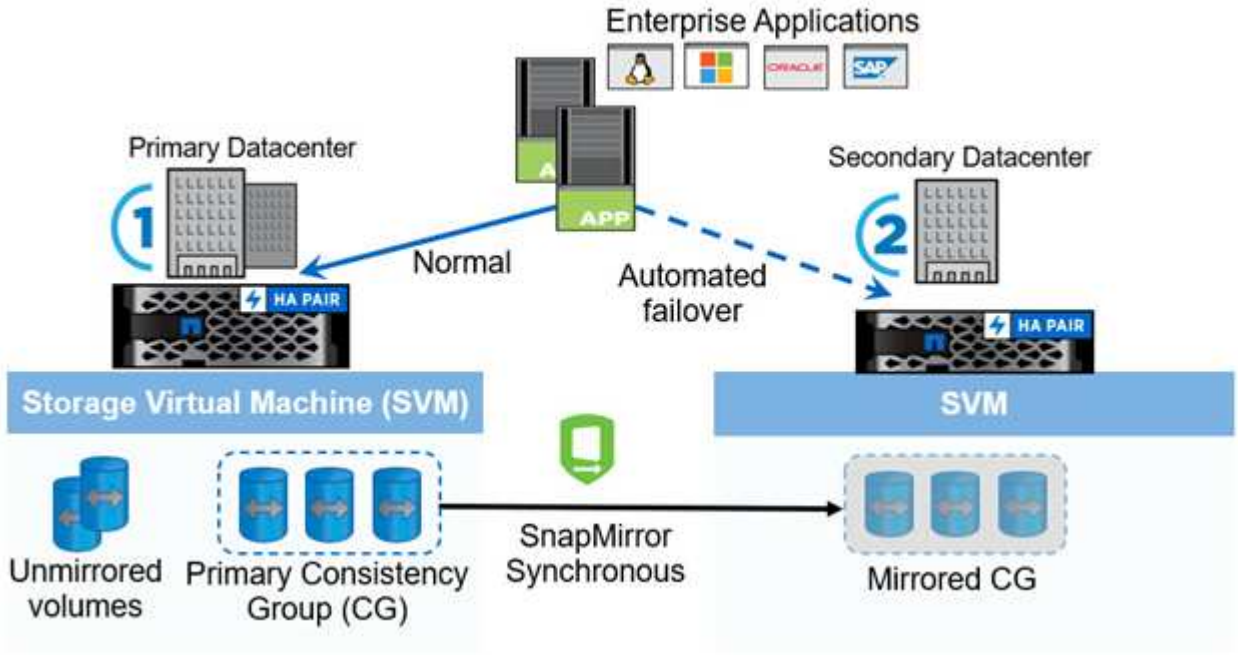
SM-BC です

ONTAP 9.8 以降では、 NetApp SM-BC を使用して、 SAN ワークロードを保護して透過的なアプリケーションフェイルオーバーを実現できます。データレプリケーション用に 2 つの AFF クラスタ間または 2 つの ASA クラスタ間に整合グループ関係を作成することで、 RPO をゼロ、 RTO をほぼゼロにすることができます。

SM-BC 解決策 は、 IP ネットワーク上で SnapMirror Synchronous テクノロジを使用してデータを複製します。アプリケーションレベルのきめ細かさと自動フェイルオーバー機能を提供し、 iSCSI または FC プロトコルベースの SAN LUN を使用して、 Microsoft SQL Server や Oracle などのビジネスクリティカルなデータサービスを保護します。3 番目のサイトに導入された ONTAP メディエーターは、 SM-BC 解決策 を監視し、サイト障害時の自動フェイルオーバーを有効にします。

整合グループ（ CG ）は、アプリケーションワークロードに対して書き込み順序の整合性が保証される FlexVol ボリュームの集まりで、ビジネス継続性のために保護する必要があります。一度に複数のボリュームについて、 crash-consistent Snapshot コピーを同時に作成できます。SnapMirror 関係は、 CG 関係とも呼ばれ、ソース CG とデスティネーション CG の間に確立されます。CG に属するボリュームグループを、アプリケーションインスタンス、アプリケーションインスタンスのグループ、または解決策 全体にマッピングできます。また、ビジネス要件や変更に基づいて、 SM-BC 整合グループ関係をオンデマンドで作成または削除できます。

次の図に示すように、整合グループ内のデータは、ディザスタリカバリとビジネス継続性のために 2 つ目の ONTAP クラスタにレプリケートされます。アプリケーションは両方の ONTAP クラスタ内の LUN に接続されています。通常はプライマリクラスタが I/O を処理し、プライマリで災害が発生するとセカンダリクラスタから自動的に再開します。SM-BC 解決策 を設計する場合は、サポートされる制限を超えないように、 CG 関係でサポートされるオブジェクト数（最大 20 個の CG 、最大 200 個のエンドポイントなど）を確認する必要があります。



"次の例は、 FlexPod SM-BC 解決策 です。"

FlexPod SM-BC 解決策 の略

"前へ：はじめに。"

解決策の概要

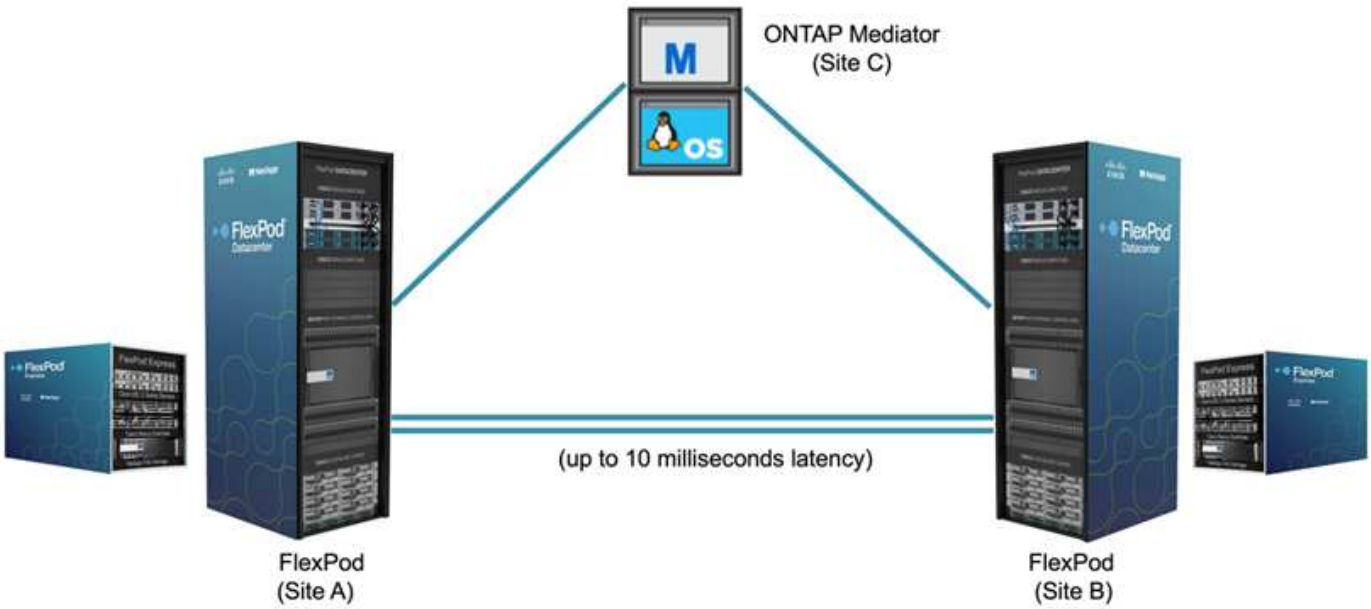
FlexPod SM-BC 解決策 は、高いレベルで 2 つの FlexPod システムで構成されています。これらのシステムは、ある程度離れた場所に設置され、接続され、ペアリングされているため、可用性が高く、柔軟性と信頼性に優れたデータセンター解決策 を提供し、サイト障害時にもビジネス継続性を提供できます。

2 つの新しい FlexPod インフラを導入して FlexPod SM-BC 解決策 を作成するだけでなく、 SM-BC と互換性のある既存の 2 つの FlexPod インフラに解決策 を実装したり、既存の FlexPod とピア関係を構築するために新しい FlexPod を追加したりすることもできます。

FlexPod SM-BC 解決策 の 2 つの FlexPod システムは、設定で同じである必要はありません。ただし、 2 つの ONTAP クラスタは同じストレージファミリーである必要があります。 2 つの AFF システムまたは 2 つの ASA システムのどちらかですが、必ずしも同じハードウェアモデルである必要はありません。SM-BC 解決策 は FAS システムをサポートしません。

2 つの FlexPod サイトには、解決策 の帯域幅とサービス品質の要件を満たすネットワーク接続が必要です。また、 ONTAP SM-BC 解決策 で必要とされる、サイト間のラウンドトリップレイテンシは 10 ミリ秒（ 10 ミリ秒）未満です。この FlexPod SM-BC 解決策 検証では、同じラボの拡張レイヤ 2 ネットワークを介して 2 つの FlexPod サイトが相互接続されます。

NetApp ONTAP SM-BC 解決策 は、キャンパスエリアまたはメトロポリタンエリアにおける高可用性とディザスタリカバリを実現するために、 2 つのネットアップストレージクラスタ間で同期レプリケーションを提供します。第 3 のサイトに導入された ONTAP メディエーターは解決策 を監視し、サイト障害が発生した場合に自動フェイルオーバーを可能にします。次の図に、解決策 コンポーネントの概要を示します。



FlexPod SM-BC 解決策 を使用すると、 VMware vSphere ベースのプライベートクラウドを、分散した統合インフラストラクチャ上に導入できます。解決策 の統合により、複数のサイトを単一の解決策 インフラとして調整し、さまざまな単一点障害のシナリオとサイト全体の障害からデータサービスを保護することができます。

このテクニカルレポートでは、 FlexPod SM-BC 解決策 の設計に関するエンドツーエンドの考慮事項をいくつか紹介します。その他の FlexPod 解決策 実装の詳細については、 FlexPod CVD や NVA に掲載されている情報を参照することを推奨します。

解決策 は、 CVD に記載されている FlexPod のベストプラクティスに基づいて 2 つの FlexPod システムを導入することで検証されましたが、 SM-BC 解決策 の要件を考慮しています。このレポートで説明している FlexPod SM-BC 解決策 は、さまざまな障害シナリオでの耐障害性とフォールトトレランスのほか、サイト障害のシミュレーションシナリオで検証されています。

解決策の要件

FlexPod SM-BC 解決策 は、次の主要な要件に対応するように設計されています。

- データセンター（サイト）全体で障害が発生した場合の、ビジネスクリティカルなアプリケーションおよびデータサービスのビジネス継続性
- データセンター間でワークロードを移動できる柔軟な分散型ワークロード配置
- 通常運用時に、同じデータセンターサイトからローカルに仮想マシンデータがアクセスされるサイトアフィニティ
- サイト障害発生時にデータ損失ゼロで迅速にリカバリできます

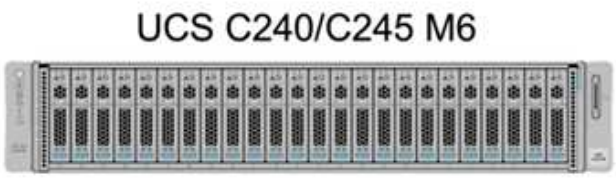
解決策コンポーネント

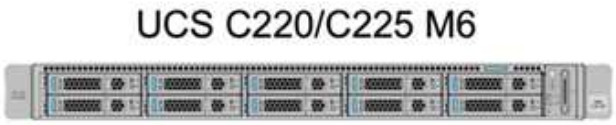
Cisco のコンピューティングコンポーネント

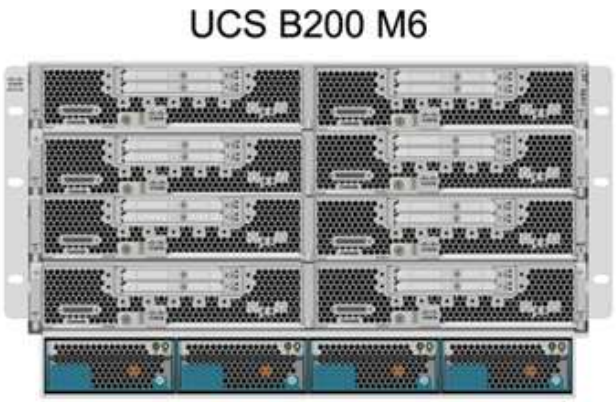
Cisco UCS は、ユニファイドコンピューティングリソース、ユニファイドファブリック、統合管理を提供する統合コンピューティングインフラです。仮想化やベアメタルワークロードなどのアプリケーションの導入を自動化し、高速化できます。Cisco UCS は、リモートとブランチオフィス、データセンター、ハイブリッドクラウドのユースケースなど、さまざまな導入ユースケースに対応しています。解決策 の具体的な要件に応じて、 FlexPod のシスコのコンピューティング実装では、さまざまな規模のコンポーネントを利用できます。次のサブセクションでは、一部の UCS コンポーネントについて追加情報 を説明します。

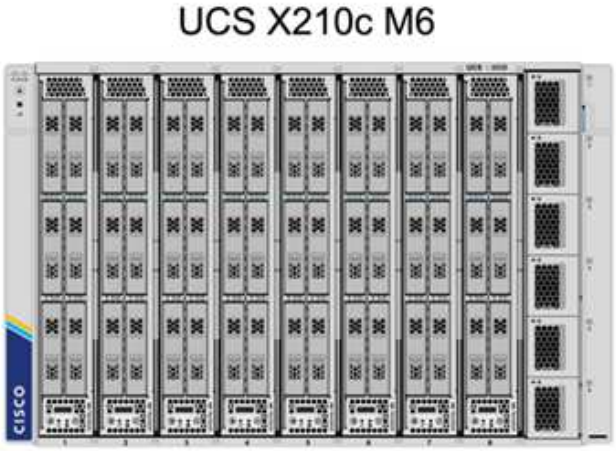
UCS サーバとコンピューティングノード

次の図に、 UCS C シリーズラックサーバ、 B シリーズブレードサーバを搭載した UCS 5108 シャーシ、 X シリーズコンピューティングノードを搭載した新しい UCS X9508 シャーシなど、 UCS サーバコンポーネントの例を示します。Cisco UCS C シリーズラックサーバには、 1 ラックユニット（ RU ）と 2 ラックユニット（ RU ）のフォームファクタ、 Intel および AMD CPU ベースのモデル、およびさまざまな CPU 速度とコア、メモリ、 I/O オプションが用意されています。Cisco UCS B シリーズブレードサーバと新しい X シリーズコンピューティングノードには、さまざまな CPU 、メモリ、 I/O オプションが用意されており、これらはすべて FlexPod アーキテクチャでサポートされているため、多様なビジネス要件に対応できます。









この図に示す最新世代の C220 、 C225 、 C240 、 C245 M6 ラックサーバ、 B200 M6 ブレードサーバ、および X210c コンピューティングノードに加えて、従来世代のラックサーバおよびブレードサーバも引き続きサポートされている場合に使用できます。

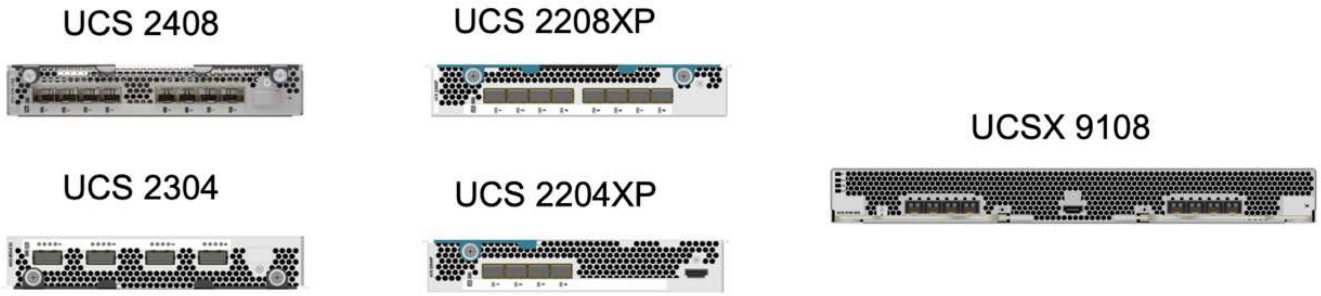
I/O モジュールおよびインテリジェントファブリックモジュール

I/O モジュール（ IOM ） / ファブリックエクステンダおよび Intelligent Fabric Module （ IFM ）は、 Cisco UCS 5108 ブレードサーバシャーシと Cisco UCS X9508 X シリーズシャーシのユニファイドファブリック接続を提供します。

第 4 世代の UCS IOM 2408 には、 UCS 5108 シャーシとファブリックインターコネクト（ FI ）を接続するための 8 つの 25 G ユニファイドイーサネットポートがあります。各 2408 には、ミッドプレーン経由でシャーシ内の各ブレードサーバへの 4 つの 10-G バックプレーンイーサネット接続があります。

UCSX 9108 25G IFM には、ファブリックインターコネクトを使用して UCS X9508 シャーシ内のブレードサーバを接続するための、 8 個の 25 G ユニファイドイーサネットポートがあります。各 9108 には、 X9108 シャーシの各 UCS X210c コンピューティングノードへの 25 G 接続が 4 つあります。9108 IFM は、ファブリックインターコネクトと連携してシャーシ環境を管理します。

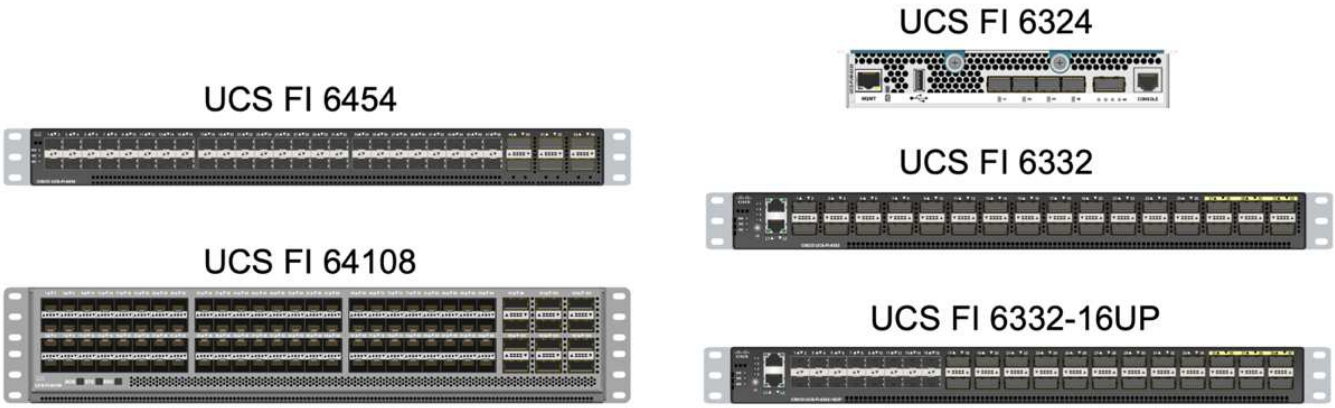
次の図は、 UCS 5108 シャーシの場合は UCS 2408 以前の IOM 世代、 X9508 シャーシの場合は 9108 IFM を示しています。



UCS ファブリックインターコネクト

Cisco UCS Fabric Interconnect （ FI ）は、 Cisco UCS 全体の接続性と管理を提供します。通常、システムの FI はアクティブ / アクティブペアとして展開され、すべてのコンポーネントを Cisco UCS Manager または Cisco Intersight によって制御される、可用性の高い単一の管理ドメインに統合します。Cisco UCS FI は、単一のケーブルセットを使用して LAN 、 SAN 、および管理トラフィックをサポートする低遅延でロスレスなカットスルースイッチングを提供する、単一のユニファイドファブリックをシステムに提供します。

第 4 世代の Cisco UCS FI には、 UCS FI 6454 と 64108 の 2 つのバリエーションがあります。10 / 25GbE イーサネットポート、 1 / 10 / 25Gbps イーサネットポート、 40 / 100Gbps イーサネットアップリンクポート、および 10 / ギガビットイーサネットまたは 8 / 16 / 32 Gbps ファイバチャネルをサポートするユニファイドポートのサポートが含まれます。次の図に、第 4 世代の Cisco UCS FI と、サポートされている第 3 世代のモデルを示します。

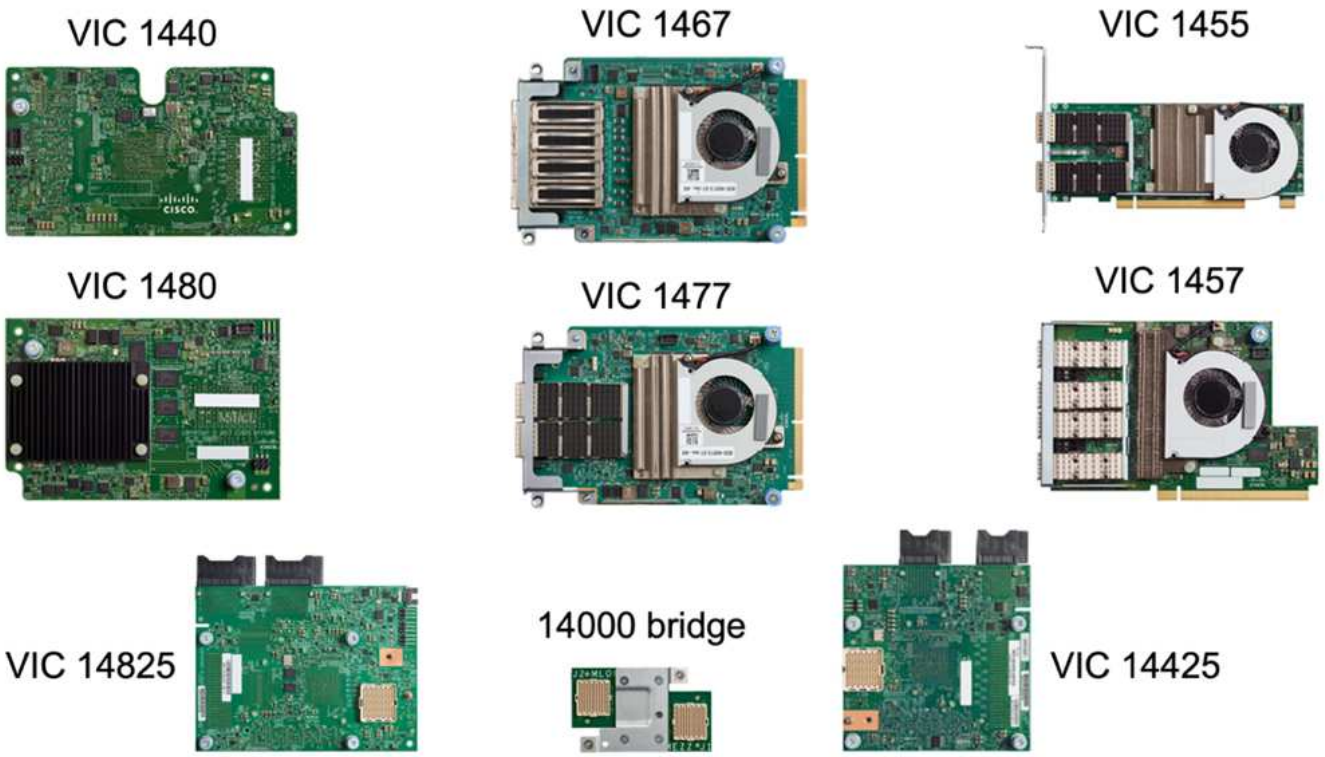


Cisco UCS X シリーズシャーシをサポートするには、 Intersight Managed Mode （ IMM ）で設定された第 4 世代のファブリックインターコネクトが必要です。ただし、 Cisco UCS 5108 B シリーズシャーシは、 IMM モードと UCSM 管理モードの両方でサポートできます。

UCS FI 6324 は IOM フォームファクタを使用し、 UCS Mini シャーシに組み込まれているため、小規模な UCS ドメインだけを必要とする導入に適しています。

UCS 仮想インターフェイスカード

Cisco UCS 仮想インターフェイスカード（ VIC ）は、ラックサーバやブレードサーバのシステム管理と LAN および SAN 接続を統合します。仮想ネットワークインターフェイスカード（ vNIC ）として、または Cisco SingleConnect テクノロジーを使用する仮想ホストバスアダプタ（ vHBA ）として、最大 256 の仮想デバイスをサポートします。仮想化の結果、 VIC カードによってネットワーク接続が大幅に簡易化され、解決策 の導入に必要なネットワークアダプタ、ケーブル、スイッチポートの数が削減されます。次の図は、 B シリーズおよび C シリーズのサーバと X シリーズのコンピューティングノードで使用できる Cisco UCS VIC の一部を示しています。



アダプタモデルによって、ポート数、ポート速度、モジュラ LAN on Motherboard （ mLOM ）、メザニンカード、 PCIe インターフェイスのフォームファクタが異なるブレードサーバとラックサーバがサポートされます。このアダプタは、 10/25/40/100-G イーサネットと Fibre Channel over Ethernet （ FCoE ）の組み合わせをサポートしています。シスコの Converged Network Adapter （ CNA; 統合ネットワークアダプタ）テクノロジーを採用し、包括的な機能セットをサポートし、アダプタ管理とアプリケーションの導入を簡素化します。たとえば、 VIC は、 Cisco UCS ファブリックインターコネクトポートを仮想マシンに拡張するシスコのデータセンター仮想マシンファブリックエクステンダ（ VM-FEX ）テクノロジーをサポートしているため、サーバ仮想化の導入が簡素化されます。

mLOM 、メザニン、およびポートエキスパンダとブリッジカード構成に Cisco VIC を組み合わせることで、ブレードサーバで利用できる帯域幅と接続性を最大限に活用できます。たとえば、 VIC 14825 （ mLOM ）と 14425 （メザニン）の 2 つの 25 G リンクと、 X210c コンピューティングノードの 14000 （ブリッジカード）を使用することで、 VIC 帯域幅の組み合わせは 2 x 50 - G + 2 x 50 - G 、 または、ファブリック /IFM あたり 100G 、およびデュアル IFM 構成のサーバあたり合計 200G 。

Cisco UCS 製品ファミリ、技術仕様、およびマニュアルの詳細については、を参照してください "Cisco UCS の場合" Web サイトを参照してください。

Cisco スイッチングコンポーネント

Nexus スイッチ

FlexPod は、 Cisco Nexus シリーズスイッチを使用して、 Cisco UCS とネットアップストレージコントローラ間の通信用のイーサネットスイッチファブリックを提供します。現在サポートされている Cisco Nexus スイッチモデル（ Cisco Nexus 3000 、 5000 、 7000 、 9000 シリーズを含む）は、すべて FlexPod 環境でサポートされています。

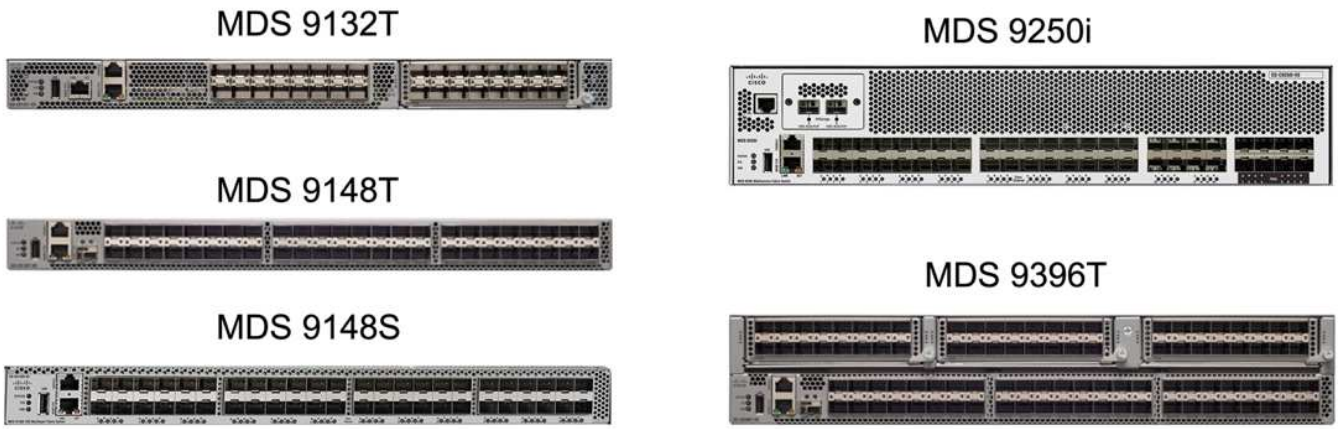
FlexPod 環境のスイッチモデルを選択する際には、パフォーマンス、ポート速度、ポート密度、スイッチング遅延など、さまざまな要因を考慮する必要があります。 また、 ACI や VXLAN などのプロトコルをサポートしているため、設計目的やスイッチのタイムスパンがサポートされます。

最近の FlexPod CVD の多くは、 Nexus 9336C-FX2 や Nexus 93180YC-FX3 などの Cisco Nexus 9000 シリーズスイッチを使用して検証されています。このスイッチは、 40 / 100G および 10 / 25G ポート、低レイテンシ、優れた電力効率をコンパクトな 1U フォームファクタで提供します。アップリンクポートとブレークアウトケーブルを使用して、さらに速度をサポートします。次の図に、この検証に使用される Nexus 9336C-FX2 および Nexus 3232C を含む、いくつかの Cisco Nexus 9K および 3k スイッチを示します。

を参照してください "Cisco データセンタースイッチ" 使用可能な Nexus スイッチとその仕様およびマニュアルの詳細については、を参照してください。

MDS スイッチ

Cisco MDS 9100/9200/9300 シリーズファブリックスイッチは、 FlexPod アーキテクチャのオプションコンポーネントです。これらのスイッチは、信頼性と柔軟性が高く、セキュアであり、ファブリック内のトラフィックフローを可視化できます。次の図は、 FlexPod 解決策 用の冗長 FC SAN ファブリックを構築してアプリケーションとビジネスの要件を満たす MDS スイッチの例を示しています。



Cisco MDS 9132T/9148T/9396T ハイパフォーマンス 32G マルチレイヤファブリックスイッチはコスト効率が高く、信頼性、柔軟性、拡張性に優れています。高度なストレージネットワーキング機能は管理が容易で、Cisco MDS 9000 ファミリポートフォリオ全体と互換性があり、信頼性の高い SAN を実装できます。

最新の SAN 分析機能と計測機能がこの次世代ハードウェアプラットフォームに組み込まれています。フレームヘッダーの検査から抽出されたテレメトリデータは、 Cisco Data Center Network Manager を含む分析視覚化プラットフォームにストリーミングできます。MDS 9148S など、 16G FC をサポートする MDS スイッチも FlexPod でサポートされます。また、 FC プロトコルに加えて FCoE プロトコルと FCIP プロトコルをサポートする MDS 9250i などのマルチサービス MDS スイッチも、 FlexPod 解決策 ポートフォリオに含まれます。

9132T や 9396T などの半モジュラー型 MDS スイッチでは、追加のデバイス接続をサポートするために、ポート拡張モジュールとポートライセンスを追加できます。9148T などの固定スイッチでは、必要に応じてポートライセンスを追加できます。このようなビジネスの成長に応じた柔軟性により、運用コストが発生します。 MDS スイッチベースの SAN インフラの導入と運用にかかるコストを削減できます。

を参照してください "Cisco MDS ファブリックスイッチ" 使用可能な MDS ファブリックスイッチの詳細については、を参照してください "NetApp IMT" および "シスコのハードウェアおよびソフトウェア互換性リスト" サポートされる SAN スイッチの一覧を確認できます。

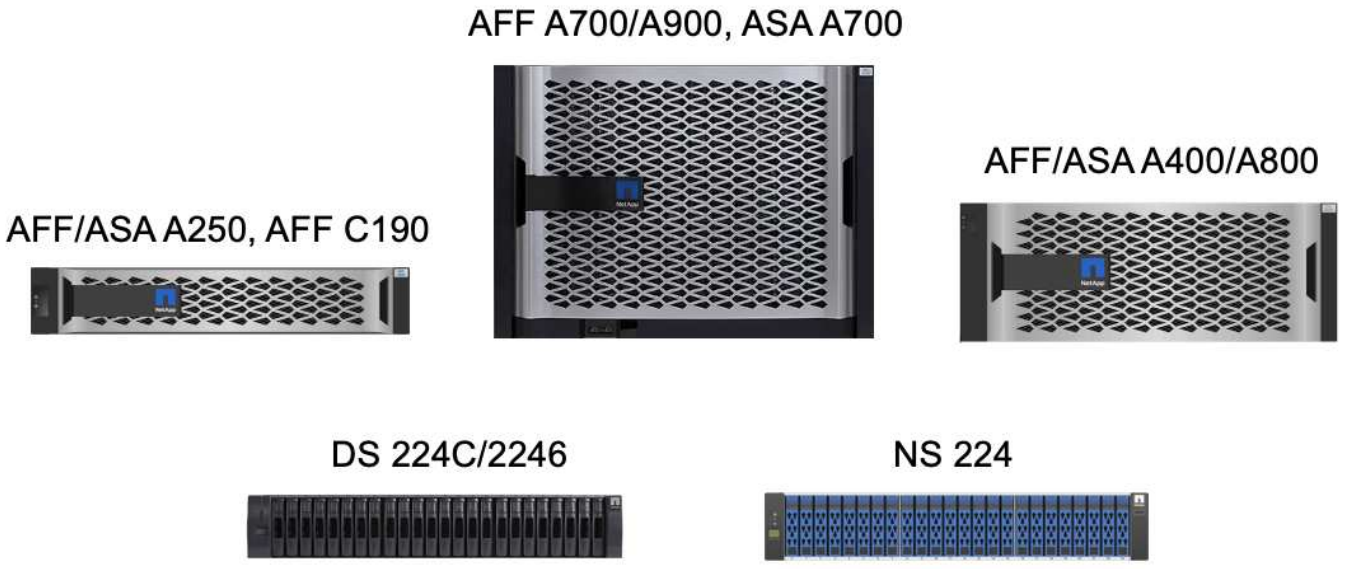
NetApp コンポーネント

FlexPod SM-BC 解決策 を作成するには、 ONTAP ソフトウェア 9.8 以降のリリースを実行している冗長な NetApp AFF コントローラまたは ASA コントローラが必要です。SM-BC を導入する場合は、最新の ONTAP リリース 9.10.1 が推奨されます。これにより、 ONTAP の継続的な革新的技術、パフォーマンス、品質の向上、および SM-BC サポートでの最大オブジェクト数の増加を活用できます。

業界をリードするパフォーマンスと革新的なテクノロジを搭載した NetApp AFF および ASA コントローラは、エンタープライズデータを保護し、機能豊富なデータ管理機能を提供します。AFF システムと ASA システムは、 NVMe に接続された SSD や NVMe over Fibre Channel （ NVMe/FC ）フロントエンドホスト接続など、エンドツーエンドの NVMe テクノロジをサポートしています。NVMe/FC ベースの SAN インフラを採用することで、ワークロードのスループットを向上させ、 I/O レイテンシを低減できます。ただし、現在 NVMe / FC ベースのデータストアは、 SM-BC で保護されていないワークロードにのみ使用できます。これは、 SM-BC 解決策 では現在 iSCSI プロトコルと FC プロトコルしかサポートされていないためです。

また、 NetApp AFF と ASA ストレージコントローラは、ネットアップデータファブリックによって実現されるシームレスなデータ移動のメリットをお客様に提供するためのハイブリッドクラウド基盤を提供します。データファブリックを使用すると、生成されたエッジから使用されるコア、クラウドまで容易にデータを取得でき、オンデマンドで柔軟なコンピューティング機能と AI 機能、 ML 機能を活用して、実用的なビジネスインサイトを獲得できます。

次の図に示すように、ネットアップでは、パフォーマンスと容量の要件を満たすためにさまざまなストレージコントローラとディスクシェルフを提供しています。NetApp AFF および ASA コントローラの機能と仕様に関する製品ページへのリンクについては、次の表を参照してください。

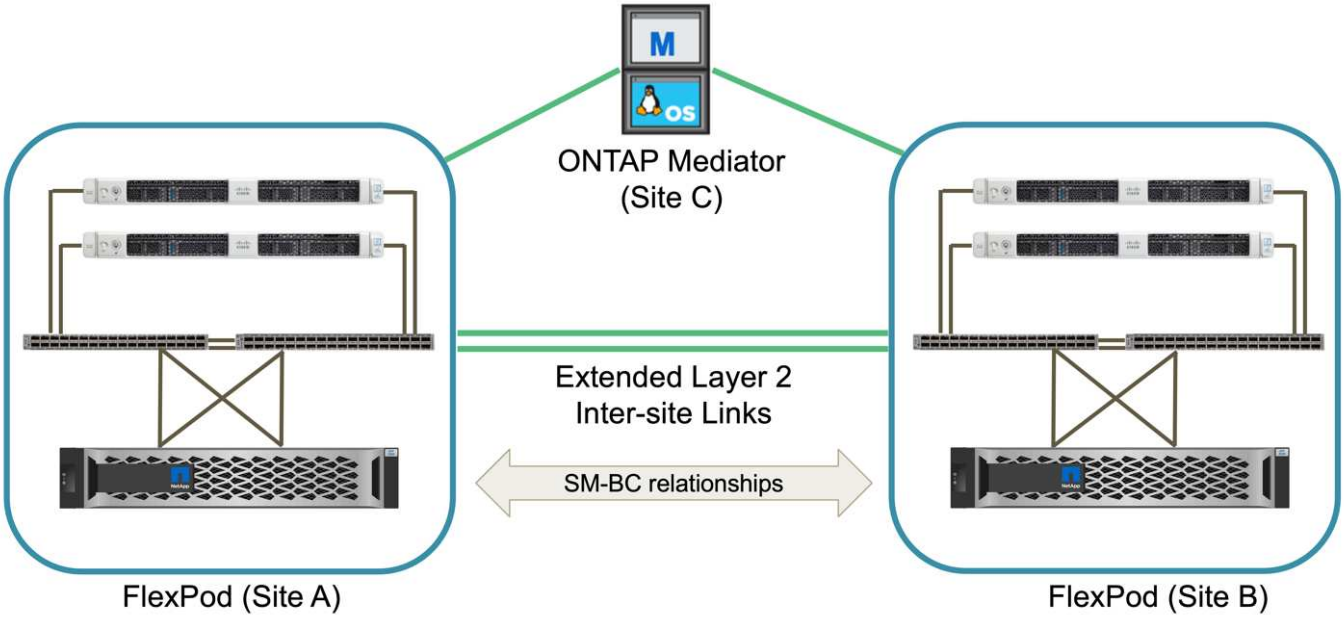


製品ファミリー	技術仕様
AFF シリーズ	"AFF シリーズのドキュメント"
ASA シリーズ	"ASA シリーズのドキュメント"

を参照してください "ネットアップのディスクシェルフとストレージメディアのドキュメント" および "NetApp Hardware Universe の略" ディスクシェルフ、および各ストレージコントローラモデルでサポートされているディスクシェルフの詳細については、を参照してください。

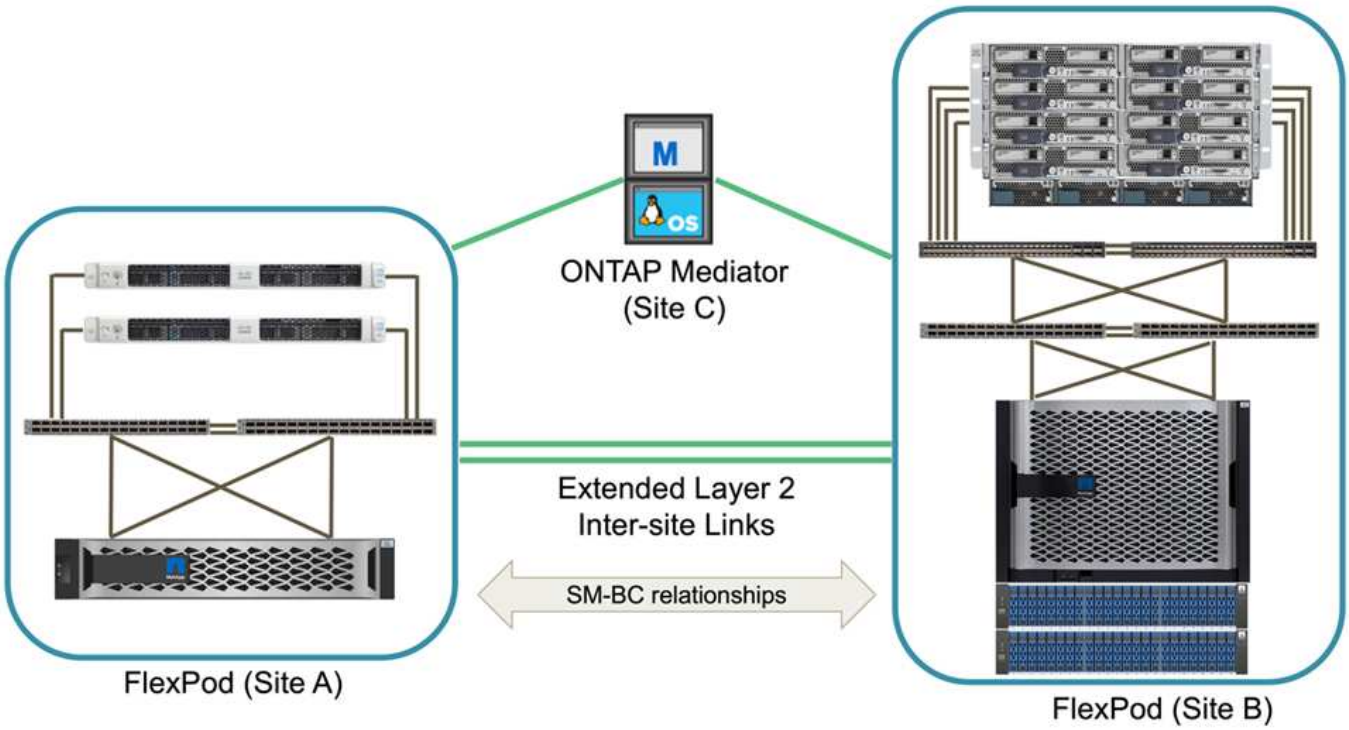
解決策 トポロジ

FlexPod ソリューションはトポロジに柔軟に対応しており、さまざまな解決策 要件に合わせてスケールアップまたはスケールアウトすることができます。次の図に示すように、ビジネス継続性保護を必要とし、最小限のコンピューティングリソースとストレージリソースしか使用できない解決策 では、単純な解決策 トポロジを使用できます。この単純なトポロジでは、 UCS C シリーズラックサーバと、ディスクシェルフを追加せずにコントローラ内の SSD を搭載した AFF / ASA コントローラを使用します。



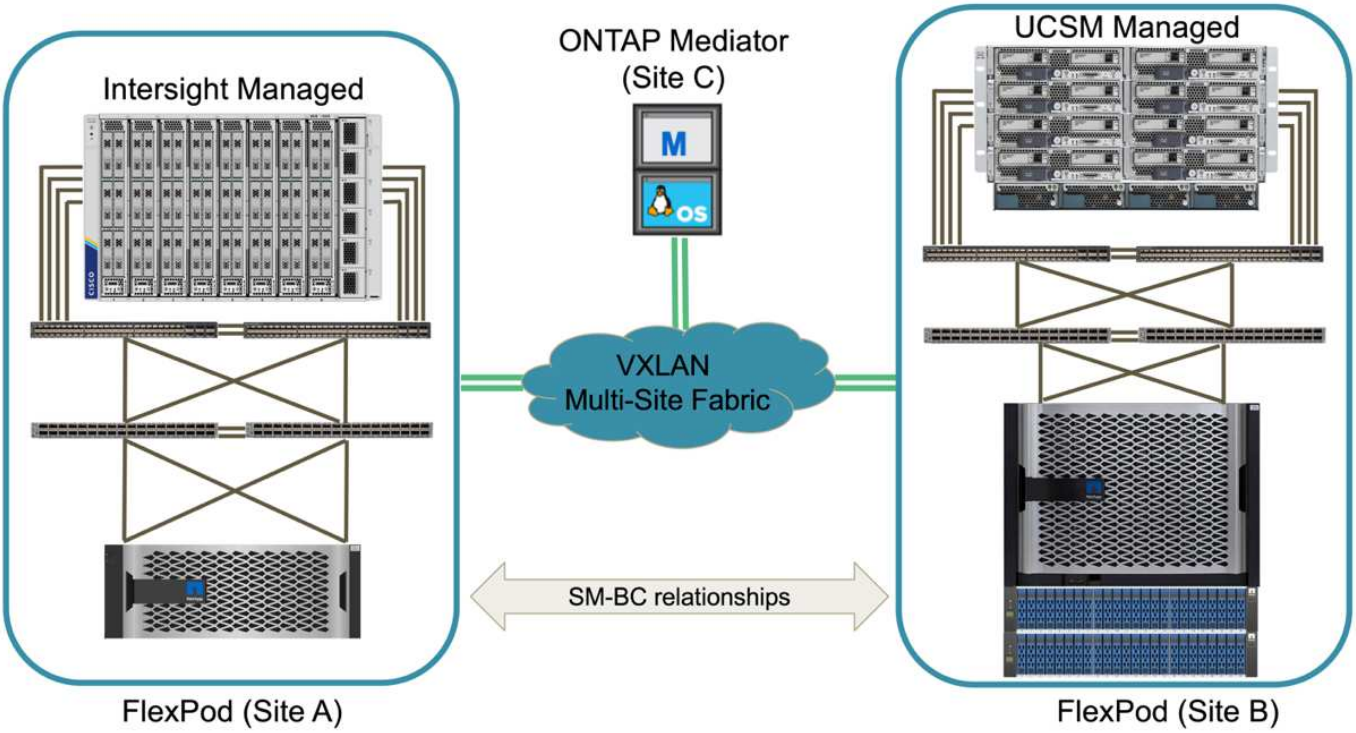
コンピューティング、ネットワーク、ストレージの冗長コンポーネントは、コンポーネント間の冗長な接続によって相互接続されます。この高可用性設計は、解決策 の耐障害性を提供し、単一点障害のシナリオに耐えることができます。マルチサイト設計と ONTAP SM-BC 同期データレプリケーション関係により、単一サイトのストレージ障害が発生しても、ビジネスクリティカルなデータサービスを提供します。

データセンターとメトロポリタンエリア内のブランチオフィスの間の企業が使用できる非対称展開トポロジは、次のようになります。この非対称設計の場合、データセンターには、より多くのコンピューティングリソースとストレージリソースを備えた、より高いパフォーマンスの FlexPod が必要です。ただし、ブランチオフィスの要件は小さく、はるかに小さな FlexPod で満たすことができます。

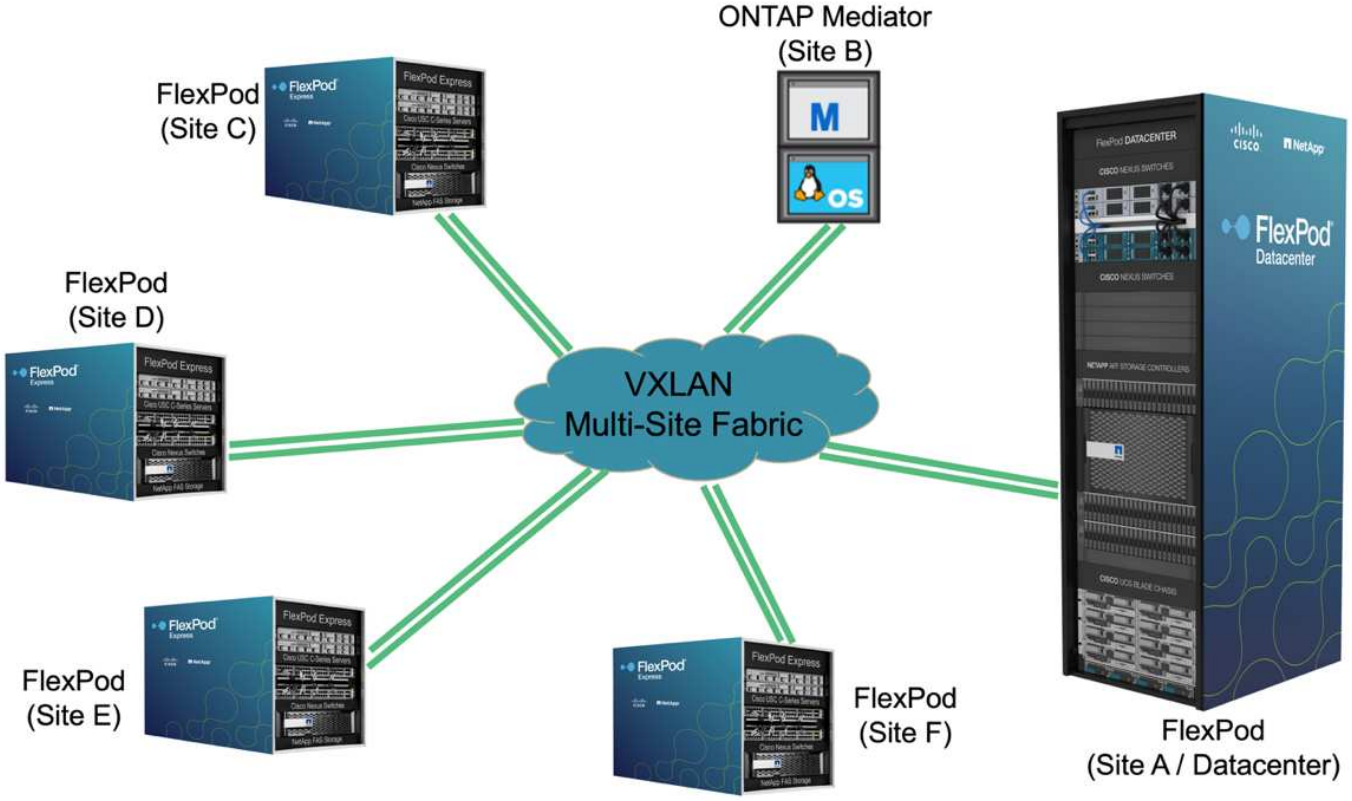


VXLAN ベースのマルチサイトファブリックを使用すると、コンピューティングリソースとストレージリソースの要件が大きくなり、複数のサイトにシームレスなネットワークファブリックを構築して、アプリケーションのモビリティを促進し、アプリケーションを任意のサイトから提供できるようになります。

新しい FlexPod インスタンスで保護する必要がある Cisco UCS 5108 シャーシおよび B シリーズブレードサーバを使用する既存の FlexPod 解決策 がある場合があります。新しい FlexPod インスタンスは、次の図に示すように、 Cisco Intersight で管理される X210c コンピューティングノードを搭載した最新の UCS X9508 シャーシを使用できます。この場合、各サイトの FlexPod システムはより大規模なデータセンターファブリックに接続され、サイトはインターコネクトネットワークを介して VXLAN マルチサイトファブリックを形成します。



データセンターと複数のブランチオフィスがある企業が、ビジネス継続性を確保するために保護する必要がある場合は、次の手順を実行します。 次の図に示す FlexPod SM-BC 導入トポロジを実装して、重要なアプリケーションおよびデータサービスを保護し、すべてのブランチサイトで RPO ゼロおよび RTO ほぼゼロを達成できます。



この導入モデルでは、各ブランチオフィスが、データセンターで必要とする SM-BC 関係と整合グループを確立します。サポートされる SM-BC オブジェクトの制限を考慮する必要があります。そのため、整合グループ

関係およびエンドポイント数全体が、データセンターでサポートされる最大数を超えないようにする必要があります。

"次：解決策 の検証の概要"

解決策の検証

解決策 の検証 - 概要

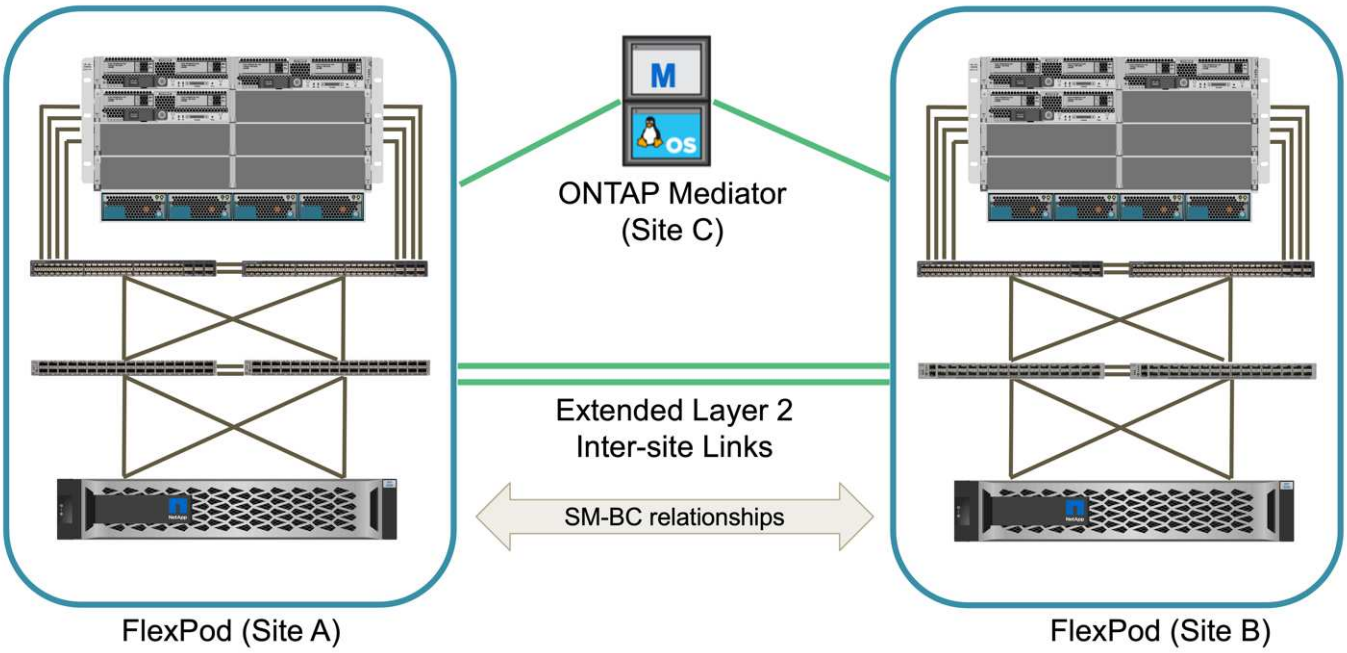
"前のページ： FlexPod SM-BC 解決策"

FlexPod SM-BC 解決策 の設計および実装の詳細は、特定の FlexPod 状況の設定および解決策 の目的によって異なります。ビジネス継続性に関する一般的な要件を定義したあと、 FlexPod SM-BC 解決策 を作成するには、 2 つの新しい FlexPod システムを使用してまったく新しい解決策 を実装し、別のサイトに新しい FlexPod を追加して既存の FlexPod とペアリングするか、 2 つの既存の FlexPod システムをペアリングします。

FlexPod ソリューションは構成に柔軟性があるため、サポートされるすべての FlexPod 構成とコンポーネントを使用できます。このセクションの残りの部分では、 VMware ベースの仮想インフラストラクチャ解決策に対して実行される実装検証について説明します。SM-BC に関連する要素を除き、実装は標準の FlexPod 配置プロセスに従います。FlexPod の実装の一般的な詳細については、ご使用の構成に適した FlexPod CVD および NVA を参照してください。

検証トポロジ

FlexPod SM-BC 解決策 の検証には、ネットアップ、 Cisco 、 VMware が提供するサポート対象のテクノロジコンポーネントを使用します。解決策 には、 ONTAP 9.10.1 を実行する NetApp AFF A250 HA ペア、サイト A にデュアル Cisco Nexus 9336C-FX2 スイッチ、サイト B にデュアル Cisco Nexus 3232C スイッチ、両方のサイトに Cisco UCS 6454 FI が搭載されています。 VMware vSphere 7.0u2 を実行し、 UCS Manager および VMware vCenter サーバによって管理される各サイトの 3 台の Cisco UCS B200 M5 サーバ次の図は、 2 つの FlexPod システムをサイト A で実行し、サイト B は拡張レイヤ 2 サイト間リンクで接続し、 ONTAP メディエーターはサイト C で実行しているコンポーネントレベルの解決策 検証トポロジを示しています



ハードウェアとソフトウェア：

次の表に、解決策 の検証に使用したハードウェアとソフトウェアを示します。Cisco 、ネットアップ、VMware は、 FlexPod の具体的な実装のサポートを判断するために相互運用性マトリックスを使用します。

- "http://support.netapp.com/matrix/"
- "Cisco UCS ハードウェアおよびソフトウェア相互運用性ツール"
- "http://www.vmware.com/resources/compatibility/search.php"

カテゴリ	コンポーネント	ソフトウェアのバージョン	数量
コンピューティング	Cisco UCS ファブリックインターコネクト 6454	4.2 （1f）	4 （1 サイトにつき 2 つ）
	Cisco UCS B200 M5 サーバ	4.2 （1f）	6 （1 サイトにつき 3 つ）
	Cisco UCS IOM 2204XP	4.2 （1f）	4 （1 サイトにつき 2 つ）
	Cisco VIC 1440 （PID ： UCSB-mLOM40G-04）	5.2 （1a）	2 （1 サイトにつき 1 つ）
	Cisco VIC 1340 （PID ： UCSB-mLOM-40G-03）	4.5 （1a）	4 （1 サイトにつき 2 つ）
ネットワーク	Cisco Nexus 9336C-FX2	9.3 （6）	2 （サイト A）
	Cisco Nexus 3232C	9.3 （6）	2 （サイト B）
ストレージ	NetApp AFF A250	9.10.1	4 （1 サイトにつき 2 つ）
	NetApp System Manager の略	9.10.1	2 （1 サイトにつき 1 つ）

カテゴリ	コンポーネント	ソフトウェアのバージョン	数量
	NetApp Active IQ Unified Manager の略	9.10	1.
	NetApp ONTAP Tools for VMware vSphere の略	9.10	1.
	NetApp SnapCenter Plugin for VMware vSphere 用です	4.6	1.
	NetApp ONTAP メディエーター	1.3	1.
	ナボックス	3.0.2	1.
	ネットアップハーベスト	21.11.1-1.	1.
仮想化	VMware ESXi	7.0U2	6 （1 サイトにつき 3 つ）
	VMware ESXi nenic イーサネットドライバ	1.0.35.0	6 （1 サイトにつき 3 つ）
	VMware vCenter	7.0U2	1.
	NetApp NFS Plug-in for VMware VAAI	"2.0"	6 （1 サイトにつき 3 つ）
テスト中です	Microsoft Windows の場合	2022	1.
	Microsoft SQL Server の場合	2019 年	1.
	Microsoft SQL Server Management Studio の略	18.10	1.
	HammerDB	4.3	1.
	Microsoft Windows の場合	10.	6 （1 サイトにつき 3 つ）
	Iometer	1.1.0	6 （1 サイトにつき 3 つ）

"次のステップ：解決策 の検証 - コンピューティング。"

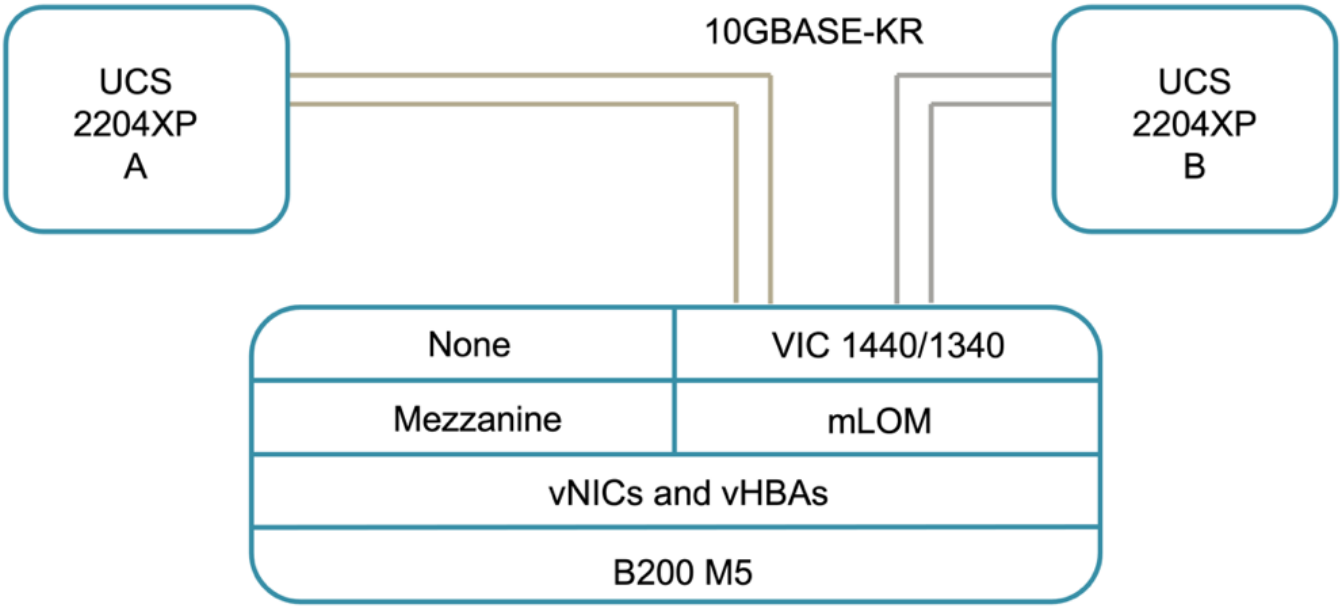
解決策 の検証 - コンピューティング

"事前定義：解決策 の検証 - 概要。"

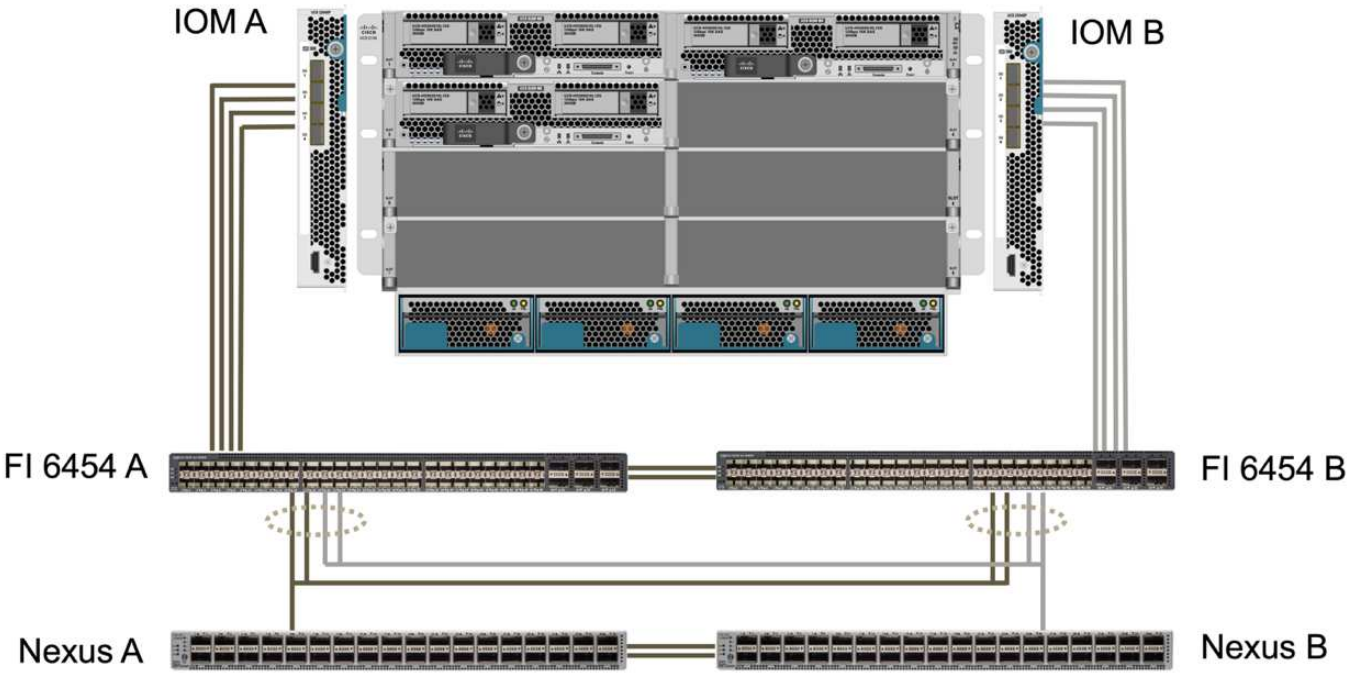
FlexPod SM-BC 解決策 のコンピューティング設定は、一般的な FlexPod 解決策 のベストプラクティスに従います。以降のセクションでは、検証に使用する接続と構成の一部を紹介します。また、 SM-BC に関連する考慮事項の一部は、実装のリファレンスとガイダンスを提供するために強調表示されています。

接続性

UCS B200 ブレードサーバと IOM 間の接続は、 UCS 5108 シャーシバックプレーン接続を介して UCS VIC カードによって提供されます。検証に使用する UCS 2204XP ファブリックエクステンダには、それぞれ 16 個の 10G ポートがあり、それぞれ 8 台のハーフ幅ブレードサーバに接続します（たとえば、サーバごとに 2 個）。サーバの接続帯域幅を増やすために、メザニンベースの VIC を追加して、サーバを代替 UCS 2408 IOM に接続し、各サーバに 4 つの 10G 接続を提供できます。



検証に使用される UCS 5108 シャーシと UCS 6454 FI 間の接続は、 4 つの 10G 接続を使用する IOM 2204XP によって提供されます。FI ポート 1 ～ 4 は、これらの接続用のサーバーポートとして設定されます。FI ポート 25 ～ 28 は、ローカルサイトの Nexus スイッチ A および B へのネットワークアップリンクポートとして設定されます。次の図と表に、 UCS 5108 シャーシおよび Nexus スイッチに接続する UCS 6454 FI の接続図とポート接続の詳細を示します。



ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
UCS 6454 FI A	1.	IOM A	1.
	2.		2.
	3.		3.
	4.		4.
	25	Nexus A	1/13/1
	26		1/13/2
	27	Nexus B	1/3
	28		1/4
	L1	UCS 6454 FI B	L1
	L2 （ L2 ）		L2 （ L2 ）
UCS 6454 FI B	1.	IOM B	1.
	2.		2.
	3.		3.
	4.		4.
	25	Nexus A	1/3
	26		1/4
	27	Nexus B	1/13/1
	28		1/13/2
	L1	UCS 6454 FI A	L1
	L2 （ L2 ）		L2 （ L2 ）

Nexus 9336C-FX2switches を使用したサイト A と Nexus 3232C スイッチを使用したサイト B にもかかわらず、上記の接続はサイト A とサイト B の両方で同様です。40G ~ 4x10G ブレークアウトケーブルは、 Nexus から FI への接続に使用されます。Nexus への FI 接続はポートチャネルを使用し、 Nexus スイッチで仮想ポートチャネルが設定されて各 FI への接続が集約されます。

IOM 、 FI 、 Nexus スイッチの各コンポーネントを別々に組み合わせて使用する場合は、環境の組み合わせに適したケーブルとポート速度を使用してください。

より高速な接続またはより多くの接続をサポートするコンポーネントを使用することで、帯域幅を増やすことができます。冗長性をさらに高めるには、それをサポートするコンポーネントとの接続を追加します。

サービスプロファイル

UCS Manager （ UCSM ）または Cisco Intersight によって管理されるファブリックインターコネクトを備えたブレードサーバシャーシは、 UCSM で使用可能なサービスプロファイルと Intersight のサーバプロファイルを使用して、サーバを抽象化できます。この検証では、 UCSM とサービスプロファイルを使用してサーバ

管理を簡素化します。サービスプロファイルを使用すると、元のサービスプロファイルを新しいハードウェアに関連付けるだけで、サーバを交換またはアップグレードできます。

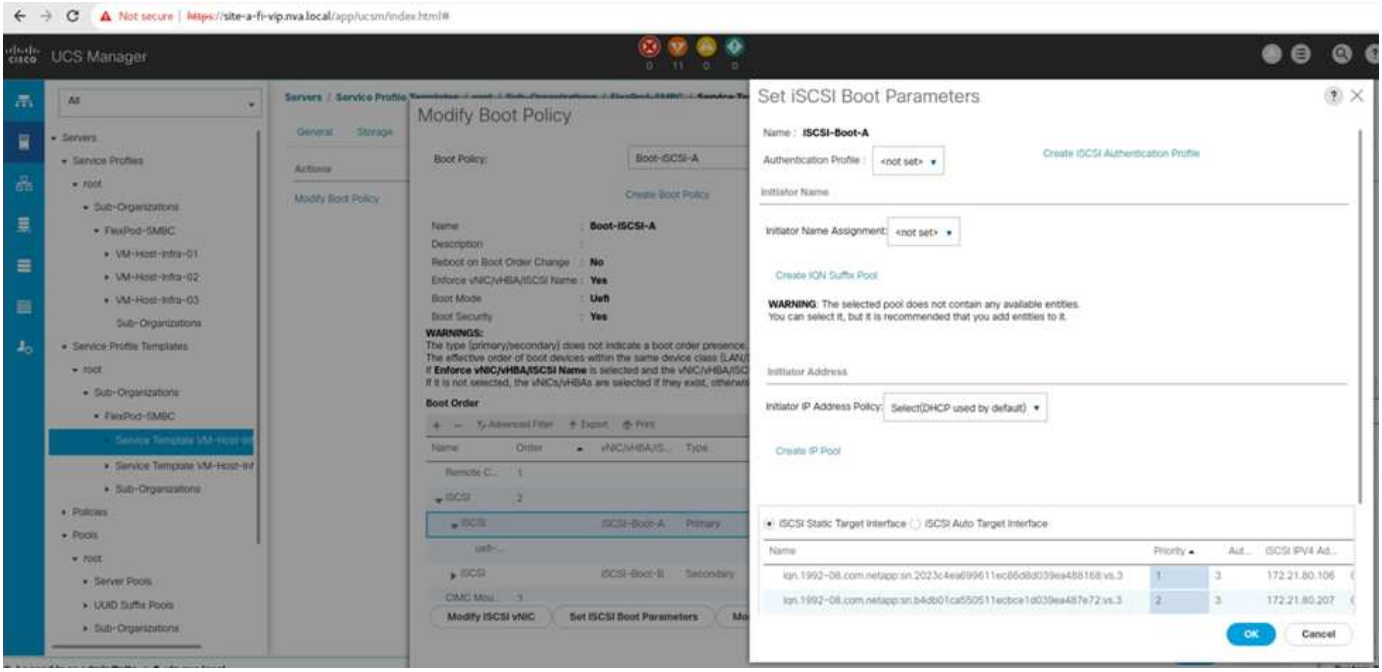
作成されるサービスプロファイルでは、 VMware ESXi ホストに対して次の情報がサポートされます。

- iSCSI プロトコルを使用して、いずれかのサイトの AFF A250 ストレージから SAN をブートします。
- サーバには次の 6 つの vNIC が作成されます。
  - 2 つの冗長 vNIC （ vSwitch0-A と vSwitch0-B ）がインバンド管理トラフィックを伝送します。オプションで、これらの vNIC は、 SM-BC で保護されていない NFS プロトコルデータでも使用できます。
  - VMware vMotion およびその他のアプリケーショントラフィックを伝送するために、 vSphere Distributed Switch によって 2 つの冗長 vNIC （ vDS-A および vDS-B ）が使用されます。
  - iSCSI-A vSwitch が使用する vNIC で、 iSCSI-A パスへのアクセスを提供します。
  - iSCSI-B vSwitch が iSCSI-B パスへのアクセスを提供するために使用する iSCSI-B vNIC 。

SAN ブート

iSCSI SAN ブート構成では、 iSCSI ブートパラメータは、両方の iSCSI ファブリックからの iSCSI ブートを許可するように設定されています。プライマリクラスタが使用できない場合に、 iSCSI SAN ブート LUN がセカンダリクラスタから提供される SM-BC フェイルオーバーシナリオに対応するには、 iSCSI 静的ターゲット構成にサイト A とサイト B の両方のターゲットを含める必要がありますさらに、ブート LUN の可用性を最大限に高めるために、すべてのストレージコントローラからブートするように iSCSI ブートパラメータを設定します。

iSCSI スタティックターゲットは、次の図に示すように、 Set iSCSI Boot Parameter （ iSCSI ブートパラメータの設定）ダイアログの下にあるサービスプロファイルテンプレートのブートポリシーで設定できます。推奨される iSCSI ブートパラメータ設定を次の表に示します。この表には、高可用性を実現するために前述したブート戦略が実装されています。



iSCSI ファブリック	優先度	iSCSI ターゲット	iSCSI LIF
iSCSI A	1.	サイト A の iSCSI ターゲット	サイト A のコントローラ 1 の iSCSI A LIF
	2.	iSCSI ターゲット：サイト B	サイト B コントローラ 2 の iSCSI A LIF
iSCSI B	1.	iSCSI ターゲット：サイト B	サイト B コントローラ 1 の iSCSI B LIF
	2.	サイト A の iSCSI ターゲット	サイト A コントローラ 2 の iSCSI B LIF

"次の例は、解決策 の検証 - ネットワークです。"

解決策 の検証 - ネットワーク

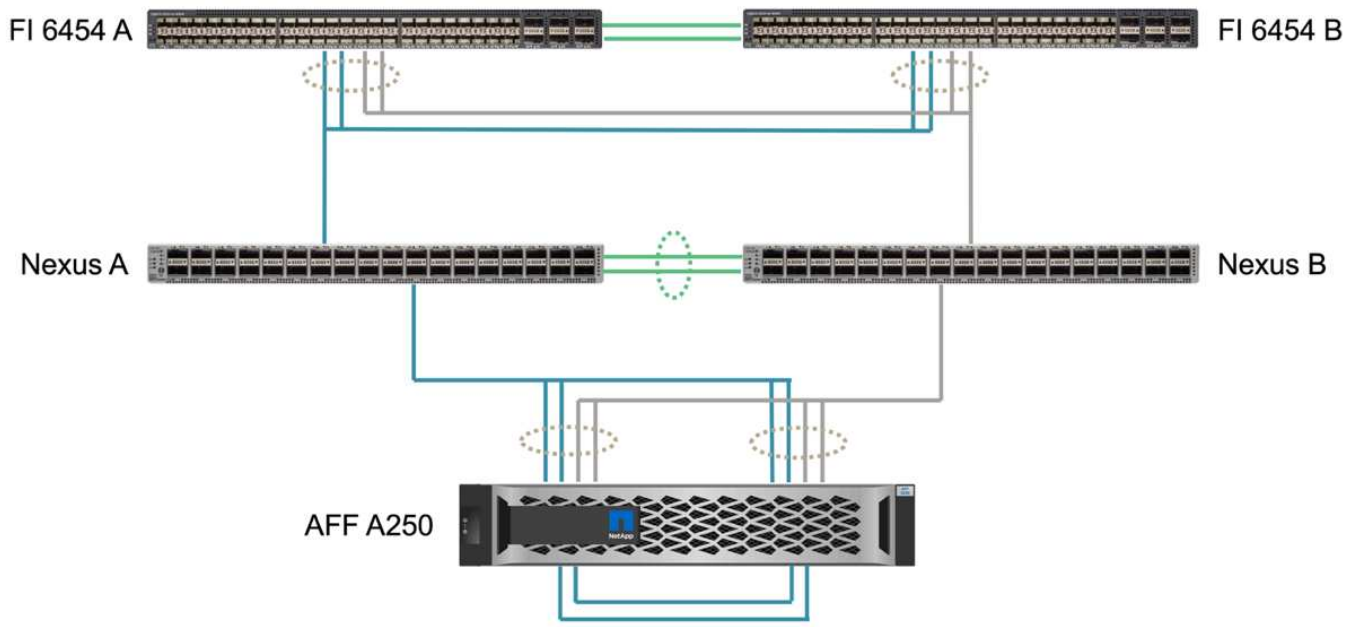
"前のバージョン：解決策 の検証 - コンピューティング。"

FlexPod SM-BC 解決策 のネットワーク設定は、各サイトでの一般的な FlexPod 解決策 のベストプラクティスに従います。サイト間接続の場合、解決策 検証設定では、 2 つのサイトの FlexPod Nexus スイッチを相互に接続して、 2 つのサイト間に VLAN を拡張するサイト間接続を提供します。以降のセクションでは、検証に使用する接続と構成の一部を紹介します。

接続性

各サイトの FlexPod Nexus スイッチは、可用性の高い構成で UCS コンピューティングと ONTAP ストレージの間をローカルで接続します。冗長コンポーネントと冗長接続により、単一点障害に対する耐障害性が確保されます。

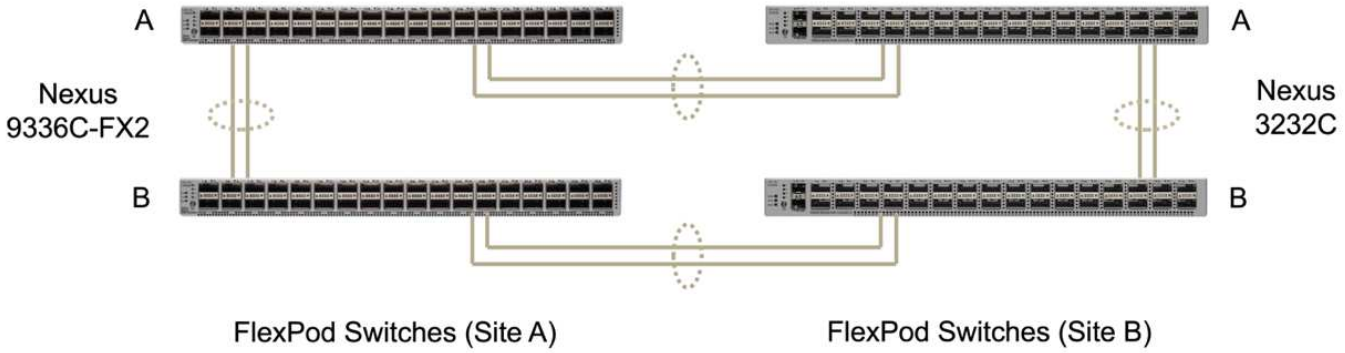
次の図は、各サイトでの Nexus スイッチのローカル接続を示しています。図に示されている内容に加えて、図に示されていない各コンポーネントのコンソールネットワーク接続と管理ネットワーク接続もあります。40G ~ 4 x 10G ブレークアウトケーブルは、 Nexus スイッチを UCS FI および ONTAP AFF A250 ストレージコントローラに接続するために使用します。また、 100G から 4 x 25G ブレークアウトケーブルを使用して、 Nexus スイッチと AFF A250 ストレージコントローラ間の通信速度を向上させることもできます。わかりやすいように、 2 台の AFF A250 コントローラは、ケーブル接続の図のために論理的に並べて表示されています。2 台のストレージコントローラを 2 つの接続で接続することで、ストレージがスイッチレスクラスタを形成できます。



次の表に、各サイトの Nexus スイッチと AFF A250 ストレージコントローラの接続を示します。

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
Nexus A	1/10/1.	AFF A250 A	E1A
	1/10/2.		e1b
	1/10/3.	AFF A250 B	E1A
	1/10/4.		e1b
Nexus B	1/10/1.	AFF A250 A	E1C
	1/10/2.		e1d
	1/10/3.	AFF A250 B	E1C
	1/10/4.		e1d

次の図に、サイト A とサイト B の FlexPod スイッチ間の接続を示します。ケーブル接続の詳細については、次の表を参照してください。各サイトの 2 つのスイッチ間の接続は、 vPC ピアリンク用です。一方、サイト間のスイッチ間の接続はサイト間リンクを提供します。リンクを使用することで、クラスタ間通信、 SM-BC データレプリケーション、インバンド管理、およびリモートサイトのリソースへのデータアクセス用に、サイト間で VLAN を拡張できます。



ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
サイト A のスイッチ A	33	サイト B のスイッチ A	31.
	34		32
	25	サイト A のスイッチ B	25
	26		26
サイト A のスイッチ B	33	サイト B のスイッチ B	31.
	34		32
	25	サイト A のスイッチ A	25
	26		26
サイト B のスイッチ A	31.	サイト A のスイッチ A	33
	32		34
	25	サイト B のスイッチ B	25
	26		26
サイト B のスイッチ B	31.	サイト A のスイッチ B	33
	32		34
	25	サイト B のスイッチ A	25
	26		26

上記の表は、各 FlexPod スイッチの観点からの接続を示しています。このため、表内で読みやすくするために情報が重複しています。

ポートチャネルと仮想ポートチャネル

ポートチャネルを使用すると、 Link Aggregation Control Protocol （ LACP ）を使用して帯域幅の集約とリンク障害の耐障害性を実現し、リンクアグリゲーションを実現できます。仮想ポートチャネル（ vPC ）を使用すると、 2 つの Nexus スイッチ間のポートチャネル接続を 1 つのポートとして論理的に認識できます。これにより、単一リンク障害や単一スイッチ障害などの障害に対する耐障害性がさらに向上します。

UCS サーバからストレージへのトラフィックは、 Nexus スイッチに到達する前に、 IOM A から FI A へ、 IOM B から FI B へのパスを経由します。Nexus スイッチへの FI 接続は、 FI 側のポートチャネルと Nexus スイッチ側の仮想ポートチャネルを利用するため、 UCS サーバは両方の Nexus スイッチを介したパスを効果的

に使用でき、単一点障害が発生しても運用できます。2 つのサイト間では、前の図に示すように、 Nexus スイッチは相互接続されています。サイト間でスイッチペアを接続するリンクと、ポートチャネル構成を使用するリンクがそれぞれ 2 つあります。

インバンド管理、クラスタ間、および iSCSI/NFS データストレージプロトコル接続は、各サイトのストレージコントローラを冗長構成のローカル Nexus スイッチに相互接続することによって提供されます。各ストレージコントローラは 2 つの Nexus スイッチに接続されます。耐障害性を高めるために、 4 つの接続がストレージのインターフェイスグループの一部として設定されます。Nexus スイッチ側では、これらのポートはスイッチ間の vPC の一部でもあります。

次の表に、各サイトのポートチャネル ID と使用状況を示します。

ポートチャネル **ID**	使用方法
10.	ローカル Nexus ピアリンク
15	ファブリックインターコネクト A リンク
16	ファブリックインターコネクト B リンク
27	ストレージコントローラ A のリンク
28	ストレージコントローラ B のリンク
100	サイト間スイッチ A のリンク
200	サイト間スイッチ B リンク

VLAN

次の表に、 FlexPod SM-BC 解決策 検証環境をセットアップするために設定された VLAN とその使用方法を示します。

名前	**VLAN ID**	使用方法
ネイティブ VLAN	2.	VLAN 2 がデフォルト VLAN ではなくネイティブ VLAN として使用される（1）
OOB-MGMT-VLAN	3333	デバイスのアウトオブバンド管理 VLAN
IB-MGMT-vlan	3334	ESXi ホスト、 VM 管理などのインバンド管理 VLAN
NFS-VLAN	3335	NFS トラフィック用のオプションの NFS VLAN
iSCSI-A VLAN	3336	iSCSI- iSCSI トラフィック用のファブリック VLAN
iSCSI-B VLAN	3337	iSCSI トラフィック用の iSCSI-B ファブリック VLAN
vMotion - VLAN	3338	VMware vMotion トラフィック VLAN
vm-traffic-vlan	3339	VMware VM トラフィック VLAN

名前	VLAN ID	使用方法
インタークラスタ VLAN	3340	ONTAP クラスタピア通信用のクラスタ間 VLAN

SM-BC は、 NFS プロトコルまたは CIFS プロトコルをサポートしていないため、ビジネス継続性を確保する必要がないワークロードにも使用できます。この検証で使用する NFS データストアは作成されませんでした。

"次の例：解決策 の検証：ストレージ。"

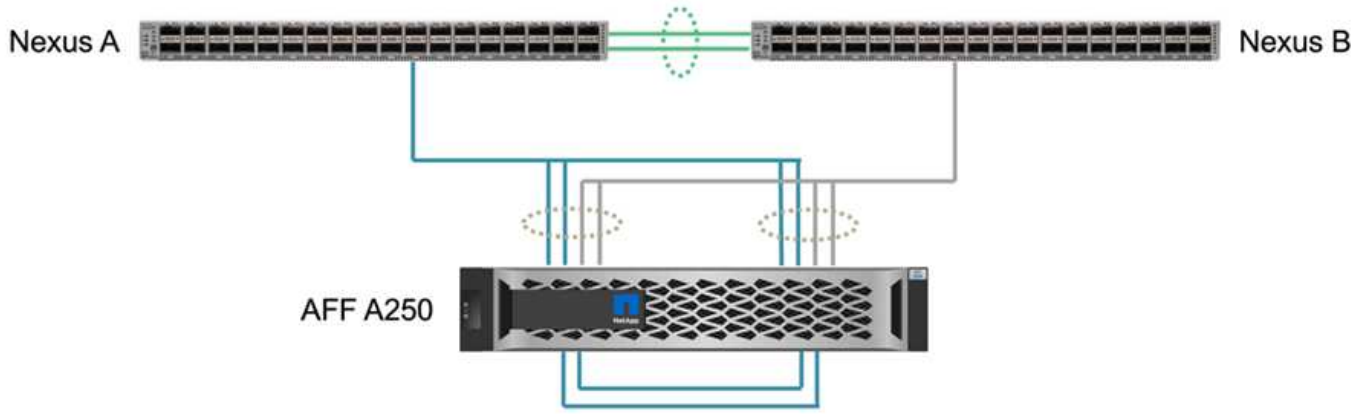
解決策 の検証 - ストレージ

"前のバージョン：解決策 の検証 - ネットワーク。"

FlexPod SM-BC 解決策 のストレージ構成は、各サイトでの一般的な FlexPod 解決策 のベストプラクティスに従います。SM-BC クラスタピアリングおよびデータレプリケーションでは、両方のサイトの FlexPod スイッチ間に確立されたサイト間リンクを使用します。以降のセクションでは、検証に使用する接続と構成の一部を紹介します。

接続性

ローカル UCS FI およびブレードサーバへのストレージ接続は、ローカルサイトの Nexus スイッチによって提供されます。サイト間の Nexus スイッチ接続を介して、リモートの UCS ブレードサーバからストレージにアクセスすることもできます。次の図と表は、各サイトのストレージ接続図とストレージコントローラの接続リストを示しています。



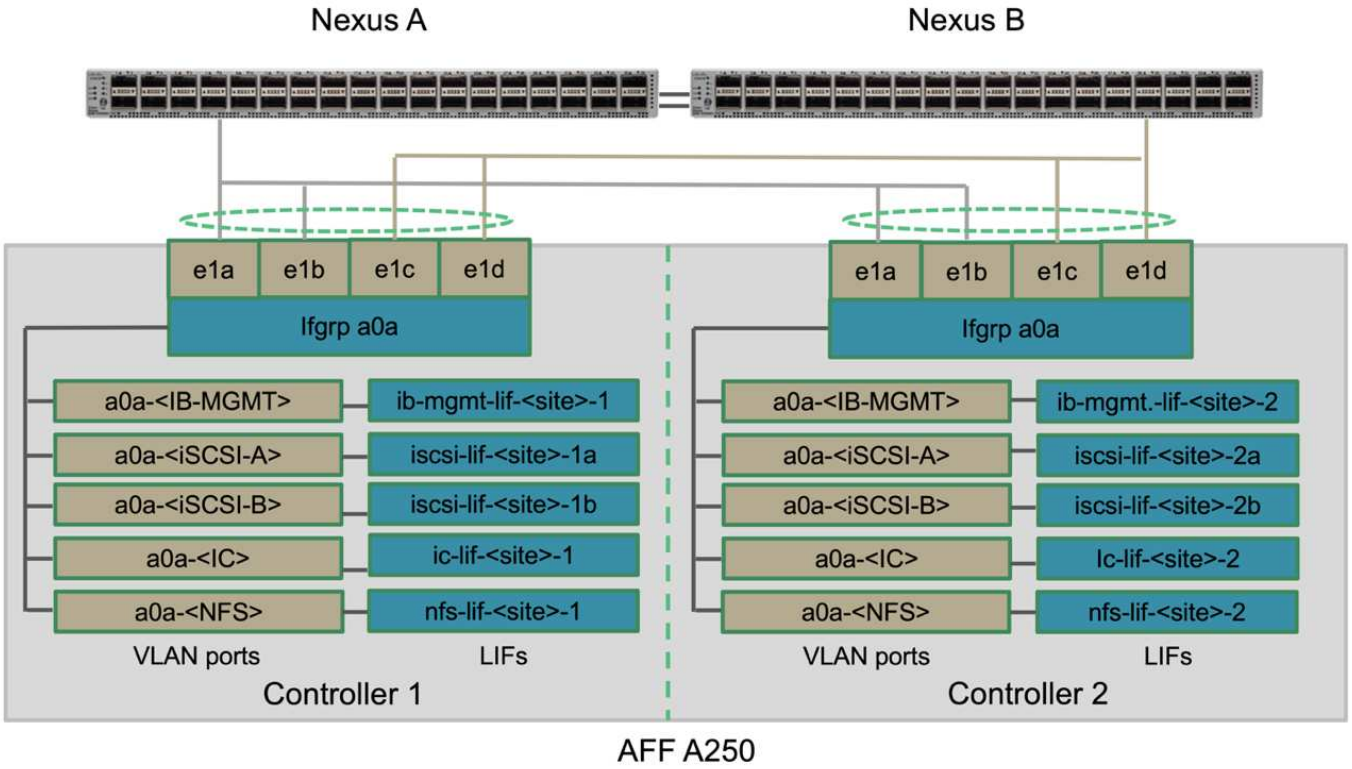
ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	E1A	Nexus A	1/10/1.
	e1b		1/10/2.
	E1C	Nexus B	1/10/1.

ローカルデバイス	ローカルポート	リモートデバイス	リモートポート
	e1d		1/10/2.
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	E1A	Nexus A	1/10/3.
	e1b		1/10/4.
	E1C	Nexus B	1/10/3.
	e1d		1/10/4.

接続およびインターフェイス

この検証では、帯域幅の集約と冗長性のために、各ストレージコントローラの 2 つの物理ポートが各 Nexus スイッチに接続されます。これら 4 つの接続は、ストレージ上のインターフェイスグループ構成に参加します。Nexus スイッチの対応するポートは、リンクアグリゲーションと耐障害性のために vPC に参加します。

インバンド管理、クラスタ間、および NFS / iSCSI データストレージプロトコルでは、 VLAN を使用します。インターフェイスグループに VLAN ポートが作成され、さまざまなタイプのトラフィックを分離します。それぞれの機能に対応する LIF が、対応する VLAN ポートの上に作成されます。次の図は、物理接続、インターフェイスグループ、 VLAN ポート、および論理インターフェイスの関係を示しています。

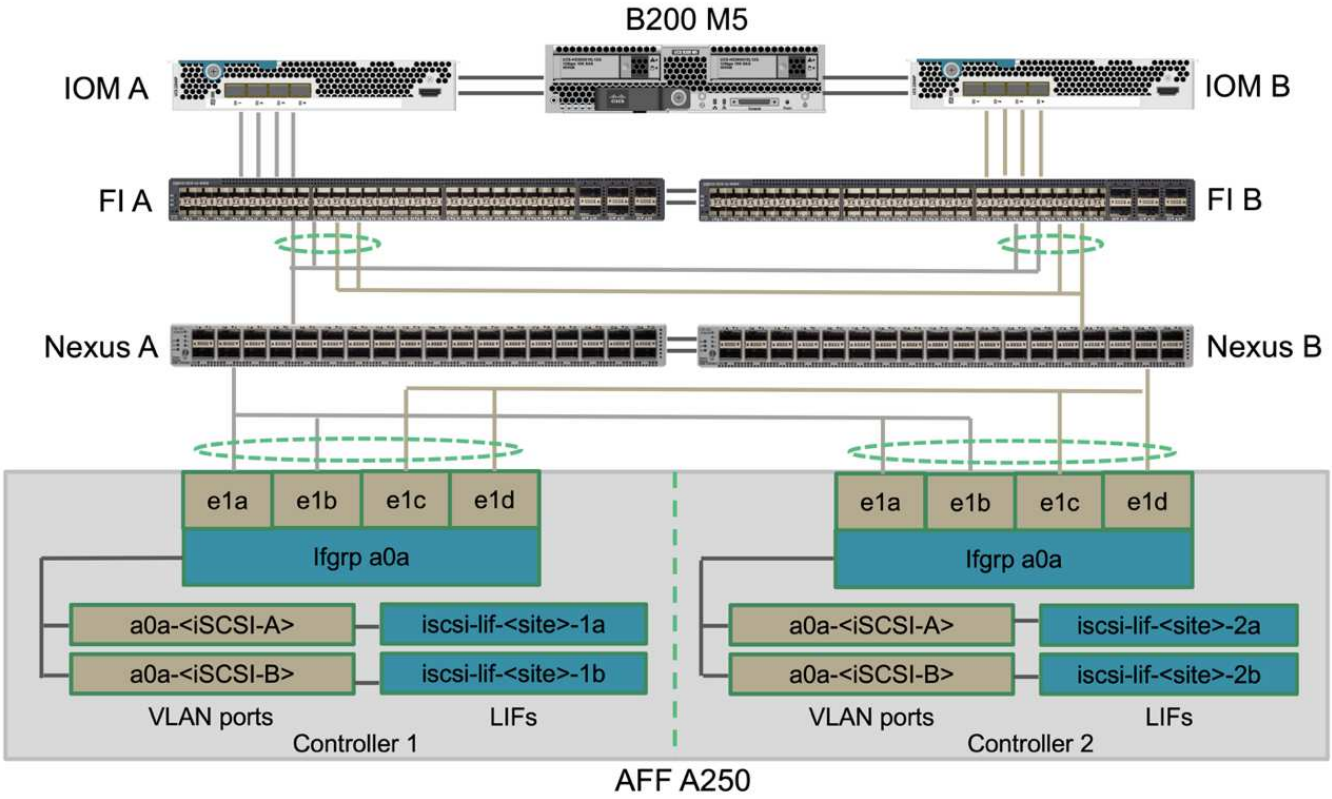


SAN ブート

FlexPod 解決策 で Cisco UCS サーバの SAN ブートを実装することを推奨します。SAN ブートを実装すると、ネットアップストレージシステム内でオペレーティングシステムを安全に保護できるため、パフォーマンスと柔軟性が向上します。この解決策 では、 iSCSI SAN ブートが検証されました。

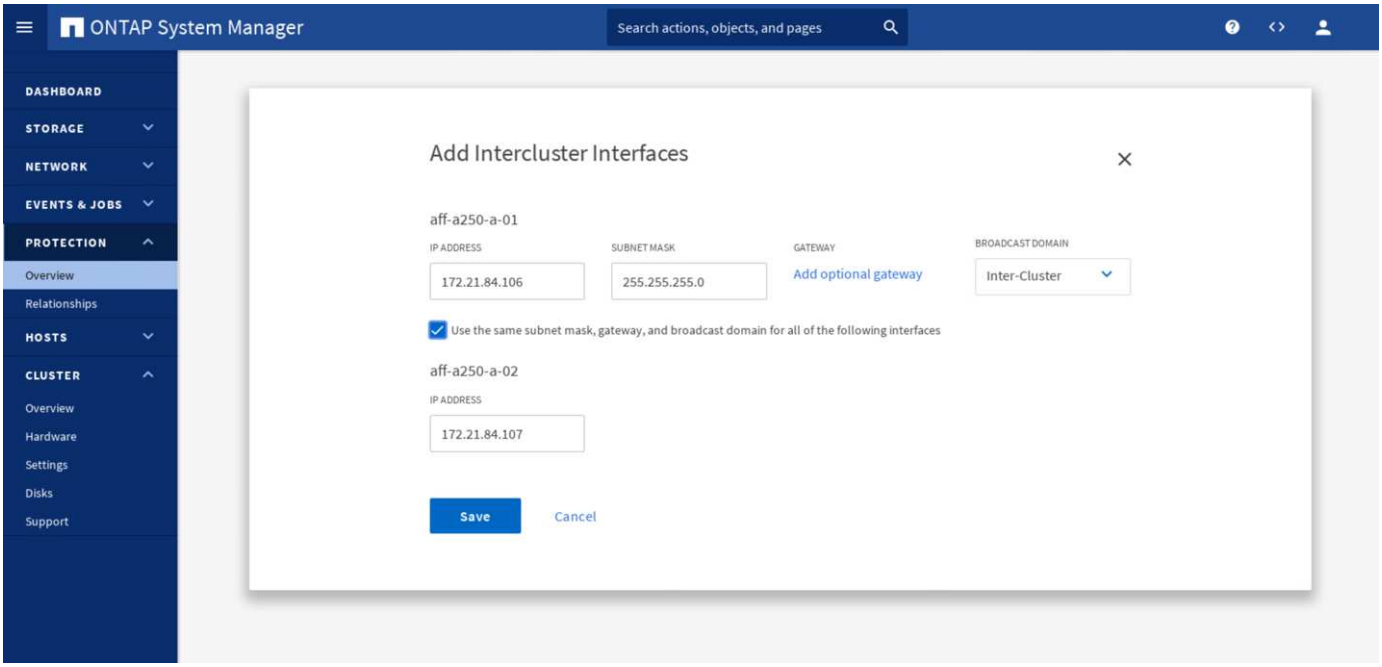
次の図は、ネットアップストレージから Cisco UCS サーバの iSCSI SAN ブートの接続を示しています。iSCSI SAN ブートでは、各 Cisco UCS サーバに 2 つの iSCSI vNIC （各 SAN ファブリックに 1 つずつ）が割り当てられ、サーバからストレージへの冗長接続が提供されます。Nexus スイッチに接続された 10 / 25 G イーサネットストレージポート（この例では e1a 、 e1b 、 e1c 、 e1d ）をグループ化して、 1 つのインターフェイスグループ（ ifgrp ）になります（この例では a0a ）。iSCSI VLAN ポートは ifgrp に作成され、iSCSI LIF は iSCSI VLAN ポートに作成されます。

各 iSCSI ブート LUN は、ブート LUN と、そのブート igroup 内のサーバの iSCSI Qualified Names （ IQNs ）を関連付けて、 iSCSI LIF を介して起動するサーバにマッピングされます。サーバのブート igroup には、各 vNIC-SAN ファブリックに対して 1 つずつ、 2 つの IQN が含まれています。この機能を使用すると、許可されたサーバだけが、そのサーバ専用に作成されたブート LUN にアクセスできます。



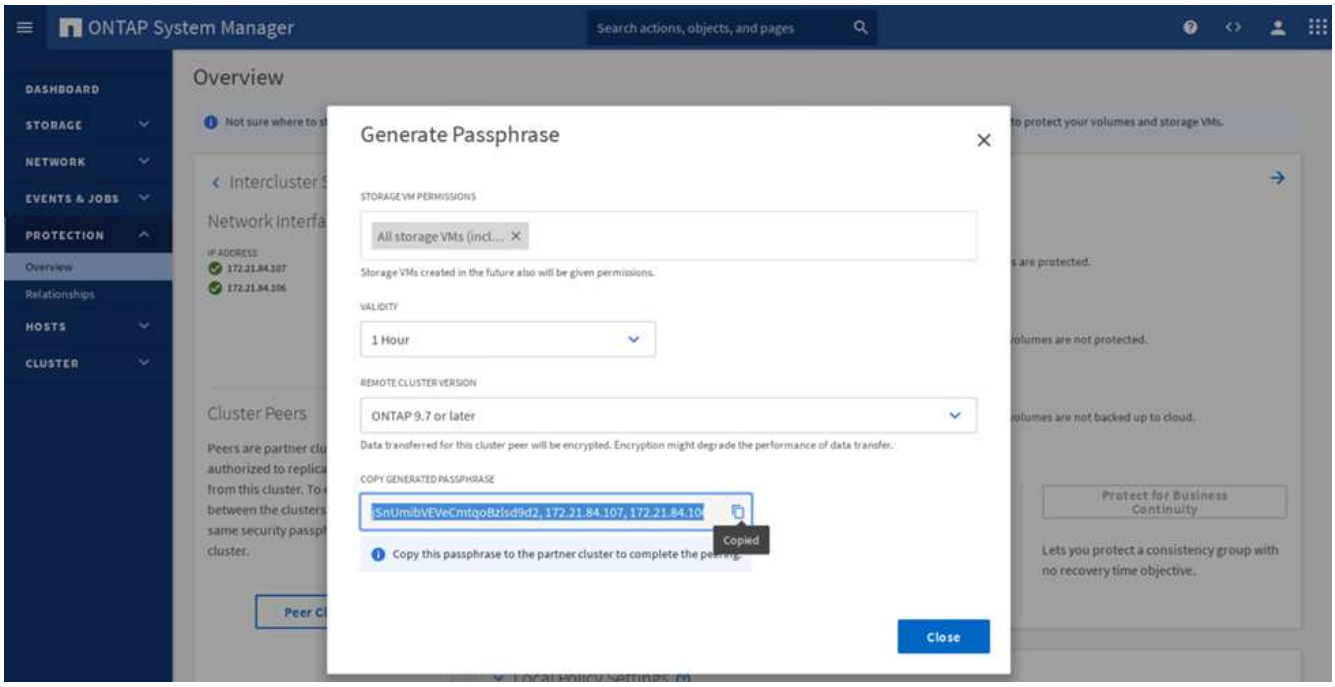
クラスタピアリング

ONTAP クラスタピアは、クラスタ間 LIF を介して通信します。2 つのクラスタで ONTAP System Manager を使用すると、 Protection > Overview ペインに、必要なクラスタ間 LIF を作成できます。

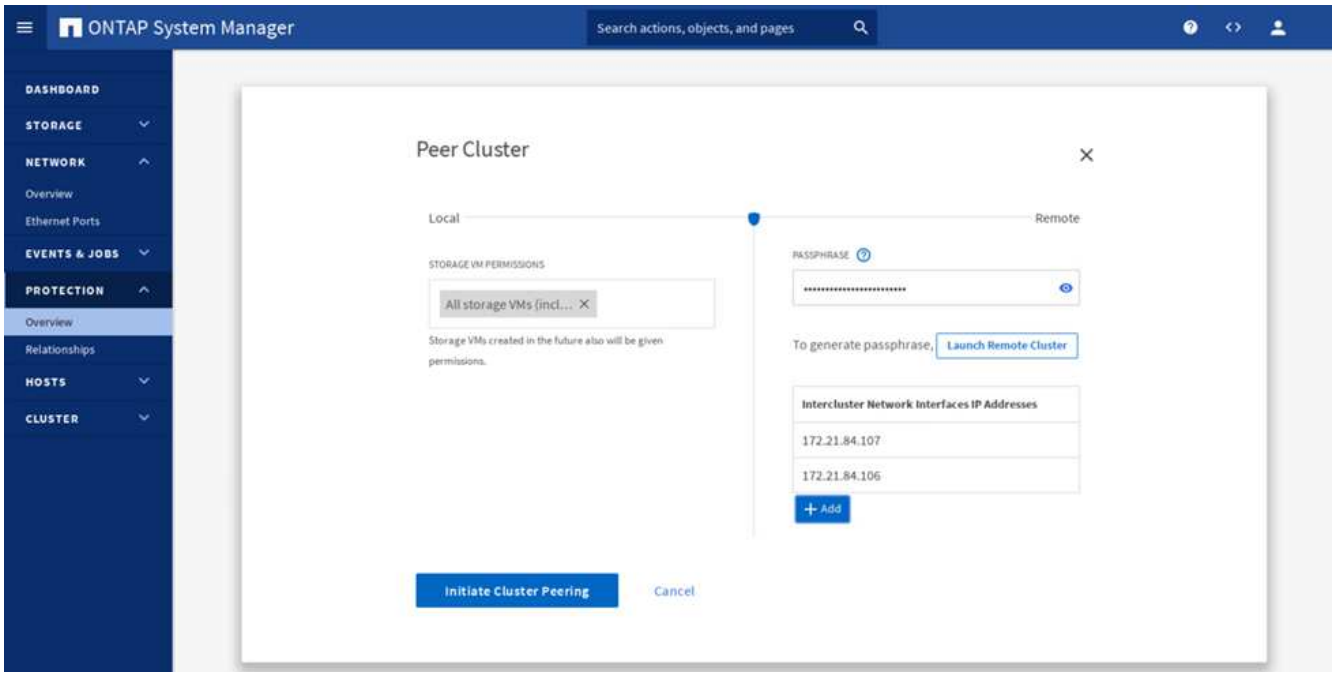


2 つのクラスタ間にピア関係を設定するには、次の手順を実行します。

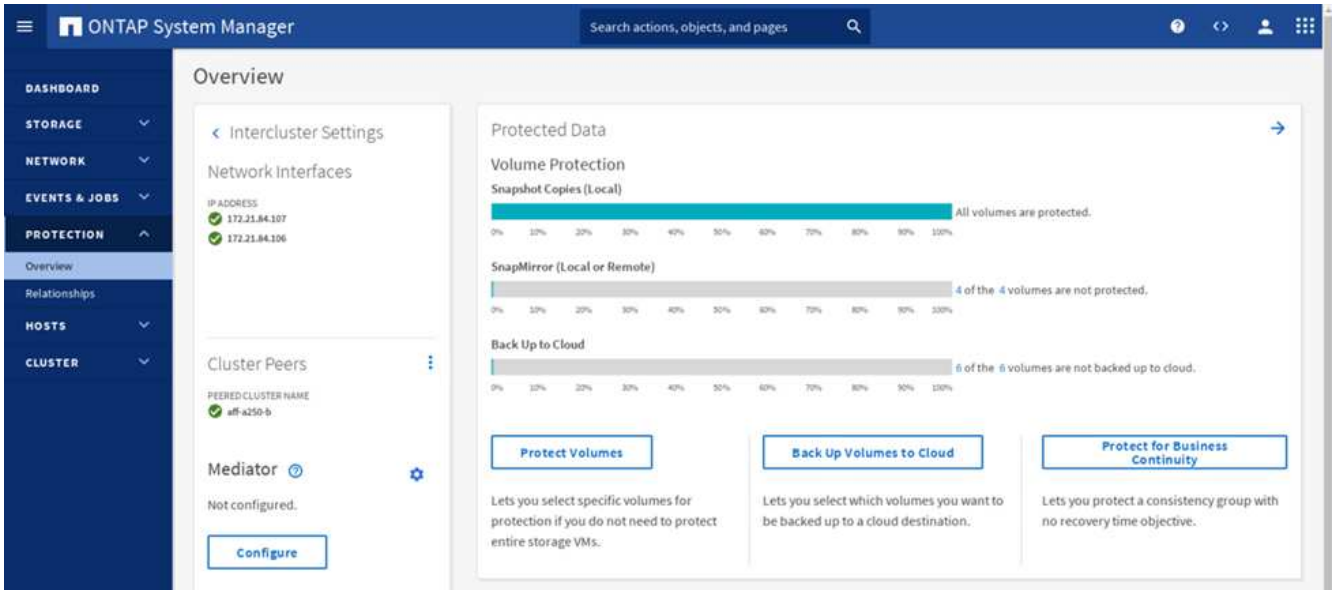
1. 1 つ目のクラスタでクラスタピアパスフレーズを生成



2. 2 番目のクラスタで Peer Cluster オプションを呼び出し、パスフレーズとクラスタ間 LIF の情報を指定します。



3. System Manager Protection > Overview ペインには、クラスタピアの情報が表示されます。



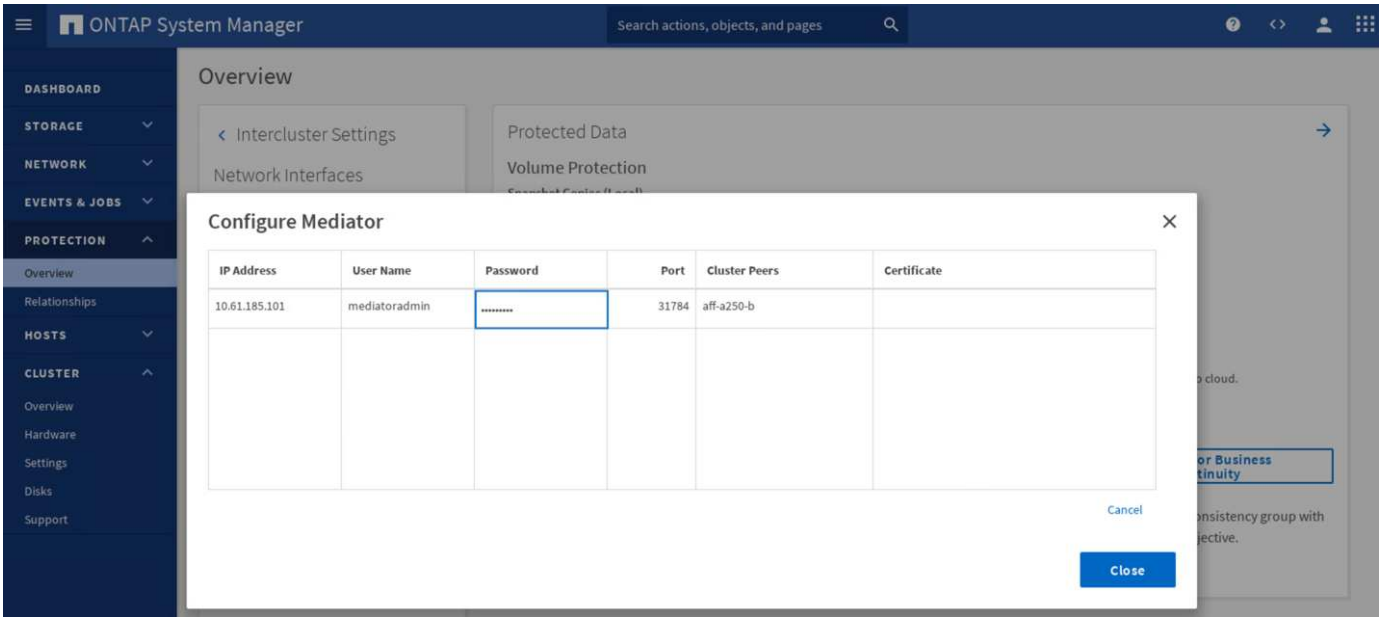
ONTAP メディエーターのインストールと設定

ONTAP メディエーターは、 SM-BC 関係にある ONTAP クラスタのクォーラムを確立します。この機能は、障害が検出されたときの自動フェイルオーバーを調整し、各クラスタが同時にプライマリクラスタとして制御を確立しようとしたときにスプリットブレインのシナリオを回避するのに役立ちます。

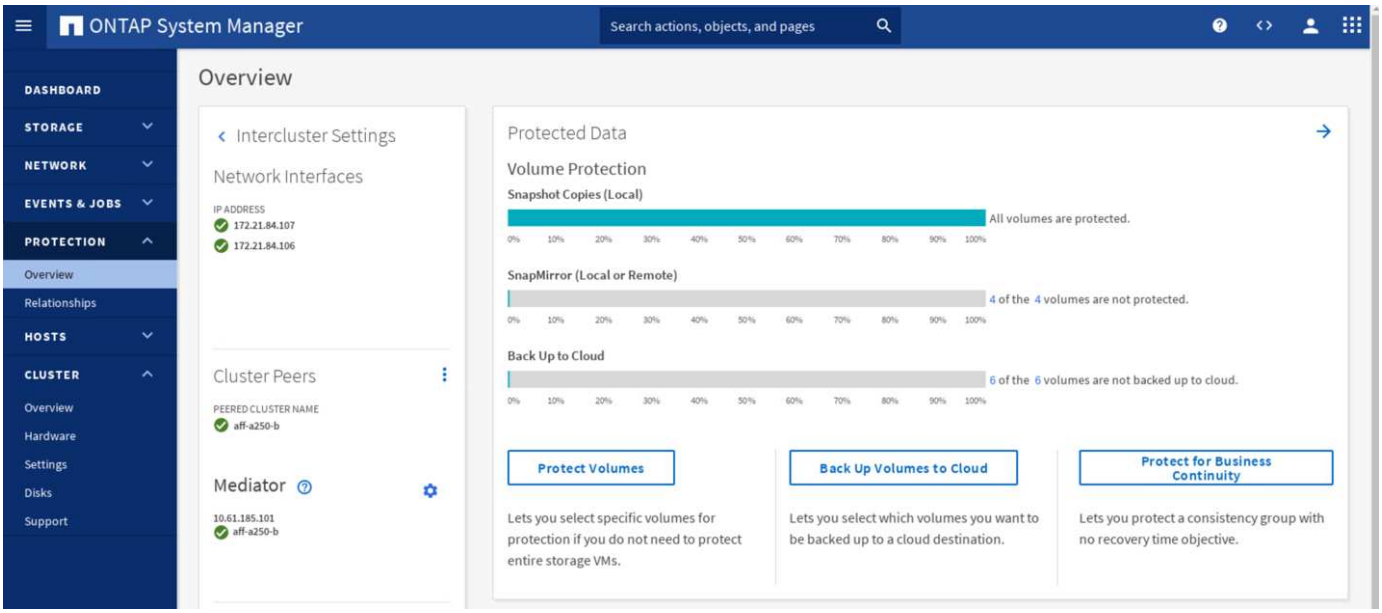
ONTAP メディエーターをインストールする前に、を確認します "ONTAP メディエーターサービスをインストールまたはアップグレードします" の各ページでは、前提条件、サポートされている Linux のバージョン、およびそれらをサポートされている各種 Linux オペレーティングシステムにインストールする手順について説明します。

ONTAP メディエーターをインストールしたら、 ONTAP メディエーターのセキュリティ証明書を ONTAP クラスタに追加し、 System Manager の Protection > Overview ペインで ONTAP メディエーターを設定できま

す。次のスクリーンショットは、 ONTAP メディエーターの設定 GUI を示しています。



必要な情報を入力すると、設定された ONTAP メディエーターが System Manager の Protection > Overview ペインに表示されます。



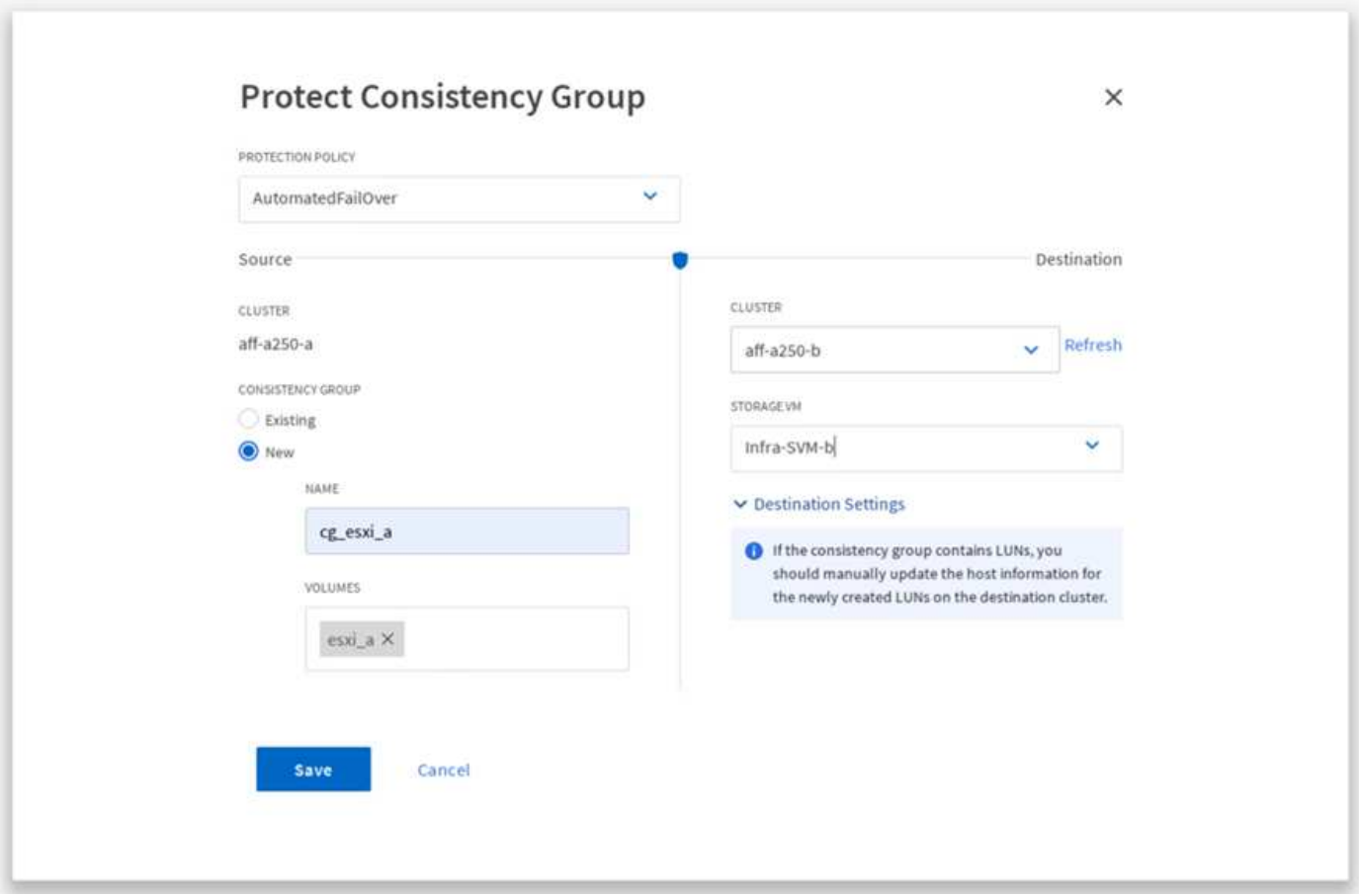
SM-BC 整合グループ

整合グループは、指定されたボリュームの集まりにまたがるアプリケーションワークロードに対して書き込み順序の整合性を保証します。ONTAP 9.10.1 では、いくつかの重要な制限事項があります。

- クラスタ内の SM-BC 整合グループ関係の最大数は 20 です。
- 各 SM-BC 関係でサポートされる最大ボリューム数は 16 です。
- クラスタ内のソースエンドポイントとデスティネーションエンドポイントの最大合計数は 200 です。

詳細については、の ONTAP SM-BC のマニュアルを参照してください "制限事項と制限事項"。

検証構成では、 ONTAP System Manager を使用して整合グループを作成し、両方のサイトの ESXi ブート LUN と共有データストア LUN の両方を保護しました。コンシステンシ・グループの作成ダイアログにアクセスするには '[保護] > [概要] > [ビジネス継続性の保護] > [コンシステンシ・グループの保護] を選択します整合グループを作成するには、作成に必要なソースボリューム、デスティネーションクラスタ、およびデスティネーション SVM の情報を指定します。

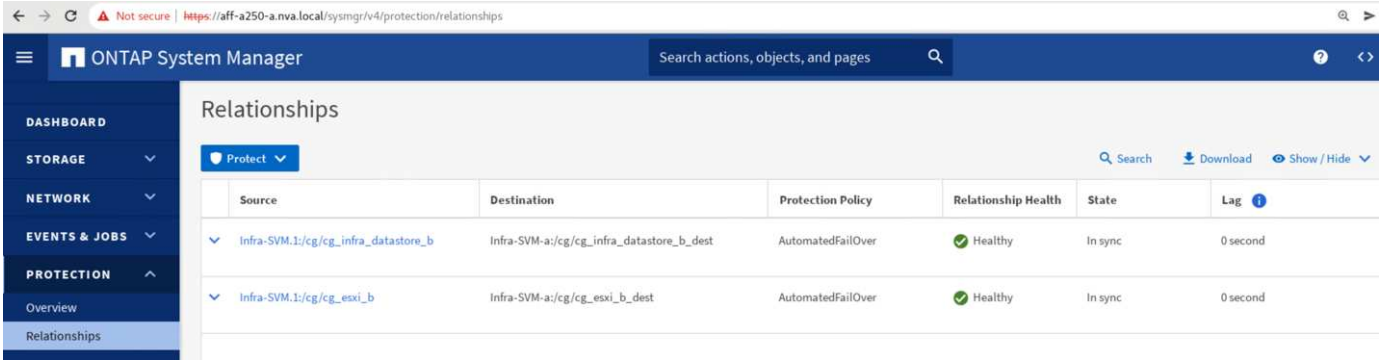


次の表に、検証テストで作成される 4 つの整合グループと各整合グループに含まれるボリュームを示します。

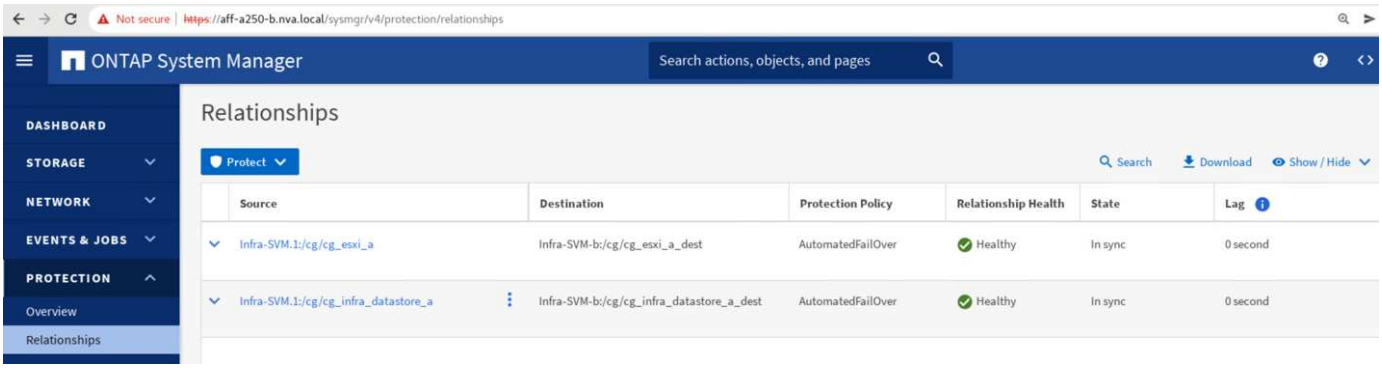
System Manager の略	整合グループ	個のボリューム
サイト A	CG_ESXi_a のようになります	esxi_a です
サイト A	cG_infra_a_a	infra_datastore_a_01 infra_a_02
サイト B	cG_esxi_b	esxi_b
サイト B	cG_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

作成された整合グループは、サイト A とサイト B のそれぞれの保護関係の下に表示されます

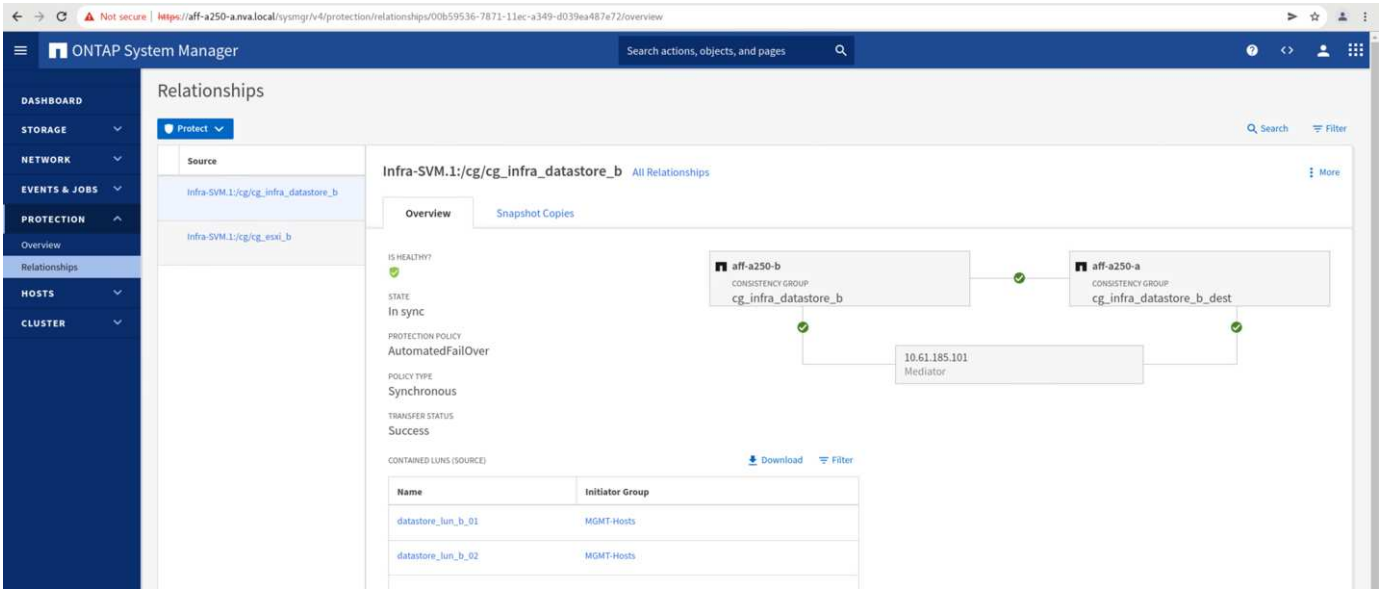
このスクリーンショットは、サイト A の整合グループ関係を示しています



このスクリーンショットは、サイト B における整合グループ関係を示しています



次のスクリーンショットは、 cg_infra_datastore_b グループの整合グループ関係の詳細を示しています。



ボリューム、 **LUN** 、およびホストのマッピング

整合グループの作成後、 SnapMirror はソースボリュームとデスティネーションボリュームを同期するため、データは常に同期された状態になります。リモートサイトのデスティネーションボリュームは、 _dest 終了中のボリューム名を伝送します。たとえば、サイト A のクラスタ内の esxi_a ボリュームには、サイト B に対応する esxi_a_dest データ保護（ DP ）ボリュームがあります

このスクリーンショットは、サイト A のボリューム情報を示しています

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

このスクリーンショットは、サイト B のボリューム情報を示しています

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

透過的なアプリケーションフェイルオーバーを可能にするには、ミラーリングされた SM-BC LUN もデスティネーションクラスタからホストにマッピングする必要があります。これにより、ホストは、ソースとデスティネーションの両方のクラスタから LUN へのパスを適切に認識できます。サイト A とサイト B の両方の「 igroup show 」出力と「 lun show 」出力は、次の 2 つのスクリーンショットでキャプチャされています。作成されたマッピングでは、クラスタ内の各 ESXi ホストが自身の SAN ブート LUN を ID 0 、 4 つすべての共有 iSCSI データストア LUN として認識します。

このスクリーンショットは、サイト A のクラスタのホスト igroup と LUN マッピングを示しています。

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01           VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02           VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03           VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                   MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01      VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02      VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03      VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b              MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

このスクリーンショットは、サイト B のクラスタのホスト igroup と LUN マッピングを示しています。

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"次に、解決策 の検証と仮想化を行います。"

解決策 の検証：仮想化

"前のバージョン：解決策 の検証 - ストレージ。"

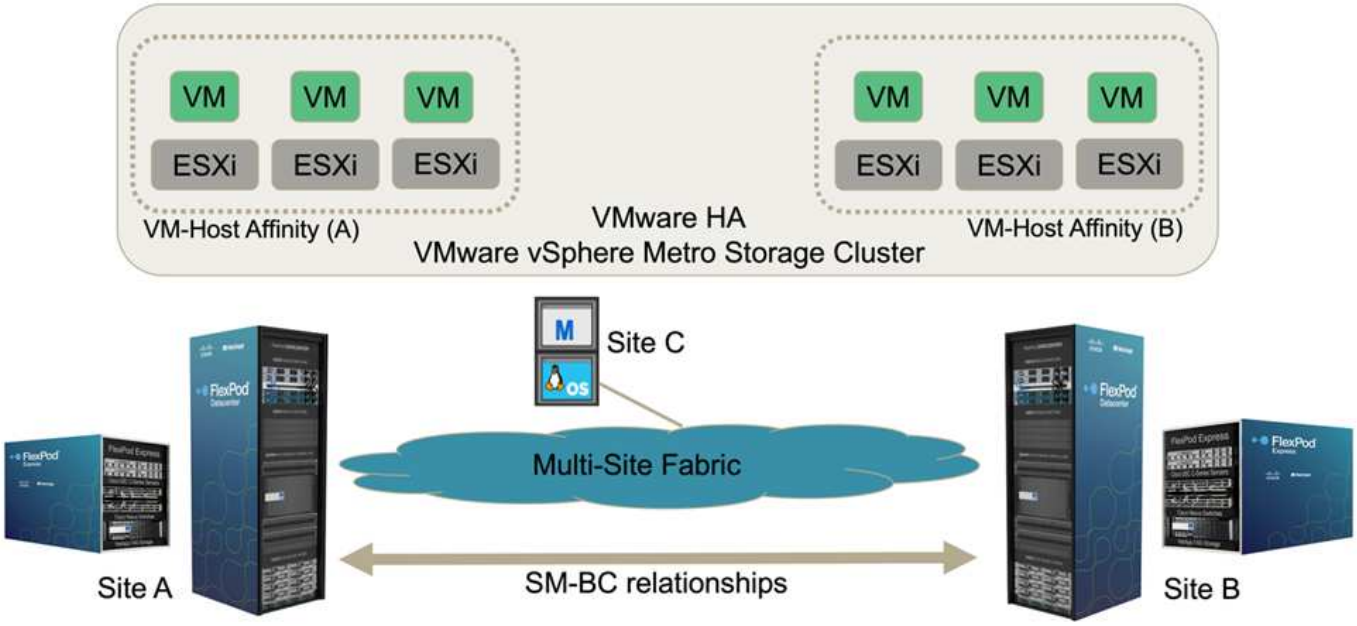
マルチサイトの FlexPod SM-BC 解決策 では、 1 つの VMware vCenter が解決策 全体の仮想インフラストラクチャリソースを管理します。両方のデータセンターのホストは、両方のデータセンターにまたがる単一の VMware HA クラスタに参加します。ホストは、 NetApp SM-BC 解決策 にアクセスできます。このでは、定義済みの SM-BC 関係にあるストレージに両方のサイトからアクセスできます。

SM-BC 解決策 ストレージは、災害やダウンタイムを避けるために、 VMware vSphere Metro Storage Cluster （ vMSC ）機能の統一されたアクセスモデルに準拠しています。仮想マシンのパフォーマンスを最適化するには、通常運用時の WAN リンク経由のレイテンシとトラフィックを最小限に抑えるために、仮想マシンディスクをローカルの NetApp AFF A250 システム上にホストする必要があります。

設計実装の一環として、 2 つのサイト間での仮想マシンの分散を決定する必要があります。この仮想マシンサイトのアフィニティとアプリケーションの 2 つのサイト間での分散は、サイトの設定とアプリケーションの要件に応じて決定できます。VMware クラスタの VM/ ホストグループおよび VM/ ホストルールを使用して、 VM/ ホストアフィニティを設定し、 VM が目的のサイトのホストで実行されていることを確認します。

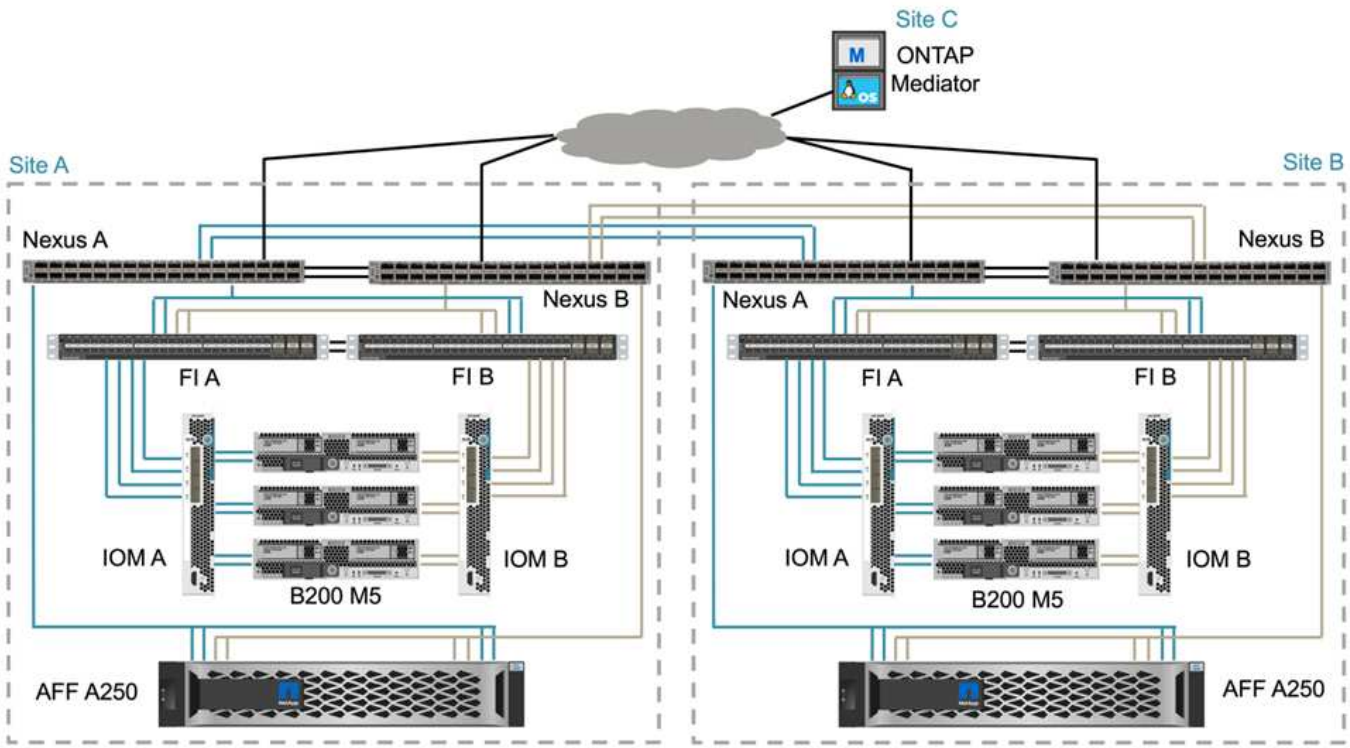
ただし、両方のサイトで VM を実行できる構成では、リモートサイトのホストで VMware HA によって VM を再起動し、解決策 の耐障害性を確保できます。両方のサイトで仮想マシンを実行する場合は、サイト間で仮想マシンの vMotion を円滑に実行するために、すべての ESXi ホストに iSCSI 共有データストアをマウントする必要があります。

次の図は、 FlexPod SM-BC 解決策 の仮想化ビューの概要を示しています。このビューには、 VMware HA と vMSC の両方の機能が含まれており、コンピューティングサービスとストレージサービスの高可用性を実現します。アクティブ / アクティブのデータセンター解決策 アーキテクチャにより、サイト間でのワークロードの移動が可能になり、 DR / BC 保護が提供されます。



エンドツーエンドのネットワーク接続

FlexPod SM-BC 解決策 には、各サイトに FlexPod インフラストラクチャ、サイト間のネットワーク接続、および 3 番目のサイトに導入された ONTAP メディエーターが含まれており、必要な RPO と RTO の目標を達成します。次の図に、各サイトの Cisco UCS B200M5 サーバと、サイト内およびサイト間の SM-BC 機能を備えたネットアップストレージとのエンドツーエンドのネットワーク接続を示します。



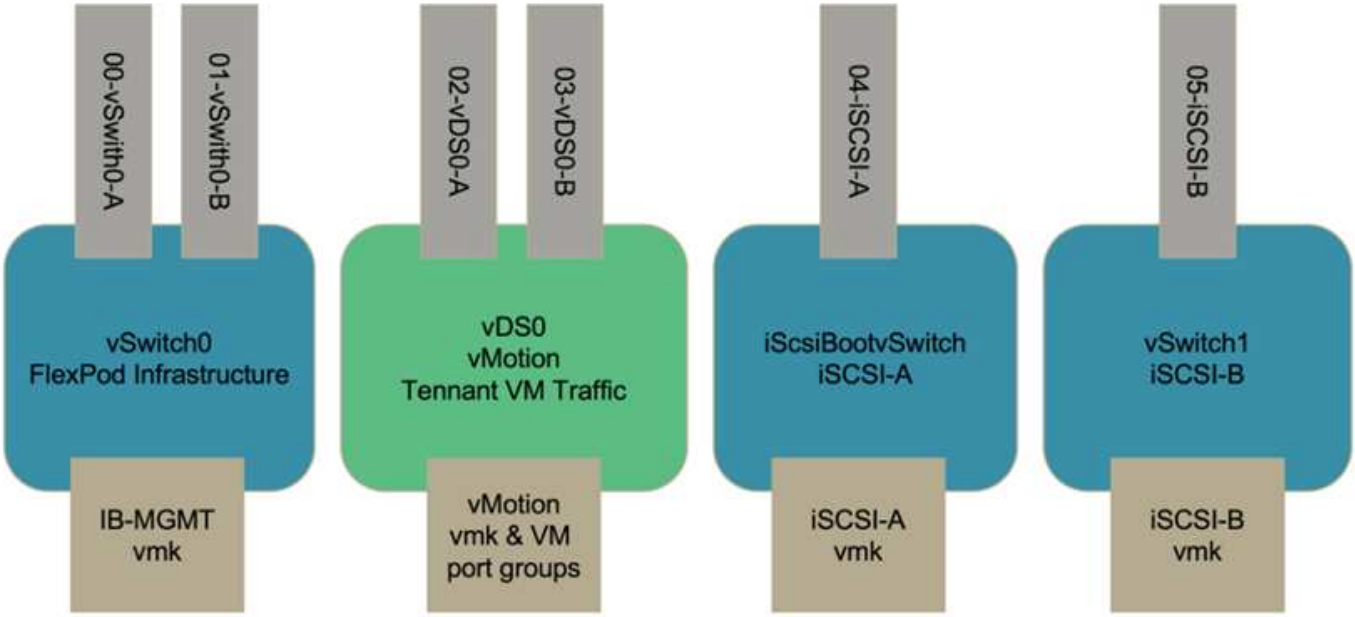
FlexPod の導入アーキテクチャは、この解決策 検証で各サイトで同じです。ただし、解決策 は非対称型の導入をサポートしており、要件を満たす既存の FlexPod ソリューションに追加することもできます。

拡張レイヤ 2 アーキテクチャは、各データセンターにおけるポートチャネルの Cisco UCS コンピューティングとネットアップストレージの間の接続、およびデータセンター間の接続を提供する、シームレスなマルチサイトデータファブリックに使用されます。ポートチャネルの構成、および必要に応じて仮想ポートチャネルの構成は、コンピューティングレイヤ、ネットワークレイヤ、ストレージレイヤ間の帯域幅集約とフォールトトレランス、およびクロスサイトリンクに使用されます。その結果、 UCS ブレードサーバは、ローカルとリモートの両方のネットアップストレージに接続され、マルチパスアクセスを提供します。

仮想ネットワーク

クラスタ内の各ホストは、場所に関係なく同一の仮想ネットワークを使用して導入されます。この設計では、VMware 仮想スイッチ（ vSwitch ）と VMware 仮想分散スイッチ（ vDS ）を使用して、さまざまなトラフィックタイプを分離しています。VMware vSwitch は主に FlexPod インフラネットワーク用、 vDS はアプリケーションネットワーク用ですが、必須ではありません。

仮想スイッチ（ vSwitch 、 vDS ）は、仮想スイッチごとに 2 つのアップリンクで展開されます。 ESXi ハイパーバイザーレベルのアップリンクは、 Cisco UCS ソフトウェアでは vmnic および仮想 NIC （ vNIC ）と呼ばれます。vNIC は、 Cisco UCS サービスプロファイルを使用して、各サーバの Cisco UCS VIC アダプタ上に作成されます。次の図に示すように、 6 つの vNIC が定義され、 vSwitch0 に 2 つ、 vDS0 に 2 つ、 vSwitch1 に 2 つ、 iSCSI アップリンクに 2 つです。



vSwitch0 は VMware ESXi ホストの設定中に定義され、管理用に FlexPod インフラ管理 VLAN と ESXi ホスト VMkernel （ VMK ）ポートが含まれています。インフラ管理仮想マシンポートグループも、必要な重要なインフラ管理仮想マシン用の vSwitch0 に配置されます。

このような管理インフラストラクチャ仮想マシンは、 vDS ではなく vSwitch0 に配置することが重要です。これは、 FlexPod インフラストラクチャがシャットダウンまたは電源の再投入された場合に、その管理仮想マシンが最初に実行されていたホスト以外のホストで、仮想マシンをアクティブ化しようとするためです。vSwitch0 のネットワークで正常にブートします。このプロセスは、 VMware vCenter が管理仮想マシンである場合は特に重要です。vCenter が vDS 上にあり、別のホストに移動してブートした場合、起動後にネットワークに接続されません。

この設計では、 2 つの iSCSI ブート vSwitch を使用します。Cisco UCS iSCSI ブートには、 iSCSI ブート用に個別の vNIC が必要です。これらの vNIC は、適切なファブリックの iSCSI VLAN をネイティブ VLAN として使用し、適切な iSCSI ブート vSwitch に接続されます。また、新しい vDS を導入するか、既存の vDS を使用して、 vDS に iSCSI ネットワークを導入することもできます。

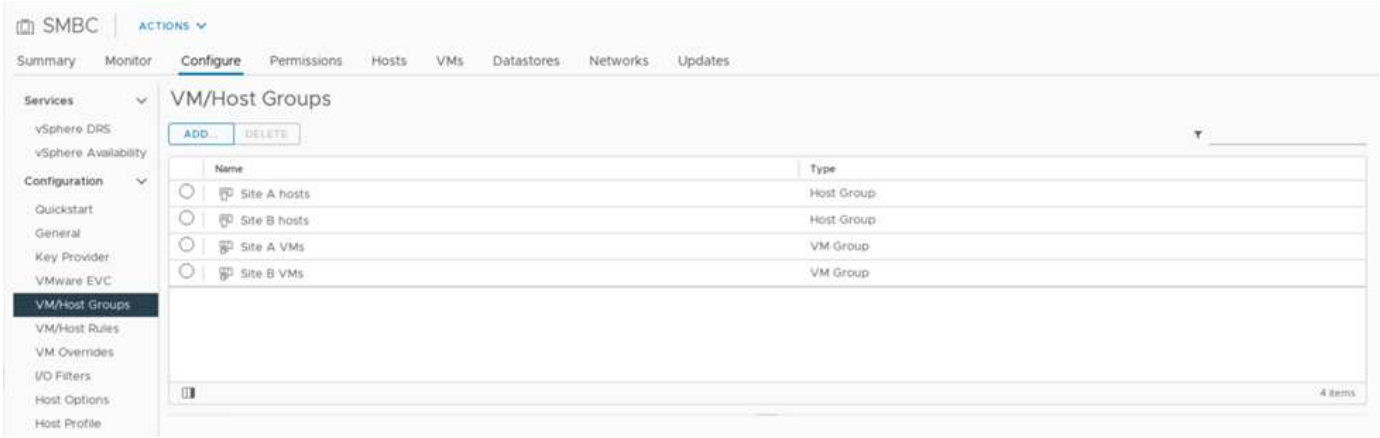
VM とホストのアフィニティグループとルール

両方の SM-BC サイトで任意の ESXi ホスト上で仮想マシンを実行できるようにするには、すべての ESXi ホストが両方のサイトから iSCSI データストアをマウントする必要があります。両方のサイトのデータストアがすべての ESXi ホストで適切にマウントされている場合は、 vMotion を使用するすべてのホスト間で仮想マシンを移行しても、それらのデータストアから作成されたすべての仮想ディスクへのアクセスは維持されます。

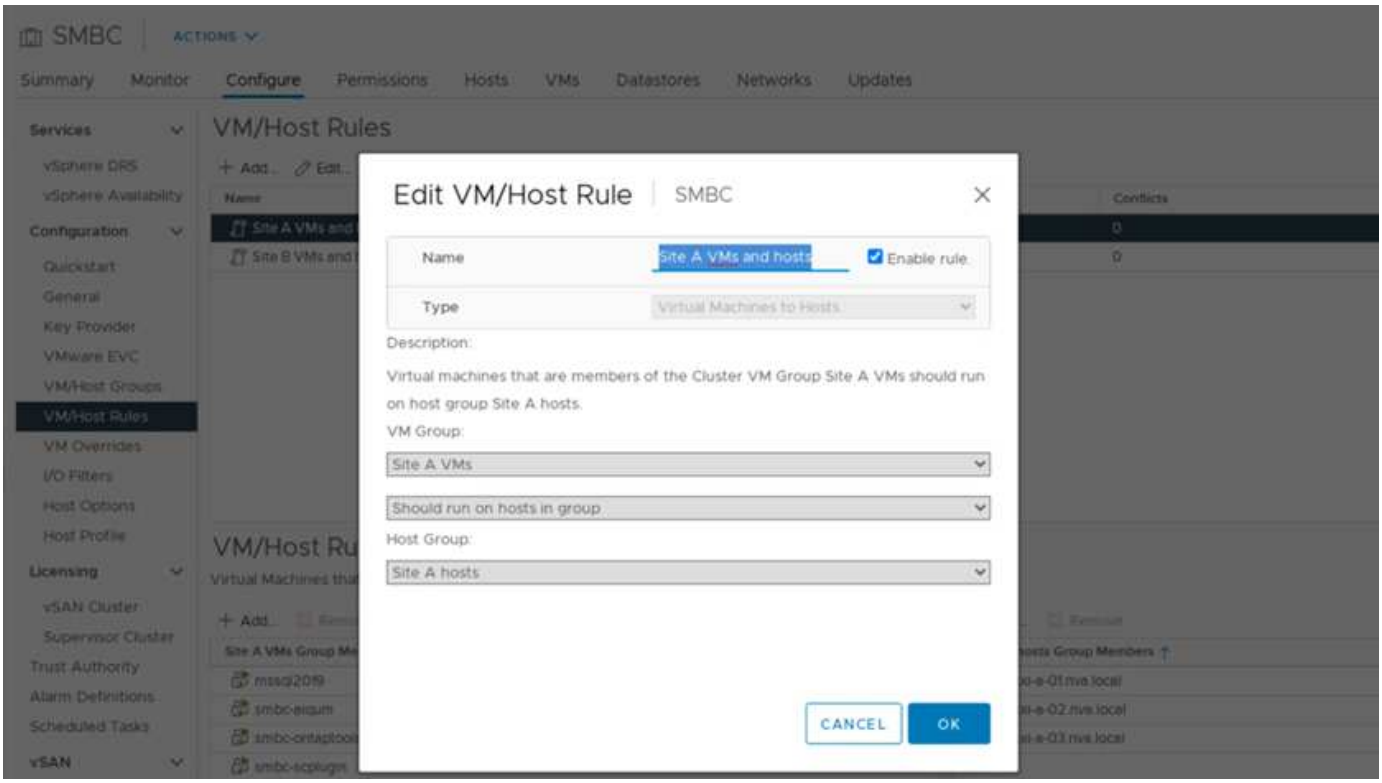
ローカルデータストアを使用する仮想マシンの場合、仮想ディスクがリモートサイトのホストに移行されると、仮想ディスクへのアクセスがリモートになり、サイト間の物理的な距離による読み取り処理のレイテンシが増加します。そのため、ローカルホストに仮想マシンを保持し、サイトでローカルストレージを利用することを推奨します。

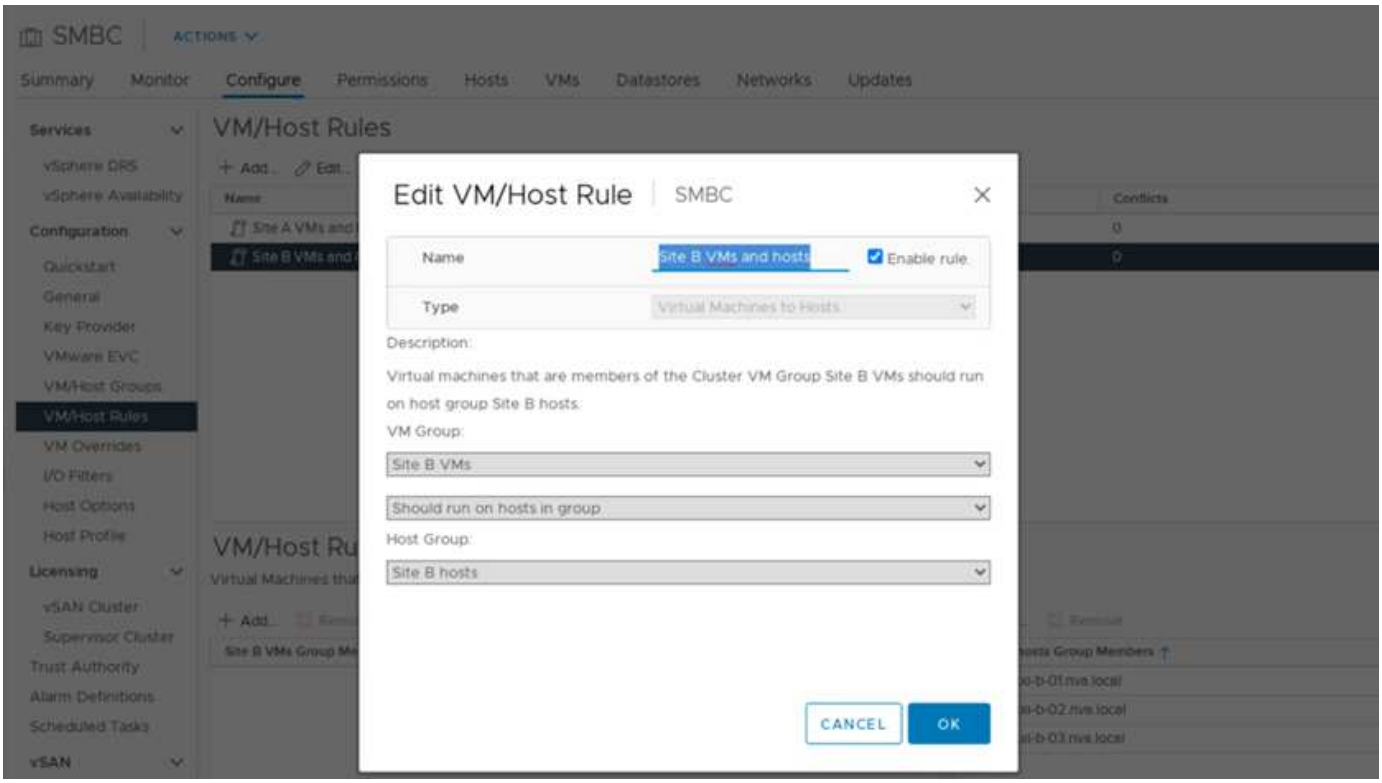
VM とホストのアフィニティメカニズムを使用すると、 VM / ホストグループを作成して、特定のサイトに配置された仮想マシンとホストの VM グループとホストグループを作成できます。VM/ ホストルールを使用して、 VM とホストが従うポリシーを指定できます。サイトのメンテナンスまたは災害時にサイト間で仮想マシンを移行できるようにするには、その柔軟性のため、「グループ内のホストで実行する」ポリシー仕様を使用します。

次のスクリーンショットは、サイト A とサイト B のホストおよび VM について、 2 つのホストグループと 2 つの VM グループが作成されたことを示しています



さらに、次の 2 つの図は、「グループ内のホストで実行する必要があります」ポリシーを使用して、サイト A およびサイト B の VM がそれぞれのサイトのホストで実行されるように作成された VM/ ホストルールを示しています。

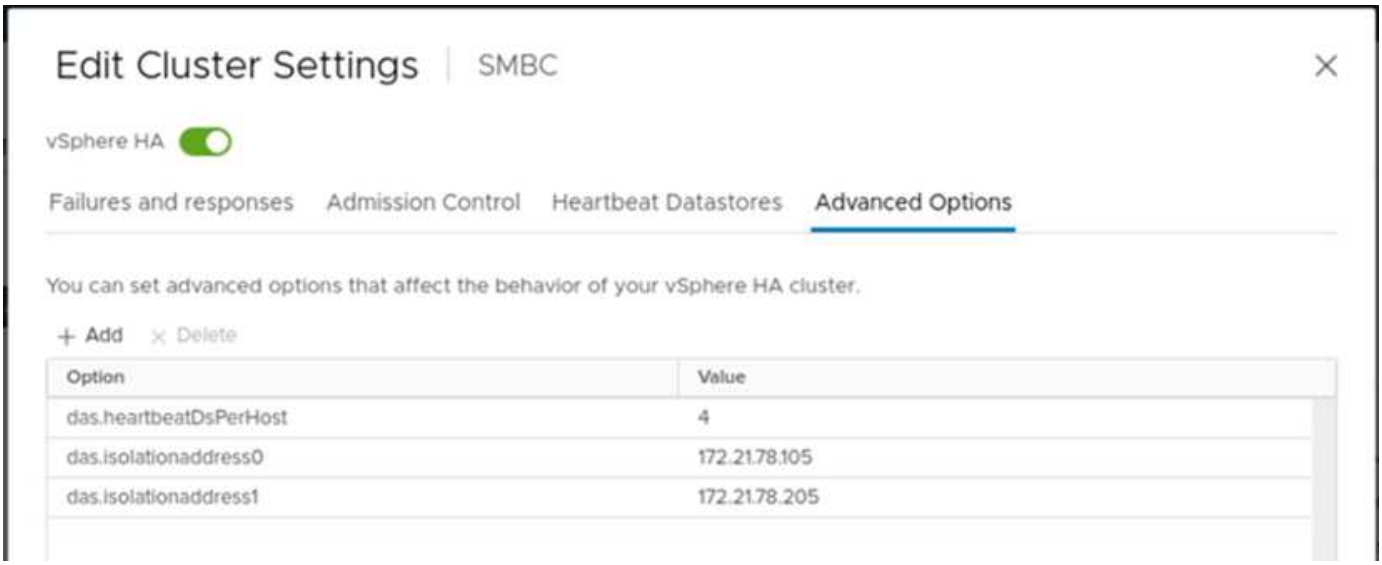




vSphere HA ハートビート

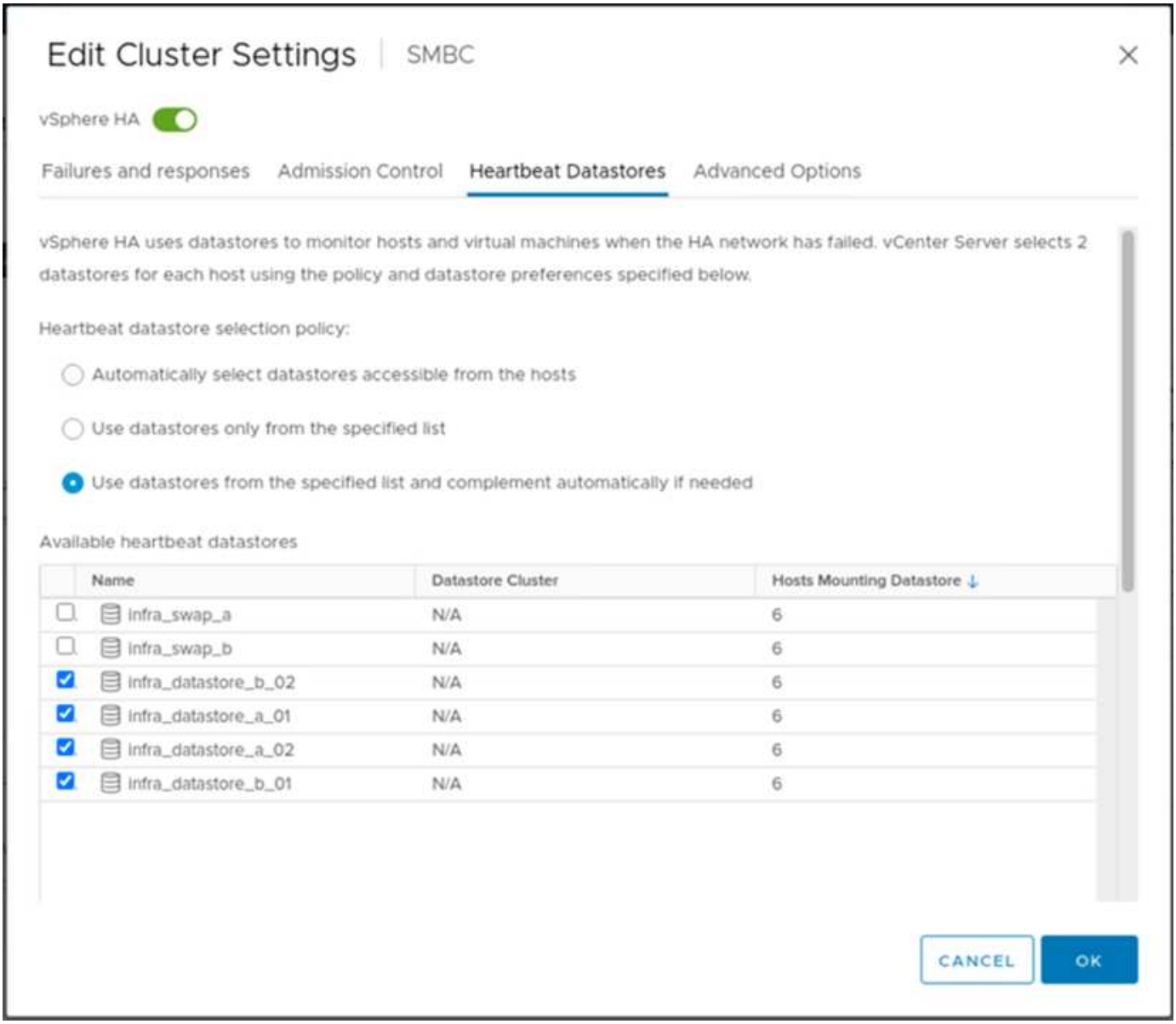
VMware vSphere HA は、ホストの状態を検証するためのハートビートメカニズムを備えています。一次ハートビートメカニズムはネットワーク経由で行われ、二次ハートビートメカニズムはデータストアを経由します。ハートビートを受信しない場合は、デフォルトゲートウェイに ping を送信するか、手動で設定した隔離アドレスに基づいて、ハートビートをネットワークから隔離するかを決定します。データストアのハートビートでは、ストレッチクラスタのハートビートデータストアを最小構成から 4 つに増やすことを推奨します。

解決策 の検証では、 2 つの ONTAP クラスタ管理 IP アドレスを隔離アドレスとして使用します。また、次の図に示すように、推奨される vSphere HA の詳細オプション「 DS.heartbeatDsPerHost 」の値が 4 に追加されました。



ハートビートデータストアの場合、クラスタから 4 つの共有データストアを指定し、次の図に示すようにそ

れを補完します。



VMware HA Cluster および VMware vSphere Metro ストレージクラスタのその他のベストプラクティスおよび設定については、を参照してください "vSphere HA クラスタを作成および使用する"、 "VMware vSphere Metro Storage Cluster （ vMSC ）" およびの VMware KB です "NetApp ONTAP と NetApp SnapMirror のビジネス継続性（ SM-BC ）および VMware vSphere Metro Storage Cluster （ vMSC ）"。

"次：解決策 の検証済みのシナリオ"

解決策 の検証済みのシナリオ

"前のバージョン：解決策 の検証 - 仮想化。"

FlexPod Datacenter SM-BC 解決策 は、さまざまな単一点障害のシナリオやサイト障害に対するデータサービスを保護します。各サイトに実装された冗長設計は高可用性を提供し、サイト間で同期データレプリケーションを行う SM-BC 実装は、サイト規模の災害からデータサービスを保護します。導入した解決策 は、目的の解決策 機能や、解決策

が保護対象として設計されたさまざまな障害シナリオに対して検証されます。

解決策 関数の検証

解決策 の機能を検証し、部分的および完全なサイト障害シナリオをシミュレートするために、さまざまなテストケースが使用されます。シスコ検証済み設計プログラムの既存の FlexPod データセンターソリューションですでに実行されているテストで重複を最小限に抑えるため、このレポートでは、解決策 の SM-BC 関連の側面に焦点を当てています。実践者が実装検証に使用する一般的な FlexPod 検証が含まれています。

解決策 の検証では、両方のサイトのすべての ESXi ホストに、 ESXi ホストごとに 1 台の Windows 10 仮想マシンが作成されました。IOMeter ツールがインストールされ、共有ローカル iSCSI データストアからマッピングされた 2 つの仮想データディスクへの I/O を生成するために使用されました。IOMeter ワークロードパラメータは、 8 KB の I/O 、 75% の読み取り、 50% のランダムで、各データディスクに 8 つの未処理 I/O コマンドを設定しました。実行されたテストシナリオのほとんどでは、 IOMeter I/O の継続は、シナリオがデータサービスの停止を原因 しなかったことを示すものです。

SM-BC はデータベース・サーバなどのビジネス・アプリケーションにとって重要であるため ' Windows Server 2022 仮想マシン上の Microsoft SQL Server 2019 インスタンスもテストの一環として提供されました。ローカルサイトのストレージが使用できず、アプリケーションがない状態でリモートサイトのストレージでデータサービスが再開される場合に、アプリケーションの実行が継続されることを確認しました 中断：

ESXi ホスト **iSCSI SAN** ブートテスト

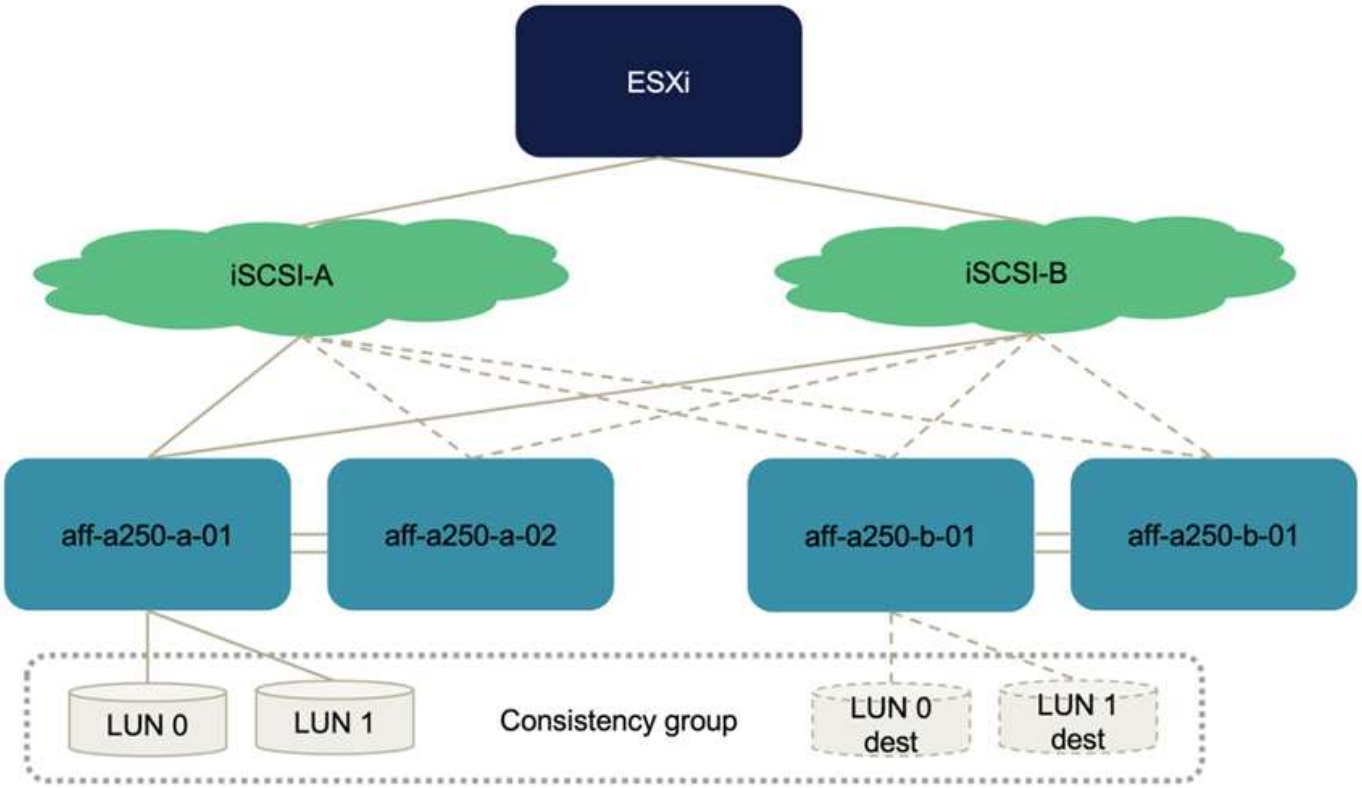
解決策 内の ESXi ホストは、 iSCSI SAN からブートするように設定されます。SAN ブートを使用すると、サーバを交換する際のサーバ管理が簡素化されます。これは、サーバのサービスプロファイルを新しいサーバに関連付けて、サーバが起動するために追加の設定変更を行う必要がないためです。

サイトにある ESXi ホストをローカルの iSCSI ブート LUN からブートする以外に、ローカルのストレージコントローラがテイクオーバー状態のときやローカルのストレージクラスタが完全に使用できないときに ESXi ホストをブートするテストも実施しました。これらの検証シナリオでは、 ESXi ホストが設計に従って適切に構成されており、ストレージのメンテナンス時やディザスタリカバリの際にブートしてビジネス継続性を実現できることを確認します。

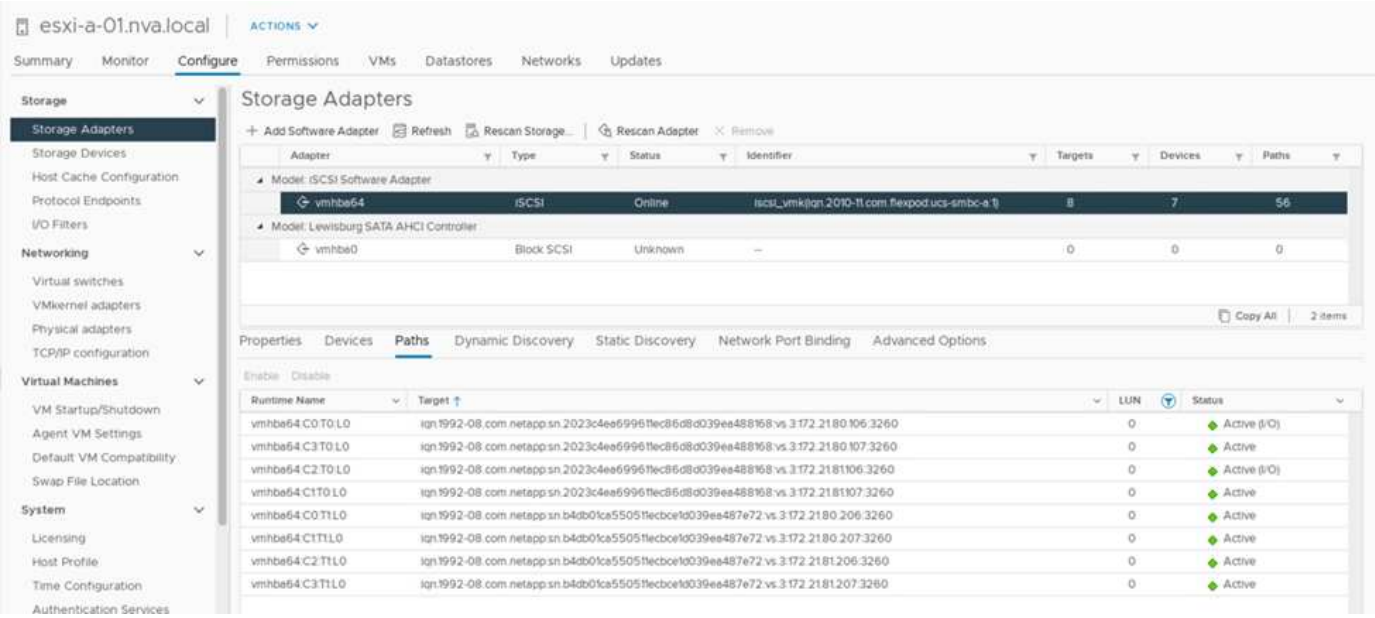
SM-BC 整合グループ関係を設定する前に、ストレージコントローラ HA ペアでホストされる iSCSI LUN には、ベストプラクティスの実装に基づいて、各 iSCSI ファブリックに 2 つずつ、合計 4 つのパスがあります。ホストは、 2 つの iSCSI VLAN / ファブリック経由で LUN にアクセスでき、 LUN ホスティングコントローラやコントローラのハイアベイラビリティパートナー経由で LUN にアクセスできます。

SM-BC 整合グループ関係を設定し、ミラーリングされた LUN をイニシエータに適切にマッピングすると、 LUN のパス数は 2 倍になります。この実装では、 2 つのアクティブ / 最適化パスと 2 つのアクティブ / 非最適化パスがあることから、 2 つのアクティブ / 最適化パスと 6 つのアクティブ / 非最適化パスがあることになります。

次の図は、 LUN 0 など、 ESXi ホストから LUN にアクセスするためのパスを示しています。LUN はサイト A のコントローラ 01 に接続されているため、そのコントローラを介して LUN に直接アクセスする 2 つのパスのみがアクティブ / 最適化され、残りの 6 つのパスはすべてアクティブ / 非最適化されます。



次のスクリーンショットは、 ESXi ホストが 2 種類のデバイスパスを認識する方法を示しています。2 つのアクティブ / 最適化されたパスは ' アクティブ (I/O) パスステータスであると表示されます一方 ' アクティブ / 非最適化パスはアクティブパスとしてのみ表示されますまた、 Target 列には、ターゲットに到達するための 2 つの iSCSI ターゲットとそれぞれの iSCSI LIF の IP アドレスが表示されます。



メンテナンスやアップグレードのために一方のストレージコントローラが停止した場合、停止しているコントローラに到達する 2 つのパスは使用できなくなり、パスステータスが「 dead 」と表示されます。

手動フェイルオーバーテストまたは自動ディザスタフェイルオーバーのために、プライマリストレージクラスタで整合性グループのフェイルオーバーが発生した場合、セカンダリストレージクラスタは引き続き、 SM-BC 整合グループ内の LUN にデータサービスを提供します。LUN ID が保持され、データが同期的にレプリケ

ートされているため、 SM-BC 整合グループで保護された ESXi ホストブート LUN は、すべてリモートストレージクラスタから引き続き使用できます。

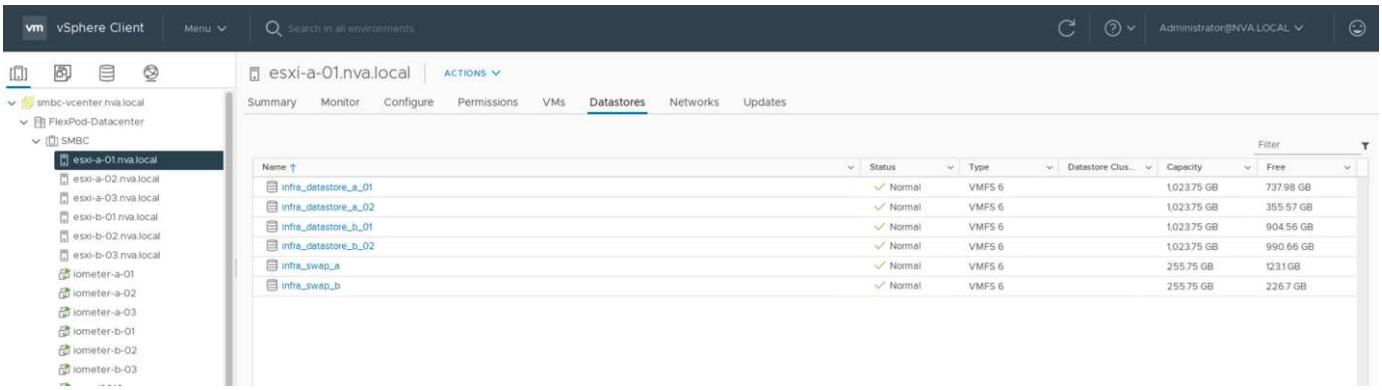
VMware vMotion と **VM** とホストのアフィニティテスト

汎用の FlexPod VMware Datacenter 解決策 は、 FC 、 iSCSI 、 NVMe 、 NFS などのマルチプロトコルをサポートしていますが、 FlexPod SM-BC 解決策 機能は、一般にビジネスクリティカルなソリューションに使用される FC および iSCSI SAN プロトコルをサポートしています。この検証で使用されるのは、 iSCSI プロトコルベースのデータストアと iSCSI SAN ブートのみです。

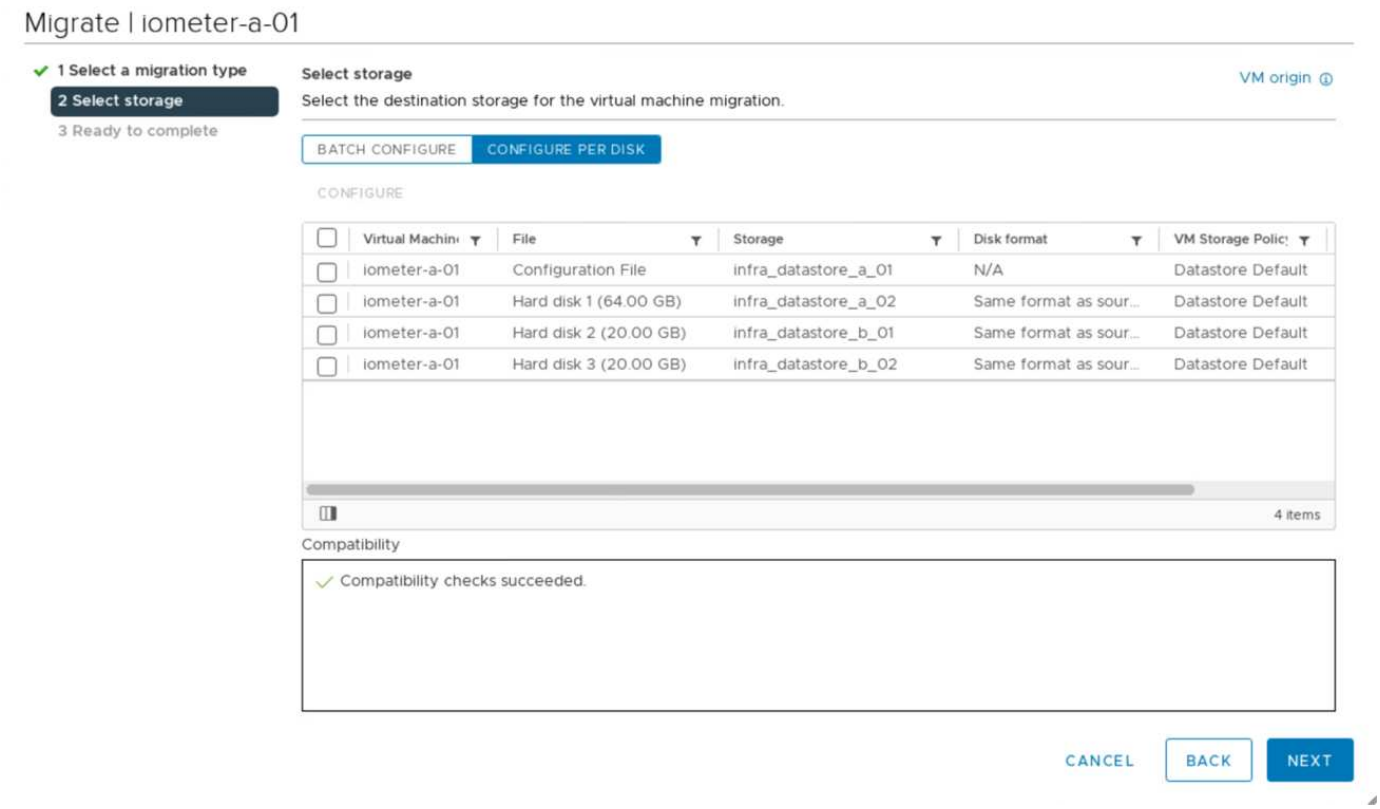
いずれかの SM-BC サイトのストレージサービスを仮想マシンで使用できるようにするには、 2 つのサイト間で仮想マシンを移行したり、災害時のフェイルオーバー・シナリオに備えて、両方のサイトの iSCSI データストアをクラスタ内のすべてのホストにマウントする必要があります。

サイト間での SM-BC 整合グループ保護を必要としない仮想インフラ上で実行されるアプリケーションの場合は、 NFS プロトコルと NFS データストアも使用できます。その場合、ビジネス継続性を確保するために、ビジネスクリティカルなアプリケーションが SM-BC 整合グループで保護された SAN データストアを適切に使用しているように、 VM にストレージを割り当てるときは注意が必要です。

次のスクリーンショットは、両方のサイトの iSCSI データストアをマウントするようにホストが設定されていることを示しています。



次の図に示すように、両方のサイトの使用可能な iSCSI データストア間で仮想マシンディスクを移行することもできます。パフォーマンスに関する考慮事項としては、ディスク I/O レイテンシを低減するために、ローカルストレージクラスタのストレージを使用する仮想マシンを用意することを推奨します。これは、 2 つのサイトが距離を隔てた場所にある場合に特に該当します。これは、距離が 100km ごとに約 1 ミリ秒という物理的なラウンドトリップ距離によるレイテンシによるものです。



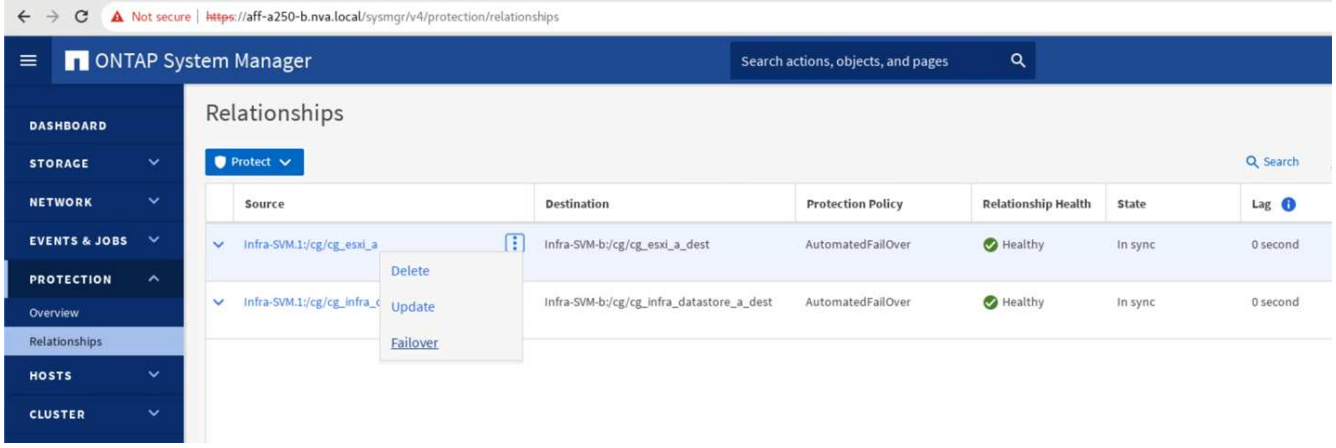
同じサイトにある別のホスト、およびサイト間で仮想マシンの vMotion をテストし、正常に実行された。サイト間で仮想マシンを手動で移行すると、 VM とホストのアフィニティルールがアクティブになり、仮想マシンが通常の状態にあるグループに移行されます。

ストレージのフェイルオーバーを計画

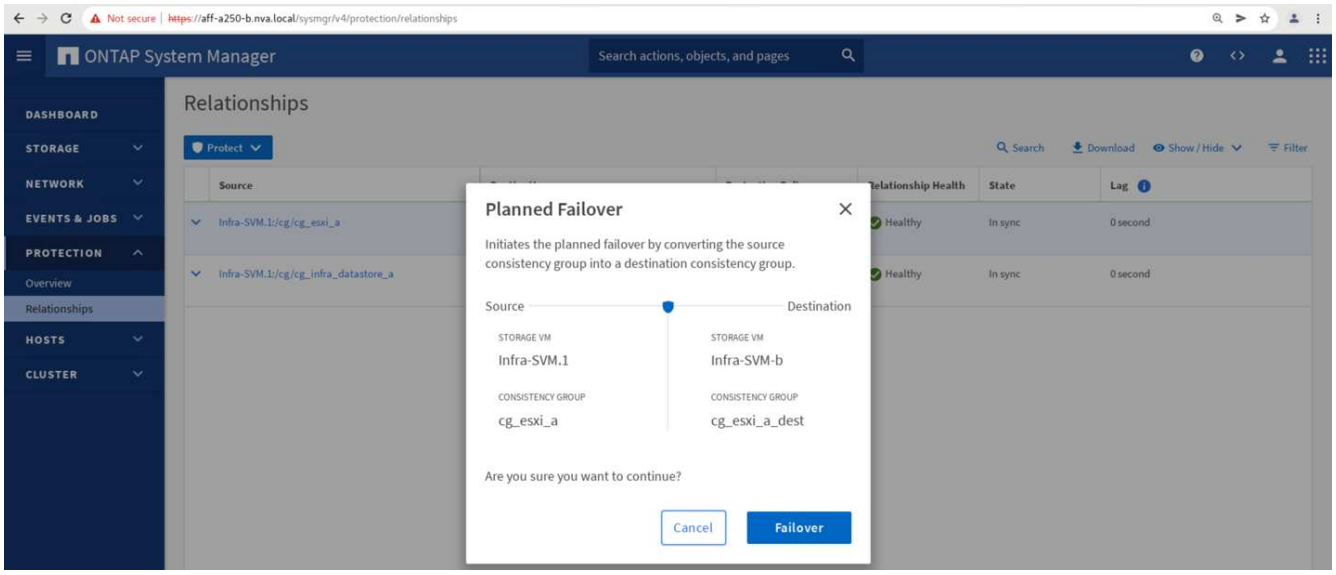
ストレージフェイルオーバー後に解決策 が適切に機能しているかどうかを確認するには、初期設定後に解決策 で計画的なストレージフェイルオーバー処理を実行する必要があります。このテストは、 I/O の停止を招く可能性のある接続や構成の問題を特定するのに役立ちます。接続や設定の問題を定期的にテストして解決することで、実際のサイトで障害が発生してもデータサービスを中断なく提供できます。計画的ストレージフェイルオーバーは、スケジュールされたストレージメンテナンスアクティビティの前にも使用できます。これにより、影響を受けないサイトからデータサービスを提供できます。

サイト A のストレージデータサービスをサイト B に手動でフェイルオーバーするには、サイト B の ONTAP システムマネージャを使用して処理を実行します。

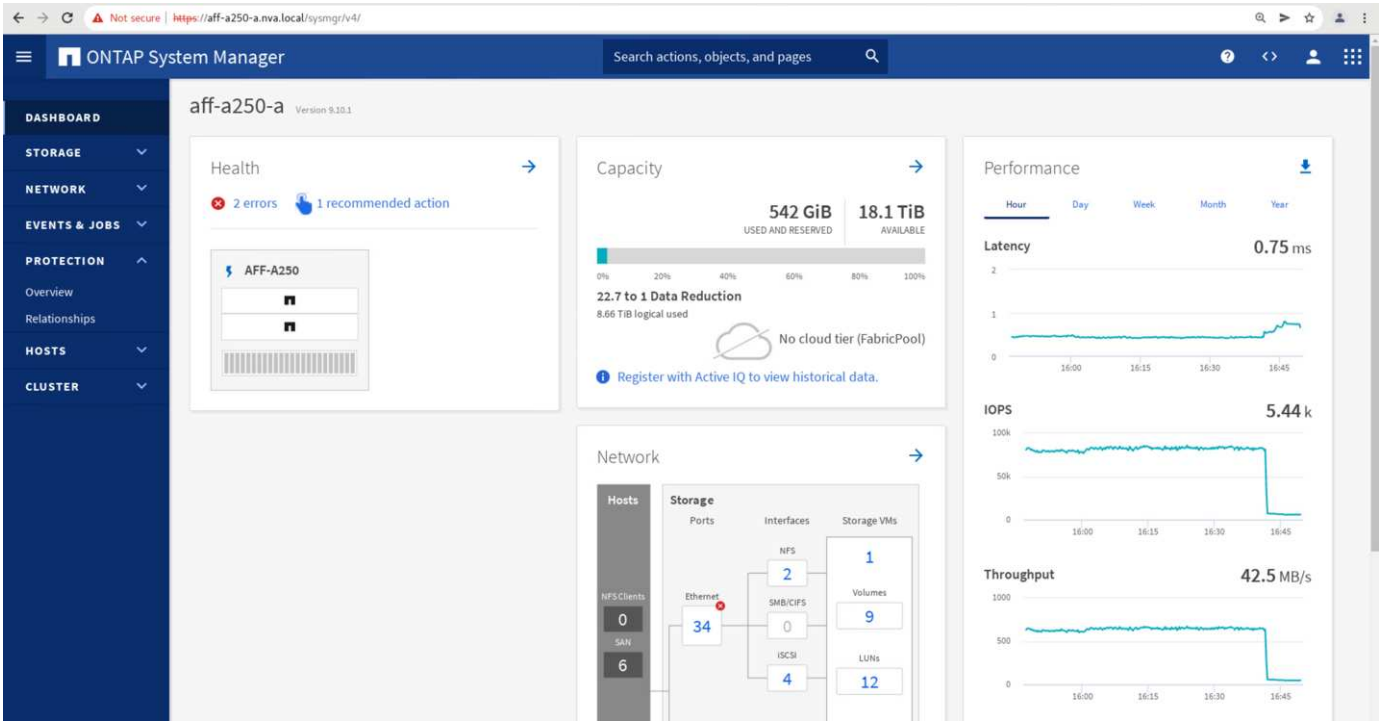
1. Protection > Relationships 画面に移動して ' コンシステンシ・グループの関係状態が In Sync' であることを確認しますまだ「同期中」状態の場合は、状態が「同期中」になるまで待ってからフェイルオーバーを実行します。
2. ソース名の横にあるドットを展開し、フェイルオーバーをクリックします。



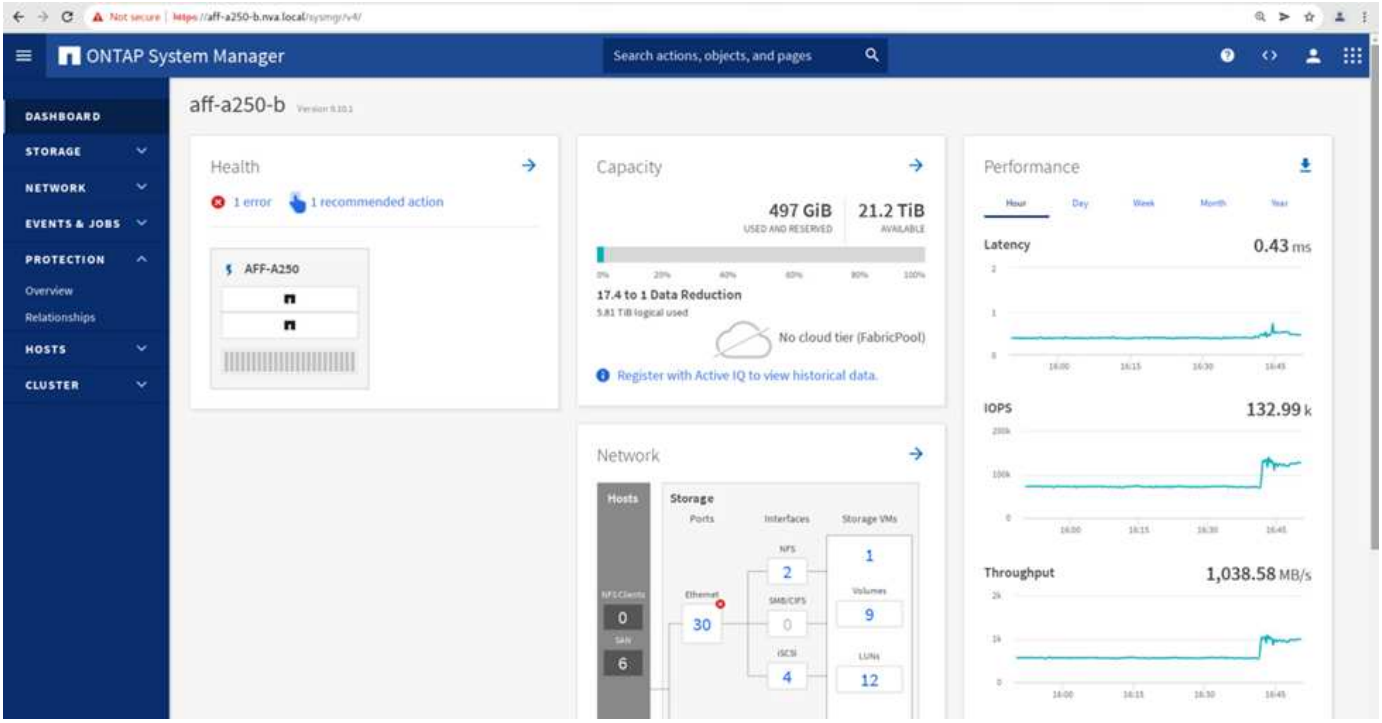
3. 処理を開始するには、フェイルオーバーを確認してください。



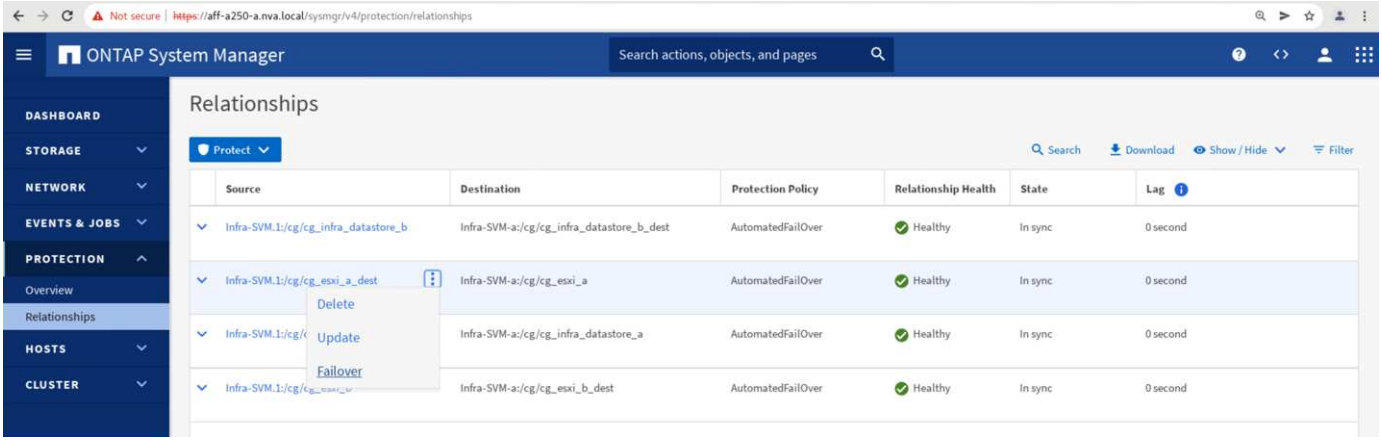
2 つのコンシステンシグループ「 cg_esxi_a 」および「 cg_infra_datastore_a 」のフェイルオーバーがサイト B の System Manager GUI で開始された直後に、これら 2 つのコンシステンシグループを処理するサイト A の I/O がサイト B に移動されましたそのため、サイト A の System Manager のパフォーマンスペインでは、サイト A の I/O が大幅に削減されました。



一方、サイト B の System Manager ダッシュボードの Performance ペインでは、サイト A から約 130K IOPS に移動された追加の I/O を処理するため、 IOPS が大幅に増加しています。 1 ミリ秒未満の I/O レイテンシを維持したまま、約 1GB/s のスループットを実現しました。

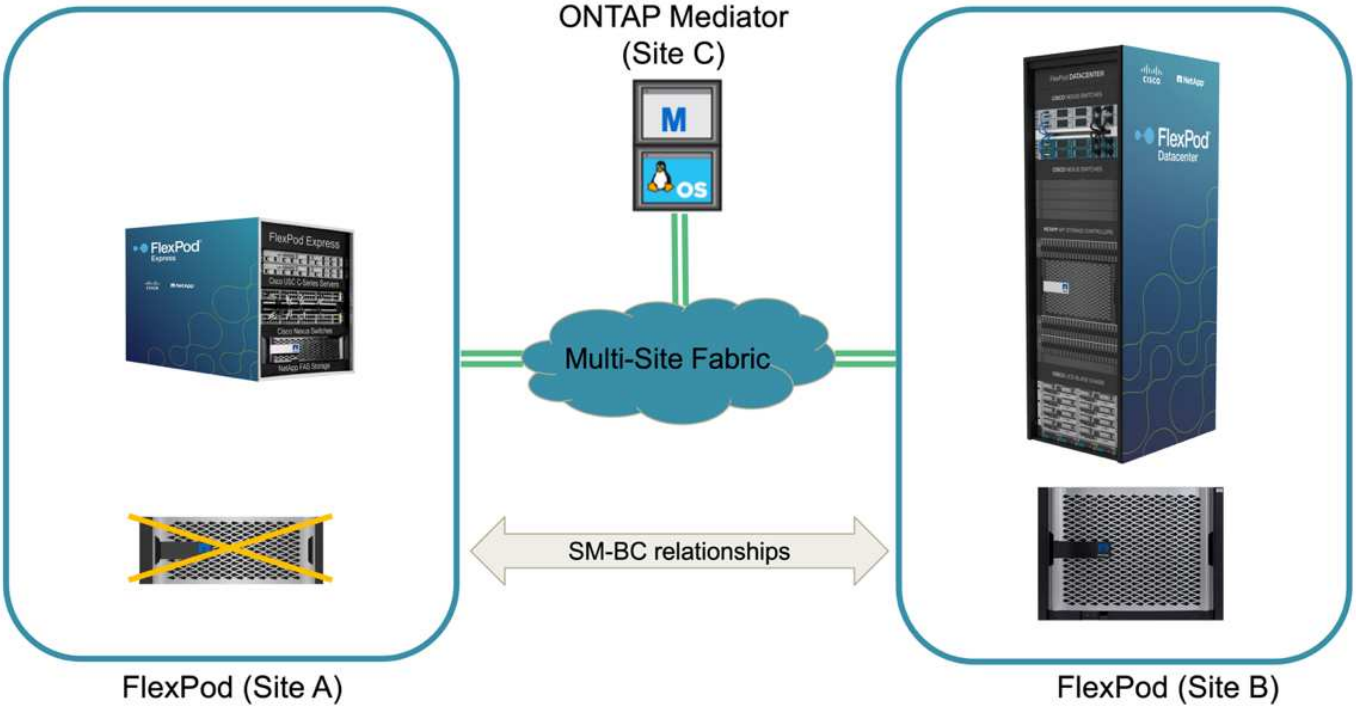


I/O をサイト A からサイト B に透過的に移行することで、計画的なメンテナンスのためにサイト A のストレージコントローラを停止できるようになります。メンテナンス作業またはテストが完了し ' サイト A のストレージ・クラスタが稼働状態に戻ったら ' フェイルオーバーを実行してサイト B からサイト A へのフェイルオーバー I/O を返す前に ' コンシステンシ・グループの保護状態が同期状態に戻るまでチェックして待機します メンテナンスまたはテストのためにサイトが停止される時間が長くなると ' データが同期されるまでの時間が長くなり ' コンシステンシ・グループは同期状態に戻ります



ストレージの計画外フェイルオーバー

実際に災害が発生した場合や災害シミュレーション中に、計画外のストレージフェイルオーバーが発生することがあります。たとえば、次の図では、サイト A のストレージシステムで停電が発生し、計画外のストレージフェイルオーバーがトリガーされたあと、サイト A の LUN が SM-BC 関係で保護されている場合、サイト B から続行します

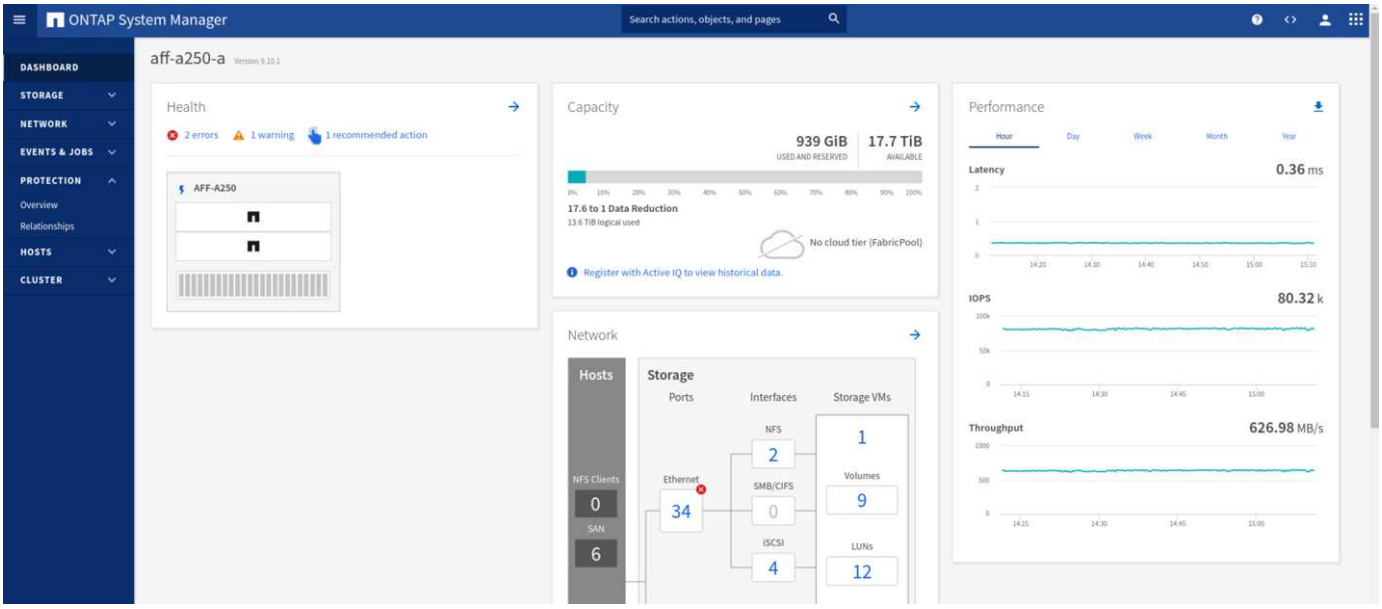


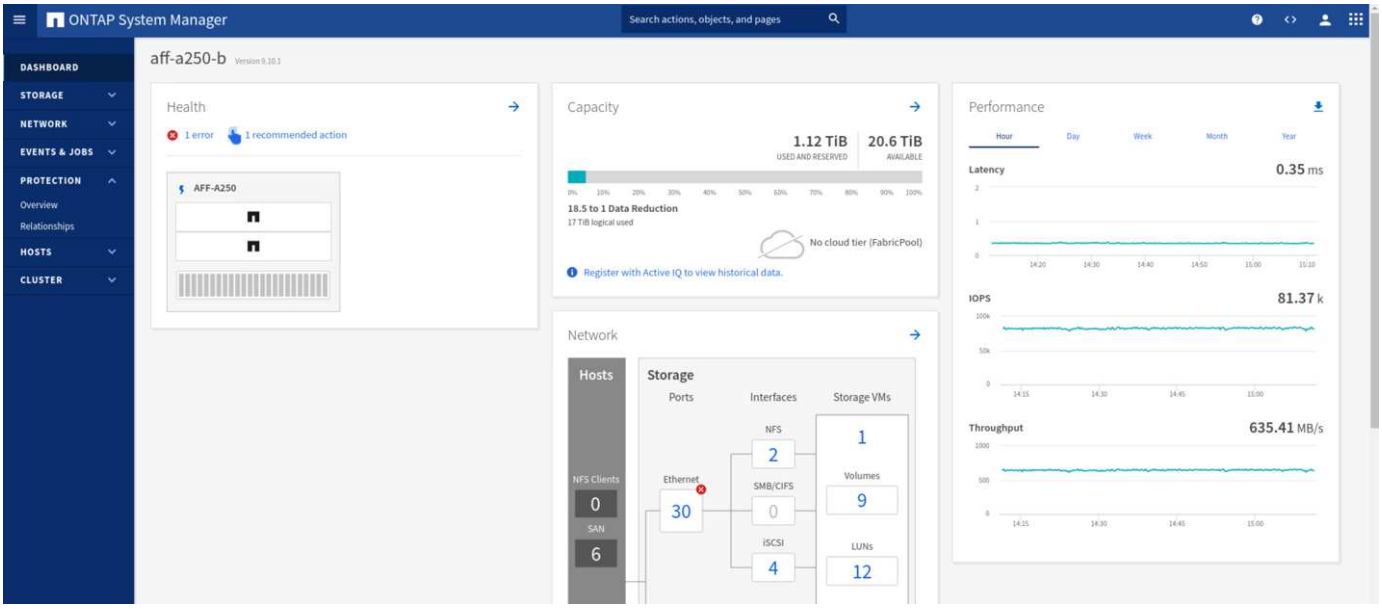
サイト A でストレージ災害をシミュレートするために、サイト A の両方のストレージコントローラの電源スイッチを物理的にオフにしてコントローラへの電源供給を停止することで、両方のコントローラの電源をオフにできます。 または、ストレージコントローラのサービスプロセッサの system power management コマンドを使用してコントローラの電源をオフにします。

サイト A のストレージクラスタが電力を喪失した場合は、サイト A のストレージクラスタが提供するデータサービスが突然停止します。次に、第 3 のサイトから SM-BC 解決策 を監視する ONTAP メディエーターが、サイト A のストレージ障害状態を検出し、 SM-BC 解決策 で自動計画外フェイルオーバーを実行できるようにします。これにより、サイト B のストレージコントローラは、サイト A との SM-BC 整合グループ関係で設定された LUN のデータサービスを継続できます

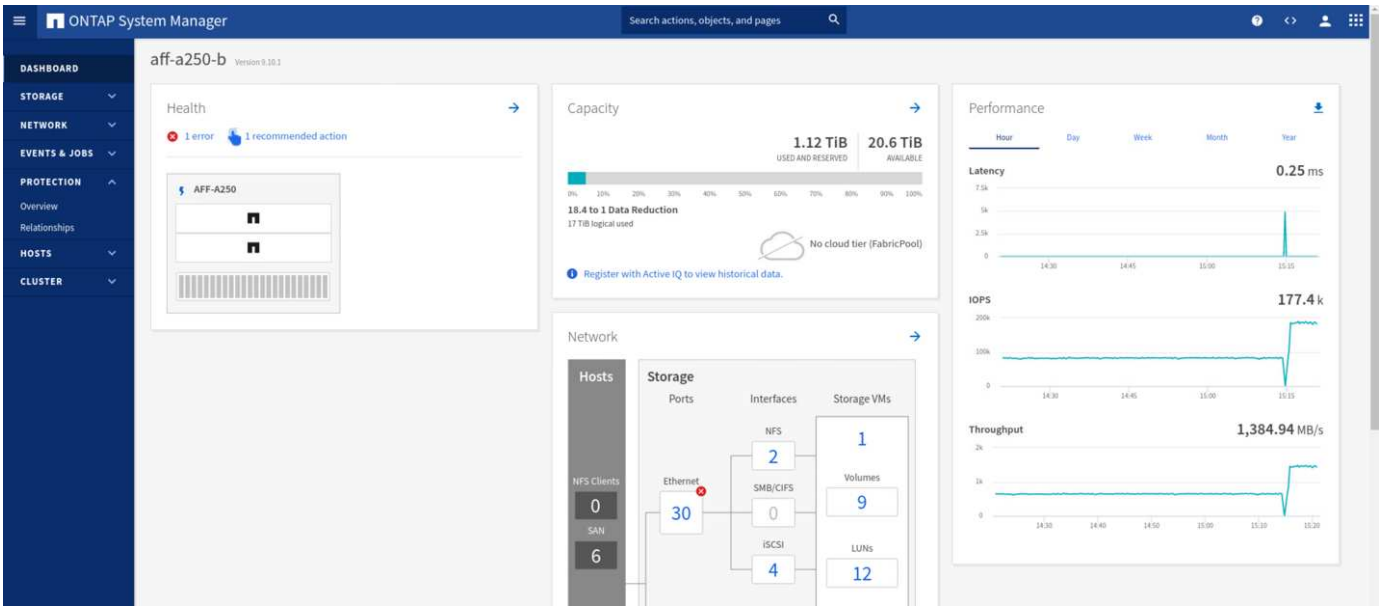
アプリケーション側では、オペレーティングシステムが LUN のパスステータスを確認し、稼働しているサイト B のストレージコントローラへの利用可能なパスで I/O を再開する間、データサービスは一時的に停止します。

検証テストでは、両方のサイトの VM の IOMeter ツールがローカルデータストアへの I/O を生成します。サイト A のクラスタの電源をオフにすると、 I/O が一時停止してから再開されます。災害発生前は、サイト A とサイト B のストレージクラスタのダッシュボードについて、次の 2 つの図をそれぞれ参照してください。各サイトでの約 80 、 000 IOPS と 600 MB/ 秒のスループットを示しています。

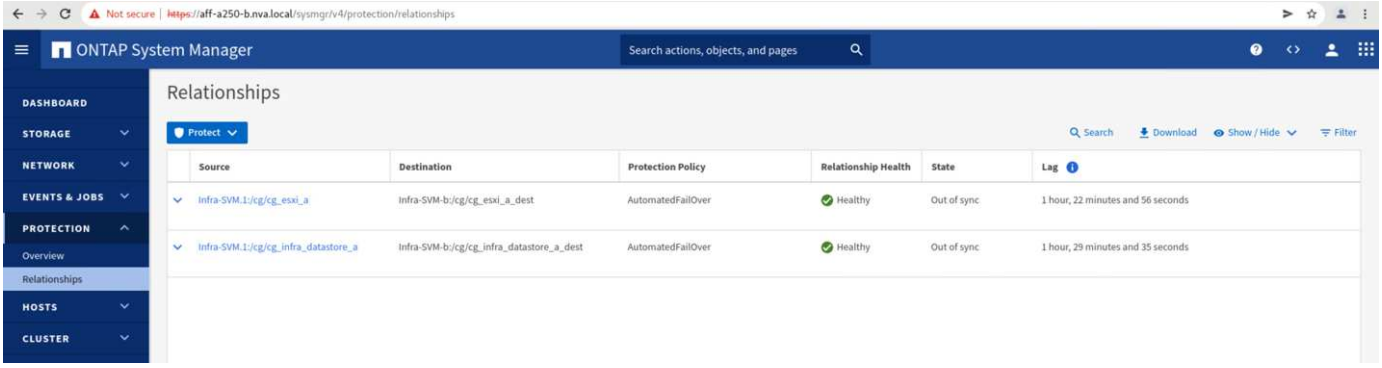




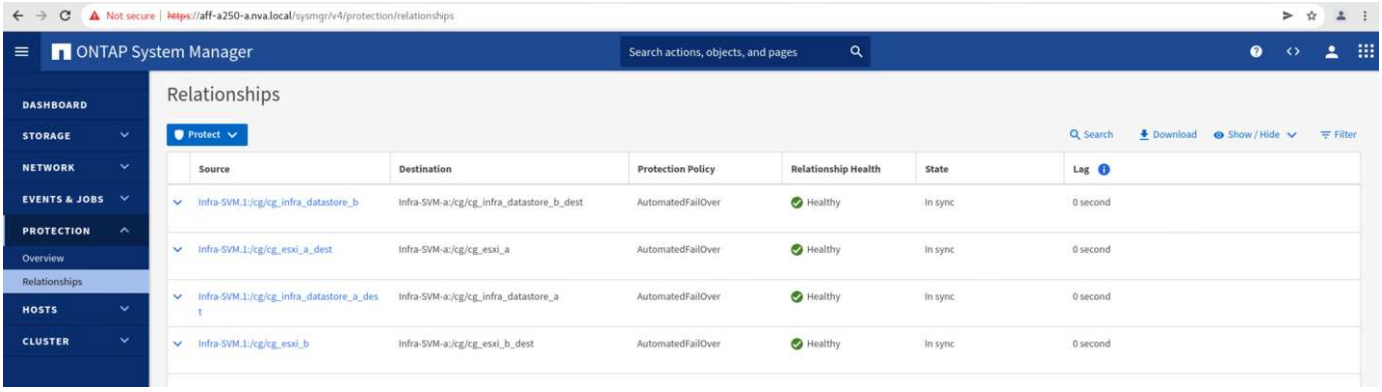
サイト A のストレージコントローラの電源をオフにしたあと、サイト A に代わって追加のデータサービスを提供するために、サイト B のストレージコントローラの I/O が大幅に増加したことを視覚的に確認できます（次の図を参照）。また、 IOMeter VM の GUI には、サイト A のストレージクラスタが停止しても I/O が継続することが示されました。SM-BC 関係で保護されていない LUN から作成されたデータストアがほかにもある場合、ストレージ災害の発生時にこれらのデータストアにアクセスできなくなります。そのため、さまざまなアプリケーションデータのビジネスニーズを評価し、ビジネス継続性を確保するために、 SM-BC 関係で保護されたデータストアに適切に配置することが重要です。



次の図に示すように ' サイト A のクラスタがダウンしている間 ' 整合性のあるグループの関係のステータスは非同期状態になりますサイト A のストレージコントローラの電源をオンに戻すと、ストレージクラスタがブートし、サイト A とサイト B の間のデータ同期が自動的に実行されます。



サイト B からサイト A にデータサービスを戻す前に、サイト A の System Manager を調べて、 SM-BC 関係がキャッチされ、ステータスが同期されていることを確認する必要があります。整合グループが同期されていることを確認したら、手動のフェイルオーバー処理を開始して、整合グループ関係のデータサービスをサイト A に戻すことができます



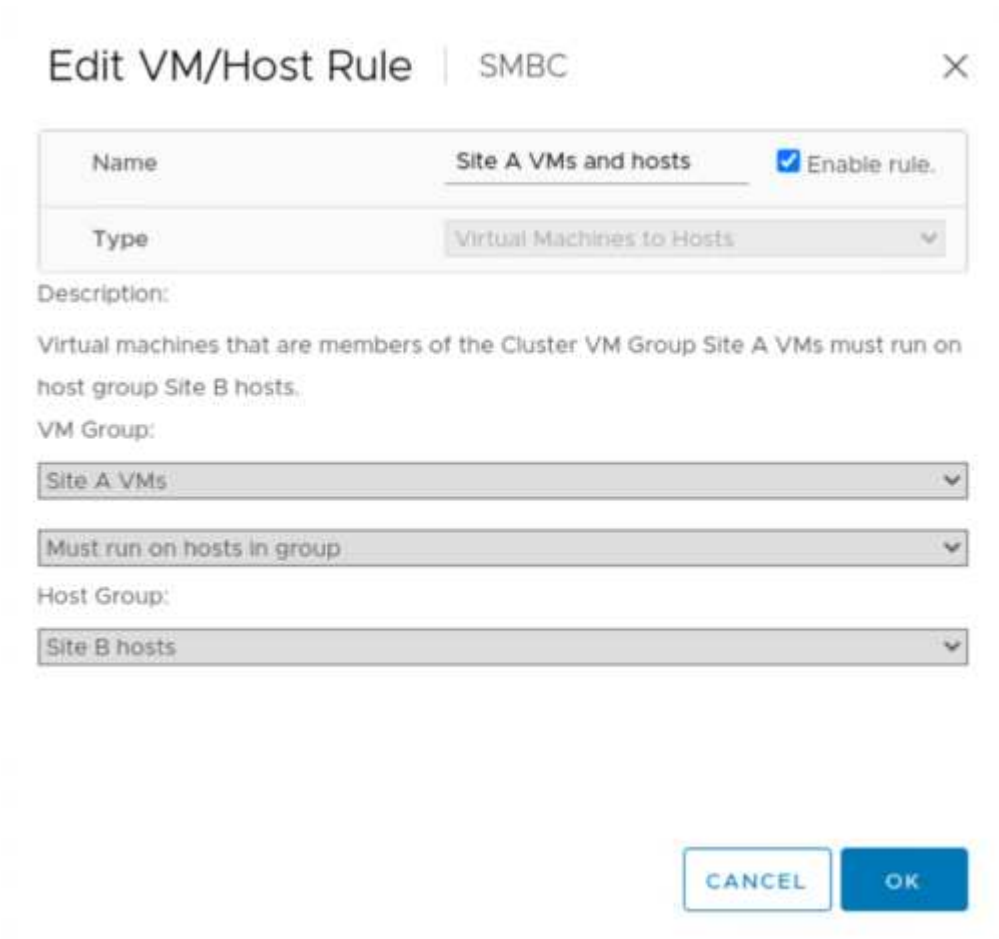
サイトのメンテナンスやサイト障害が発生したときの対処

サイトのメンテナンスや停電が発生したり、ハリケーンや地震などの自然災害によって影響が及ぶ可能性があります。そのため、計画的および計画外のサイト障害シナリオを実施して、 FlexPod SM-BC 解決策 が、ビジネスクリティカルなすべてのアプリケーションおよびデータサービスでこのような障害が発生しても運用を継続できるように適切に設定されていることを確認することが重要です。検証されたサイト関連のシナリオは次のとおりです。

- 仮想マシンと重要なデータサービスをもう一方のサイトに移行することで、サイトの計画的なメンテナンスシナリオを実施します
- ディザスタシミュレーション用にサーバとストレージコントローラの電源をオフにして、サイトが計画外停止になる状況です

サイトを計画的なサイトメンテナンスにするには、影響を受けた仮想マシンを vMotion と組み合わせてサイトから移行し、 SM-BC 整合グループ関係を手動でフェイルオーバーして、仮想マシンと重要なデータサービスを代替サイトに移行する必要があります。テストは、まず vMotion 、次に SM-BC フェイルオーバーと SM-BC フェイルオーバー、続いて vMotion という 2 つの順序で実行され、仮想マシンが引き続き実行され、データサービスが中断されないことを確認します。

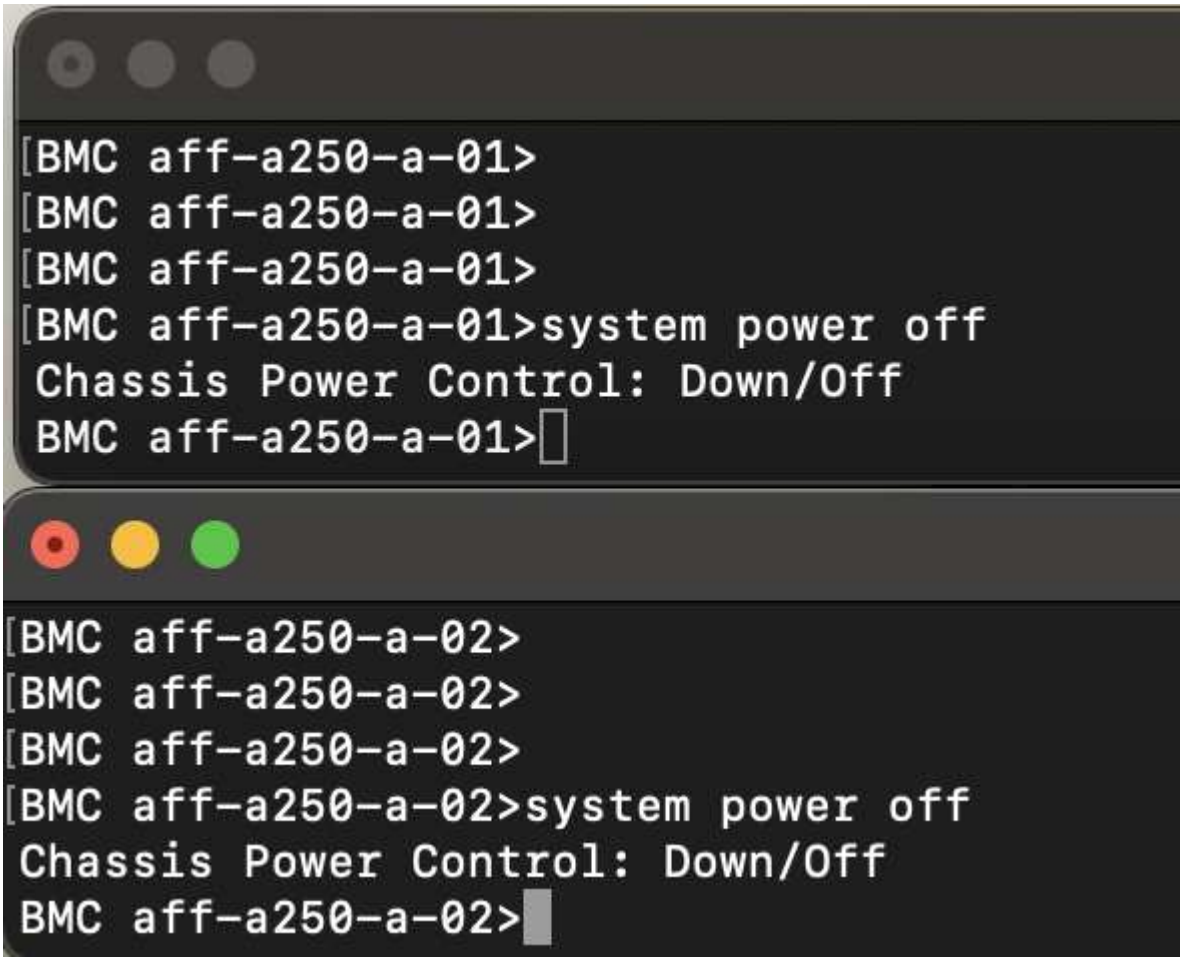
計画的な移行を実行する前に、 VM とホストのアフィニティルールを更新して、サイトで現在実行されている VM がメンテナンス中のサイトから自動的に移行されるようにします。次のスクリーンショットは、サイト A の VM とホストのアフィニティルールを変更し、サイト A からサイト B に VM を自動的に移行する例を示しています。VM をサイト B で実行するように指定する代わりに、アフィニティルールを一時的に無効にして VM を手動で移行することもできます。



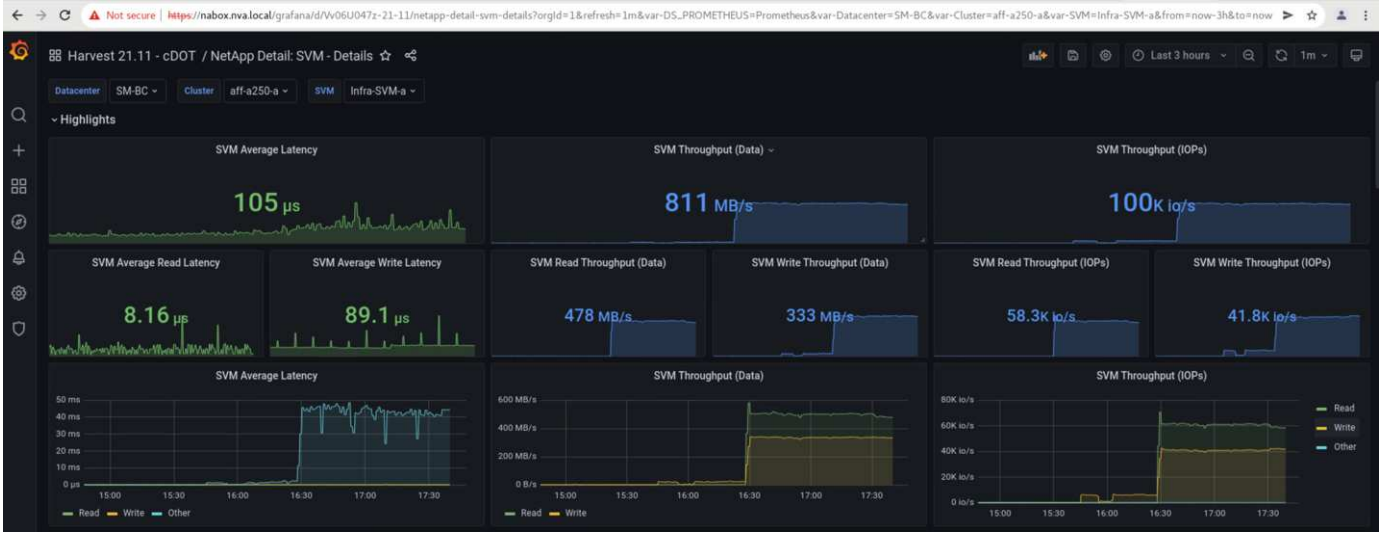
仮想マシンとストレージサービスの移行が完了したら、サーバ、ストレージコントローラ、ディスクシェルフ、およびスイッチの電源をオフにし、必要なサイトのメンテナンス作業を実行できます。サイトのメンテナンスが完了し、 FlexPod インスタンスが稼働状態に戻ったら、 VM のホストグループのアフィニティを変更して元のサイトに戻すことができます。その後、「グループ内のホストで実行する必要があります」 VM/ ホストサイトアフィニティルールを「グループ内のホストで実行する必要があります」に戻して、災害が発生した場合に、他のサイトのホストで仮想マシンを実行できるようにします。検証テストでは、すべての仮想マシンがもう一方のサイトに正常に移行され、データサービスは SM-BC 関係のフェイルオーバーの実行後も問題なく継続されました。

計画外のサイトディザスタシミュレーションでは、サイト障害をシミュレーションするためにサーバとストレージコントローラの電源をオフにしました。VMware HA 機能は、停止した仮想マシンを検出し、サバイバーサイトでその仮想マシンを再起動します。さらに、第 3 のサイトで実行されている ONTAP メディエーターでサイト障害が検出されると、サバイバーサイトがフェイルオーバーを開始して、想定どおりに停止しているサイトのデータサービスの提供を開始します。

次のスクリーンショットは、ストレージコントローラのサービスプロセッサ CLI を使用して、サイト A のストレージ障害をシミュレートするために、クラスターの電源を突然オフにしたことを示しています。



NetApp Harvest データ収集ツールでキャプチャされ、 NAbox 監視ツールで Grafana ダッシュボードに表示されるストレージクラスタの Storage Virtual Machine ダッシュボードは、次の 2 つのスクリーンショットで示されています。IOPS グラフとスループットグラフの右側にあるように、サイト B のクラスタは、サイト A のクラスタが停止したあとすぐにクラスタ A のストレージワークロードを取得します。

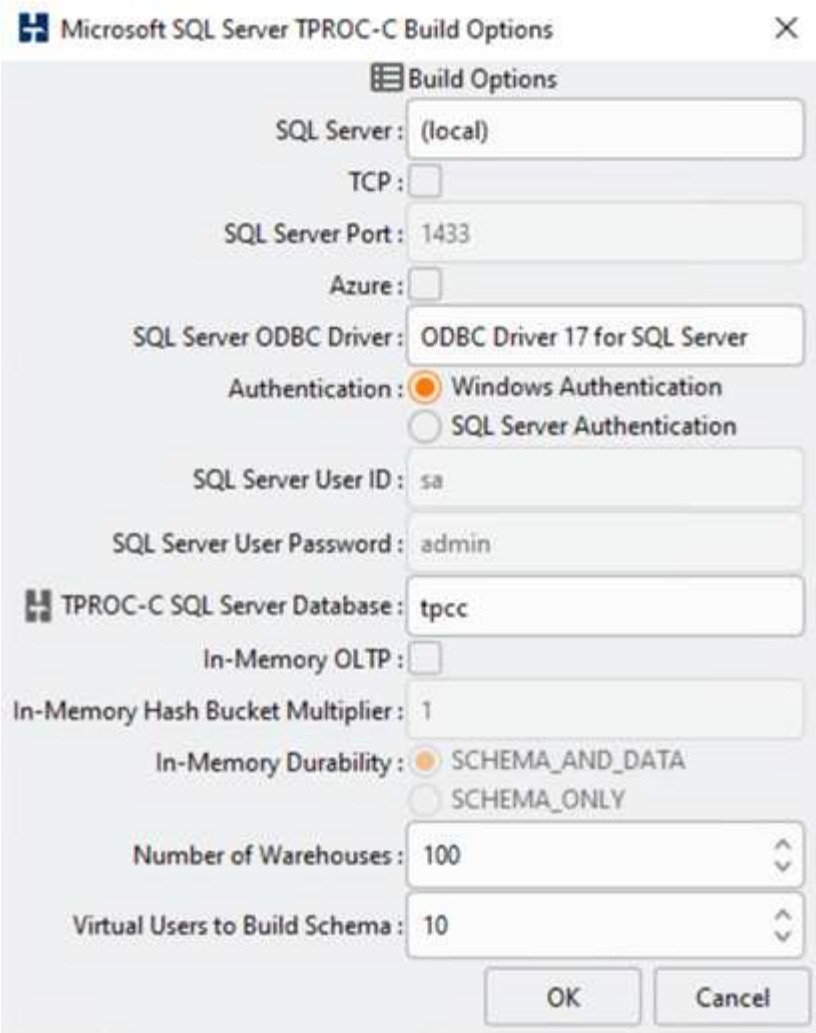


Microsoft SQL Server の場合

Microsoft SQL Server は、エンタープライズ IT に広く採用され、導入されているデータベースプラットフォームです。Microsoft SQL Server 2019 リリースでは、リレーショナルエンジンと分析エンジンに多数の新機能と機能拡張が導入されています。オンプレミス、クラウド、ハイブリッド環境で実行されているアプリケーションのワークロードをサポートし、この 2 つを組み合わせて使用できます。また、 Windows 、 Linux 、コンテナなど、複数のプラットフォームに導入することもできます。

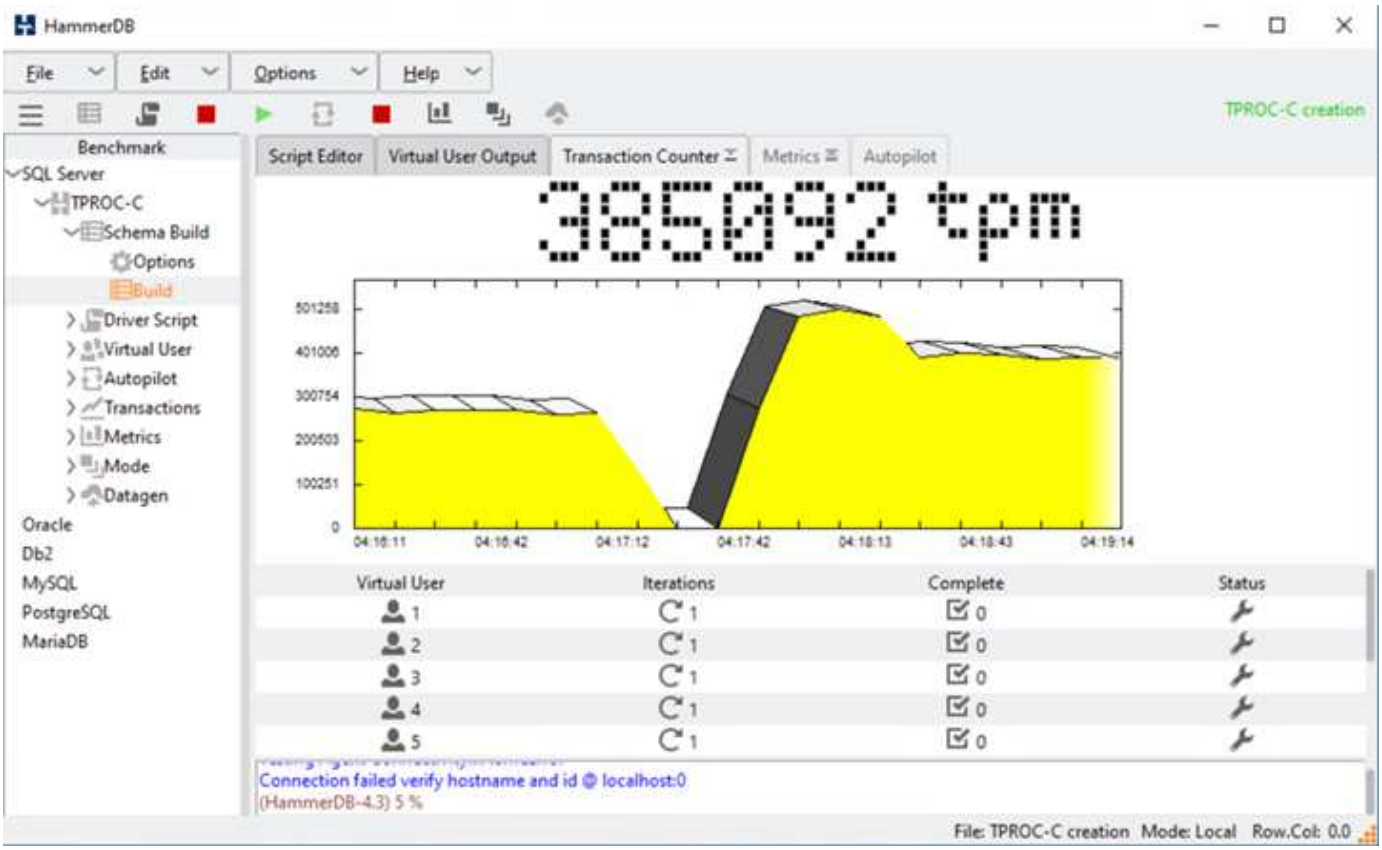
FlexPod SM-BC 解決策 のビジネスクリティカルなワークロード検証の一環として、 Windows Server 2022 VM にインストールされた Microsoft SQL Server 2019 が、 SM-BC が計画的および計画外のストレージフェイルオーバーテスト用の IOMeter VM に含まれています。Windows Server 2022 VM に SQL Server Management Studio をインストールして、 SQL Server を管理します。テストには、 HammerDB データベースツールを使用してデータベーストランザクションが生成されます。

HammerDB データベーステストツールは、 Microsoft SQL Server TPROC-C ワークロードでのテスト用に設定されました。スキーマビルドの構成では、次のスクリーンショットに示すように、オプションが更新され、10 人の仮想ユーザを持つ 100 個のウェアハウスが使用されるようになりました。



スキーマビルドオプションが更新された後、スキーマビルドプロセスが開始されました。数分後に、 system processor CLI コマンドを使用して、 2 ノード AFF A250 ストレージクラスタの両方のノードの電源をほぼ同時にオフにすることで、サイト B の予期しないシミュレートのストレージクラスタ障害が導入されました。

データベーストランザクションが短時間中断されると、災害対策の自動フェイルオーバーが開始され、トランザクションが再開されます。次のスクリーンショットは、 HammerDB トランザクションカウンタのスクリーンショットです。通常、 Microsoft SQL Server のデータベースはサイト B のストレージクラスタにあるため、サイト B のストレージが停止したときにトランザクションが一時停止され、自動フェイルオーバーの発生後に再開されます。



ストレージクラスタの指標は、 NetApp Harvest 監視ツールがインストールされた NAbox ツールを使用して収集しました。結果は、 Storage Virtual Machine とその他のストレージオブジェクトに対応した事前定義された Grafana ダッシュボードに表示されます。このダッシュボードでは、レイテンシ、スループット、 IOPS 、およびその他の詳細情報が、サイト B とサイト A の両方で分けて表示されます

このスクリーンショットは、サイト B のストレージクラスタ用の NABox Grafana パフォーマンスダッシュボードを示しています。

サイト B のストレージクラスタの IOPS は、災害発生前は約 10 万 IOPS でした。その後、災害によってグラフの右側にパフォーマンス指標の値が急激にゼロまで減少しました。サイト B のストレージクラスタが停止しているため、災害発生後にサイト B のクラスタから何も収集できませんでした。

一方、サイト A のストレージクラスタの IOPS は、自動フェイルオーバー後にサイト B から追加のワークロードを受け取りました。次のスクリーンショットでは、 IOPS およびスループットのグラフの右側に、追加のワークロードが簡単に表示されています。このスクリーンショットは、サイト A のストレージクラスタの NAbox Grafana パフォーマンスダッシュボードを示しています。

上記のストレージディザスタテストのシナリオでは、データベースが配置されたサイト B で Microsoft SQL Server ワークロードのストレージクラスタが完全に停止しても運用が継続できることが確認されました。アプリケーションは、災害の検出とフェイルオーバーの発生後、サイト A のストレージクラスタが提供するデータサービスを透過的に使用しました。

コンピューティングレイヤでは、特定のサイトで稼働している VM にホスト障害が発生すると、 VMware HA 機能によって自動的に再起動するように設計されています。サイト全体が停止した場合、 VM とホストのアフィニティルールを使用して、サバイバーサイトで VM を再起動できます。ただし、ビジネスクリティカルなアプリケーションで中断のないサービスを提供するには、アプリケーションのダウンタイムを回避するために、Microsoft Failover Cluster や Kubernetes コンテナベースのアプリケーションアーキテクチャなどのアプリケーションベースのクラスタリングが必要です。アプリケーションベースのクラスタリングの実装については、このテクニカルレポートでは説明していません。関連するドキュメントを参照してください。

"次は終わりです"

まとめ

"前のバージョン：解決策 の検証済みのシナリオ"

SM-BC を備えた FlexPod データセンターは、アクティブ / アクティブのデータセンター設計を使用して、ビジネスクリティカルなワークロードのビジネス継続性とディザスタリカバリを実現します。解決策 は通常、地理的に分散した別々の場所に導入された 2 つのデータセンターをメトロエリア内で相互接続します。NetApp SM-BC 解決策 は、同期レプリケーションを使用して、ビジネスクリティカルなデータサービスをサイト障害から保護します。解決策 では、 2 つの FlexPod 配置サイトのラウンドトリップネットワークレイテンシが 10 ミリ秒未満である必要があります。

第 3 のサイトに導入された NetApp ONTAP メディエーターは、 SM-BC 解決策 を監視し、サイト障害が検出されると自動フェイルオーバーを可能にします。VMware HA 構成および拡張された VMware vSphere Metro

Storage Cluster 構成と NetApp SM-BC をシームレスに連携させて、解決策 が目的のゼロ RPO とほぼゼロ RTO 目標を達成できるようにします。

FlexPod SM-BC 解決策 は、要件を満たしている場合には既存の FlexPod インフラにも導入できます。また、既存の FlexPod に FlexPod 解決策 を追加してビジネス継続性の目標を達成することもできます。管理、監視、自動化のための Cisco Intersight 、 Ansible 、橋本テルクラフォームベースの自動化などの追加ツールがネットアップと Cisco から提供されるため、解決策 の監視や運用に関する分析情報の取得、導入と運用の自動化を簡単に行うことができます。

Microsoft SQL Server などのビジネスクリティカルなアプリケーションの観点からは、 ONTAP SM-BC CG 関係で保護された VMware データストア上にあるデータベースは、サイトストレージが停止しても引き続き使用できます。検証テストで確認したように、データベースが存在するストレージクラスタの停電後、 SM-BC CG 関係のフェイルオーバーが発生し、 Microsoft SQL Server トランザクションがアプリケーションを停止することなく再開します。

アプリケーション単位のきめ細かなデータ保護により、ビジネスクリティカルなアプリケーション向けに ONTAP SM-BC CG 関係を作成して、 RPO ゼロや RTO ほぼゼロの要件を満たすことができます。Microsoft SQL Server アプリケーションが実行されている VMware クラスタがサイトストレージの停止時にも運用を継続できるように、各サイトの ESXi ホストのブート LUN も SM-BC CG 関係によって保護されます。

FlexPod の柔軟性と拡張性により、ビジネス要件の変化に応じて拡張および拡張できる適切なサイズのインフラから始めることができます。この検証済みの設計により、 VMware vSphere ベースのプライベートクラウドを分散型統合インフラに確実に導入できるため、単一点障害の多いシナリオや、重要なビジネスデータサービスを保護するためのサイト障害に対して耐障害性のある解決策 を提供できます。

"次へ：追加情報 およびバージョン履歴の参照先。"

追加情報およびバージョン履歴の参照先

"前へ：終わりに。"

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。

FlexPod

- FlexPod ホームページ

  "https://www.flexpod.com"

- FlexPod のシスコ検証済み設計および導入ガイド

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Cisco サーバ - Unified Computing System （ UCS ）

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- ネットアップの製品マニュアル

  "https://www.netapp.com/support-and-training/documentation/"

- UCS 管理モードの FlexPod データセンター、 VMware vSphere 7.0 U2 、および NetApp ONTAP 9.9 設計ガイド

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- 『 FlexPod Datacenter with Cisco UCS 4.2(1) in UCS Managed Mode 』、『 VMware vSphere 7.0 U2 and NetApp ONTAP 9.9 Deployment Guide 』

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- FlexPod Datacenter with Cisco UCS X シリーズ、 VMware 7.0 U2 、 and NetApp ONTAP 9.9 設計ガイド

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- 『 FlexPod Datacenter with Cisco UCS X Series 、 VMware 7.0 U2 and NetApp ONTAP 9.9 Deployment Guide 』

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- FlexPod Express for VMware vSphere 7.0 と Cisco UCS Mini および NetApp AFF / FAS NVA 設計ガイド

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- 『 FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini and NetApp AFF / FAS NVA Deployment Guide 』

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP と VXLAN マルチサイトフロントエンドファブリック

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- ナボックス

  "https://nabox.org"

- ネットアップハーベスト

  "https://github.com/NetApp/harvest/releases"

SM-BC です

- SM-BC です

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- TR-4978 ：『 SnapMirror Business Continuity （ SM-BC ） ONTAP 9.8 』

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- SnapMirror 関係 ONTAP 9 を正しく削除する方法

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- SnapMirror Synchronous ディザスタリカバリの基本

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- 非同期 SnapMirror ディザスタリカバリの基本

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- データ保護とディザスタリカバリ

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- ONTAP メディエーターサービスをインストールまたはアップグレードします

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

『 VMware vSphere HA and vSphere Metro Storage Cluster 』を参照してください

- vSphere HA クラスタを作成および使用する

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- VMware vSphere Metro Storage Cluster （ vMSC ）

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- 『 VMware vSphere Metro Storage Cluster Recommended Practices 』を参照してください

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP と NetApp SnapMirror ビジネス継続性（ SM-BC ）、 VMware vSphere Metro Storage Cluster （ vMSC ）（ 83370 ）

  "https://kb.vmware.com/s/article/83370"

- VMware vSphere Metro Storage Cluster および ONTAP を使用してティア 1 のアプリケーションとデータベースを保護します

  "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL と HammerDB

- Microsoft SQL Server 2019

"https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- 『Architecting Microsoft SQL Server on VMware vSphere Best Practices Guide』を参照してください

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- HammerDB の Web サイト

  "https://www.hammerdb.com"

互換性マトリックス

- Cisco UCS ハードウェア互換性マトリックス

  "https://ucshcltool.cloudapps.cisco.com/public/"

- NetApp Interoperability Matrix Tool で確認できます

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe の略

  "https://hwu.netapp.com"

- VMware Compatibility Guide』を参照してください

  "http://www.vmware.com/resources/compatibility/search.php"

バージョン履歴

バージョン	日付	ドキュメントのバージョン履歴
バージョン 1.0 以降	2022 年 4 月	初版リリース